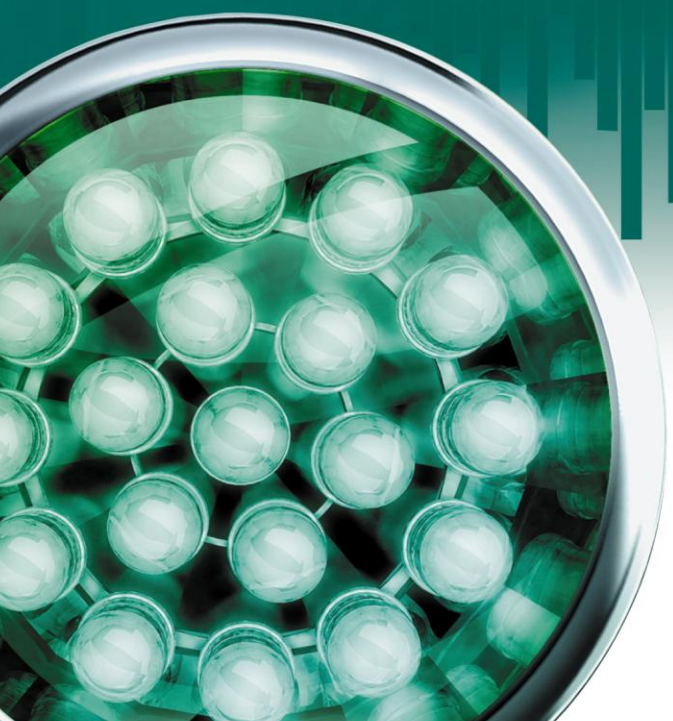
Kaspersky PURE

MANUALE DELL'UTENTE

VERSIONE DELL'APPLICAZIONE: 9.0



KASPERSKY lab

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 software cui è allegata.

Attenzione. Il presente documento è di proprietà di 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 della Federazione russa.

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

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

Il presente documento è soggetto a modifiche senza ulteriori notifiche. La versione più recente del documento è disponibile nel sito Web di 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.

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

Data di revisione: 30/12/2009

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

http://www.kaspersky.com/it/
http://support.kaspersky.com/it/

SOMMARIO

INFORMAZIONI SULLA GUIDA 11

COME OTTENERE INFORMAZIONI SULL'APPLICAZIONE 12

Fonti di informazione per l'esecuzione di ricerche 12

Come contattare l'ufficio vendite 13

Discussioni sulle applicazioni di Kaspersky Lab nel forum Web 13

KASPERSKY PURE 14

Pacchetto di distribuzione 14

Requisiti hardware e software 15

NOZIONI DI BASE SU KASPERSKY PURE 16

Backup 16

Parental Control 17

Centro di controllo 17

Crittografia dei dati 17

Gestione delle password 18

Ottimizzazione del sistema 18

Protezione del computer 18

Componenti di protezione 19

Protezione di dati e attività online 20

Controllo delle applicazioni e dell'accesso ai dati 20

Monitor di Rete 21

Attività di scansione anti-virus 21

Aggiornamenti 21

INSTALLAZIONE DI KASPERSKY PURE NEL COMPUTER 22

Passaggio 1. Verifica dei requisiti di sistema per l'installazione 23

Passaggio 2. Selezione del tipo di installazione 23

Passaggio 3. Accettazione del Contratto di licenza 23

Passaggio 4. Partecipazione al programma Kaspersky Security Network 24

Passaggio 5. Selezione della cartella di destinazione 24

Passaggio 6. Selezione dei componenti dell'applicazione per l'installazione 24

Passaggio 7. Ricerca di altre applicazioni anti-virus 25

Passaggio 8. Disabilitazione del firewall di Microsoft Windows 25

Passaggio 9. Preparazione finale per l'installazione 26

MODIFICA, RIPRISTINO E RIMOZIONE DELL'APPLICAZIONE TRAMITE L'INSTALLAZIONE GUIDATA 27

Passaggio 1. Avvio del programma di installazione 27

Passaggio 2. Selezione dell'operazione 27

Passaggio 3. Completamento della modifica, del ripristino o della rimozione dell'applicazione 28

OPERAZIONI PRELIMINARI 29

Configurazione guidata dell'applicazione 30

Passaggio 1. Attivazione dell'applicazione 31

Passaggio 2. Limitazione dell'accesso all'applicazione 32

Passaggio 3. Selezione della modalità di protezione 33

Passaggio 4. Configurazione dell'aggiornamento dell'applicazione 33

Passaggio 5. Selezione delle minacce da rilevare 34

Passaggio 6. Analisi delle applicazioni installate nel computer ... 34
Passaggio 7. Chiusura della Configurazione guidata ... 34
Selezione del tipo di rete ... 34
Aggiornamento dell'applicazione ... 35
Scansione anti-virus del computer ... 35
Ricerca delle vulnerabilità del computer ... 35
Gestione della licenza ... 36
Partecipazione a Kaspersky Security Network ... 36
Gestione della protezione ... 37
Stato della protezione ... 39
Sospensione della protezione ... 39
Backup ... 40
Parental Control ... 40
Crittografia dei dati ... 40
Gestione delle password ... 41
INTERFACCIA DELL'APPLICAZIONE ... 42
Icona dell'area di notifica ... 42
Menu di scelta rapida ... 43
Finestra principale di Kaspersky PURE ... 44
Protezione del computer ... 46
Backup ... 46
Parental Control ... 47
Notifiche ... 48
Finestra delle impostazioni dell'applicazione ... 49
PROTEZIONE DEL COMPUTER ... 51
Protezione del file system del computer ... 52
Algoritmo di funzionamento del componente ... 53
Modifica del livello di protezione per i file e la memoria ... 54
Modifica delle azioni da eseguire sugli oggetti rilevati ... 54
Creazione di un ambito di protezione ... 55
Utilizzo dell'analisi euristica ... 56
Ottimizzazione della scansione ... 56
Scansione dei file compositi ... 57
Scansione dei file compositi di grandi dimensioni ... 57
Modifica della modalità di scansione ... 58
Tecnologia di scansione ... 58
Sospensione dell'attività del componente: creazione di una pianificazione ... 59
Sospensione dell'attività del componente: creazione di un elenco di applicazioni ... 60
Ripristino delle impostazioni di protezione predefinite ... 61
Protezione della posta ... 62
Algoritmo di funzionamento del componente ... 63
Modifica del livello di protezione dei messaggi di posta elettronica ... 63
Modifica delle azioni da eseguire sugli oggetti rilevati ... 64
Creazione di un ambito di protezione ... 65
Scansione della posta elettronica in Microsoft Office Outlook ... 65
Scansione della posta elettronica in The Bat! ... 66
Utilizzo dell'analisi euristica ... 67
Scansione dei file compositi ... 67

Filtraggio degli allegati ... 67
Ripristino delle impostazioni di protezione della posta elettronica predefinite ... 68
Protezione del traffico Web ... 69
Algoritmo di funzionamento del componente ... 70
Modifica del livello di protezione del traffico HTTP ... 71
Modifica delle azioni da eseguire sugli oggetti rilevati ... 71
Creazione di un ambito di protezione ... 71
Selezione del tipo di scansione ... 72
Barra degli strumenti di Kaspersky ... 73
Utilizzo dell'analisi euristica ... 74
Ottimizzazione della scansione ... 74
Ripristino delle impostazioni di protezione Web predefinite ... 75
Protezione del traffico dei programmi di messaggistica istantanea ... 76
Algoritmo di funzionamento del componente ... 76
Creazione di un ambito di protezione ... 77
Selezione del metodo di scansione ... 77
Utilizzo dell'analisi euristica ... 79
Controllo Applicazioni ... 80
Algoritmo di funzionamento del componente ... 81
Creazione di un ambito di protezione ... 83
Regole di Controllo Applicazioni ... 85
Modalità Protetta di esecuzione delle applicazioni ... 89
Esecuzione di un'applicazione in Modalità Protetta ... 90
Creazione di un collegamento per l'esecuzione dei programmi ... 90
Creazione dell'elenco di applicazioni in esecuzione in modalità protetta ... 91
Selezione della modalità: esecuzione di un'applicazione ... 91
Selezione della modalità: cancellazione dei dati in modalità protetta ... 92
Utilizzo di una cartella condivisa ... 92
Cancellazione dei dati in modalità protetta ... 93
Firewall ... 94
Modifica della categoria della rete ... 94
Estensione dell'intervallo degli indirizzi di rete ... 95
Selezione della modalità di notifica delle modifiche alla rete ... 95
Impostazioni Firewall avanzate ... 96
Regole Firewall ... 96
Difesa Proattiva ... 101
Utilizzo dell'elenco di attività pericolose ... 101
Modifica delle regole per il monitoraggio delle attività pericolose ... 102
Creazione di un gruppo di applicazioni attendibili ... 103
Controllo degli account di sistema ... 104
Prevenzione Intrusioni ... 105
Blocco dei computer da cui proviene l'attacco ... 105
Tipi di attacchi di rete rilevati ... 105
Anti-Spam ... 107
Algoritmo di funzionamento del componente ... 108
Addestramento di Anti-Spam ... 109
Modifica del livello di protezione ... 114
Selezione del metodo di scansione ... 114
Creazione dell'elenco di URL attendibili ... 115

Creazione dell'elenco di mittenti bloccati ... 115
Creazione dell'elenco di frasi bloccate ... 116
Creazione dell'elenco di frasi oscene ... 117
Creazione dell'elenco di mittenti consentiti ... 117
Creazione dell'elenco di frasi consentite ... 118
Importazione dell'elenco di mittenti consentiti ... 119
Determinazione dei fattori di spam e probabile spam ... 120
Selezione dell'algoritmo di riconoscimento dello spam ... 120
Utilizzo delle funzioni avanzate di filtraggio anti-spam ... 121
Aggiunta di un'etichetta all'oggetto del messaggio ... 121
Filtraggio dei messaggi di posta sul server. Gestore della posta ... 122
Esclusione di messaggi di Microsoft Exchange Server dalla scansione ... 122
Azioni da eseguire con la posta spam ... 123
Ripristino delle impostazioni predefinite di Anti-Spam ... 126
Anti-Banner ... 127
Utilizzo dell'analisi euristica ... 127
Impostazioni avanzate del componente ... 128
Creazione dell'elenco di indirizzi di banner consentiti ... 128
Creazione dell'elenco di indirizzi di banner bloccati ... 129
Esportazione/importazione degli elenchi di banner ... 129
Scansione del computer ... 130
Scansione anti-virus ... 130
Scansione Vulnerabilità ... 140
Aggiornamenti ... 144
Avvio dell'aggiornamento ... 145
Rollback dell'ultimo aggiornamento ... 146
Sorgente degli aggiornamenti ... 146
Utilizzo di un server proxy ... 147
Impostazioni internazionali ... 147
Azioni da eseguire dopo l'aggiornamento ... 147
Aggiornamento da una cartella locale ... 148
Modifica della modalità di esecuzione dell'attività di aggiornamento ... 149
Esecuzione degli aggiornamenti utilizzando un altro account utente ... 149
Configurazione delle impostazioni di Protezione del computer ... 150
Protezione ... 151
Anti-Virus File ... 153
Anti-Virus Posta ... 153
Anti-Virus Web ... 154
Anti-Virus IM ... 155
Controllo Applicazioni ... 155
Firewall ... 156
Difesa Proattiva ... 157
Prevenzione Intrusioni ... 158
Anti-Spam ... 158
Anti-Banner ... 159
Scansione ... 160
Aggiornamenti ... 161
Impostazioni ... 162
Rapporti ... 172

Selezione di un componente o di un'attività per creare un rapporto ... 172
Gestione del raggruppamento delle informazioni nel rapporto ... 173
Notifica sul completamento del rapporto ... 173
Selezione dei tipi di evento ... 174
Visualizzazione dei dati sullo schermo ... 175
Modalità di visualizzazione estesa per le statistiche ... 176
Salvataggio di un rapporto in un file ... 176
Utilizzo del filtraggio complesso ... 177
Ricerca eventi ... 177

BACKUP ... 179
Creazione di un'area per l'archivio di backup ... 179
Connessione di un archivio ... 180
Cancellazione di un archivio ... 180
Rimozione di un archivio ... 181
Creazione di un'attività di backup ... 181
Esecuzione di un'attività di backup ... 182
Ricerca di copie di backup ... 182
Visualizzazione dei dati sulle copie di backup ... 183
Ripristino dei dati ... 184
Visualizzazione del rapporto sugli eventi ... 184

PARENTAL CONTROL ... 185
Attivazione e configurazione di Parental Control ... 186
Limitazione del tempo di accesso a Internet ... 187
Accesso a siti Web ... 188
Download di file da Internet ... 188
Modalità di ricerca sicura ... 189
Messaggistica immediata ... 190
Invio di dati personali ... 191
Ricerca per parole chiave ... 192
Limitazione del tempo di utilizzo del computer ... 193
Esecuzione di applicazioni e giochi ... 193
Salvataggio e download delle impostazioni di Parental Control ... 194

OTTIMIZZAZIONE DEL SISTEMA ... 196
Configurazione del browser ... 196
Ripristino dopo un'infezione ... 197
Disco di Ripristino ... 198
Creazione del Disco di Ripristino ... 198
Avvio del computer attraverso il Disco di Ripristino ... 199
Eliminazione definitiva dei dati ... 200
Eliminazione dei dati inutilizzati ... 201
Pulizia guidata dei dati riservati ... 202

TASTIERA VIRTUALE ... 204

CRITTOGRAFIA DEI DATI ... 205
Creazione di un contenitore ... 205
Connessione e disconnessione del contenitore ... 206
Aggiunta di file nel contenitore ... 207
Configurazione del contenitore ... 207

Creazione di un collegamento per l'accesso al contenitore ... 208
GESTIONE DELLE PASSWORD ... 209
Interfaccia di Gestione delle password ... 210
Icona dell'area di notifica ... 210
Menu di scelta rapida di Gestione delle password ... 210
Finestra di Gestione delle password ... 211
Finestra delle impostazioni dell'applicazione ... 211
Pulsante Titolo ... 212
Configurazione guidata ... 212
Gestione del database delle password ... 213
Accesso al database delle password ... 213
Aggiunta di dati personali ... 214
Modifica di dati personali ... 220
Utilizzo di dati personali ... 221
Ricerca di password ... 222
Eliminazione di dati personali ... 222
Importazione ed esportazione di password ... 222
Backup e ripristino del database delle password ... 224
Configurazione delle impostazioni dell'applicazione ... 225
Nome utente predefinito ... 226
Elenco degli account utilizzati di frequente ... 226
Elenco degli indirizzi Web ignorati ... 227
Elenco degli indirizzi Web attendibili ... 228
Avvio veloce delle funzioni dell'applicazione ... 228
Percorso del database delle password ... 229
Creazione di un nuovo database delle password ... 230
Backup del database delle password ... 230
Selezione del metodo di crittografia ... 231
Blocco automatico del database delle password ... 232
Metodo di autorizzazione per Gestione delle password ... 232
Utilizzo di dispositivi USB e Bluetooth ... 233
Modifica della password master ... 234
Creazione di un elenco di browser supportati ... 234
Ulteriori impostazioni ... 235
Funzioni avanzate ... 238
Generatore di password ... 238
Puntatore di Gestione delle password ... 239
CENTRO DI CONTROLLO ... 240
Configurazione della gestione remota ... 240
Analisi della protezione della rete ... 241
Gestione dei componenti di protezione ... 242
Gestione delle licenze ... 242
Gestione di Parental Control ... 242
Scansione remota di virus e vulnerabilità ... 243
Aggiornamento dei database e dei moduli dell'applicazione ... 243
Backup remoto ... 244
CONFIGURAZIONE DELLE IMPOSTAZIONI DI KASPERSKY PURE ... 245
Impostazioni generali ... 246

Esecuzione di Kaspersky PURE all'avvio di Windows ... 247
Restrizione dell'accesso a Kaspersky PURE ... 247
Auto-Difesa ... 247
Risparmio energetico per funzionamento a batteria ... 248
Compatibilità ... 248
Tecnologia avanzata di disinfezione ... 248
Prestazioni del computer durante l'esecuzione delle attività ... 249
Server proxy ... 249
Notifiche ... 249
Disabilitazione delle notifiche acustiche ... 250
Invio di notifiche via posta elettronica ... 251
Rapporti ... 251
Registrazione degli eventi nei rapporti ... 251
Cancellazione del contenuto dei rapporti dell'applicazione ... 251
Archiviazione di rapporti ... 251
Commenti ... 252
Aspetto dell'applicazione ... 252
Elementi attivi dell'interfaccia ... 252
Interfaccia di Kaspersky PURE ... 253
Profilo Gioco ... 253
Gestione delle impostazioni dell'applicazione ... 254
Esportazione e importazione delle impostazioni di Kaspersky PURE ... 254
Ripristino delle impostazioni predefinite ... 255

NOTIFICHE ... 256
Impossibile disinfettare l'oggetto ... 257
Server degli aggiornamenti non disponibile ... 258
Rilevamento di un oggetto dannoso ... 258
Rilevamento di un oggetto pericoloso nel traffico ... 258
Rilevamento di un oggetto sospetto ... 259
Rilevamento di un'attività pericolosa nel sistema ... 260
Rilevamento di processi nascosti ... 260
Rilevamento di un tentativo di accesso al Registro di sistema ... 261
Rilevamento dell'attività di rete di un'applicazione ... 261
Rilevamento di una nuova rete ... 262
Rilevamento di un attacco di phishing ... 263
Rilevamento di un collegamento sospetto ... 263
Rilevamento di un certificato non valido ... 263
Limitazione dell'utilizzo dell'applicazione ... 264
Richiesta di esecuzione di una procedura speciale ... 264
File già esistente ... 264

ELIMINAZIONE DEI PROBLEMI ... 265
Creazione di un rapporto sullo stato del sistema ... 265
Invio di file di dati ... 266
Esecuzione di script AVZ ... 267
Creazione di un file di traccia ... 268

COME CONTATTARE IL SERVIZIO DI ASSISTENZA TECNICA 269
INFORMATIVA SULLA RACCOLTA DATI PER KASPERSKY SECURITY NETWORK 270
UTILIZZO DI CODICE DI TERZE PARTI 274
Libreria Agava-C 276
Libreria di software per la protezione dei dati Crypto C 276
Libreria Fastscript 1.9 276
Libreria Pcre 7.4, 7.7 276
Libreria del parser Bison GNU 277
Libreria AGG 2.4 277
Libreria OpenSSL 0.9.8d 277
Libreria Gecko SDK 1.8 279
Libreria Zlib 1.2 279
Libreria Libpng 1.2.8, 1.2.29 279
Libreria Libnkfm 2.0.5 279
Libreria Expat 1.2, 2.0.1 279
Libreria Info-ZIP 5.51 280
Libreria Windows Installer XML (WiX) 2.0 280
Libreria Passthru 283
Libreria Filter 283
Libreria Netcfg 283
Libreria Pcre 3.0 283
Libreria RFC1321-based (RSA-free) MD5 284
Libreria Windows Template (WTL 7.5) 284
Libreria Libjpeg 6b 286
Libreria Libungif 3.0 288
Libreria Libxdr 288
Libreria Tiniconv - 1.0.0 288
Libreria Bzip2/libbzip2 1.0.5 293
Libreria Libspf2-1.2.9 294
Libreria Protocol Buffer 294
Libreria Sqlite 3.5.9 295
Libreria Icu 4.0 295
Altre informazioni 295
GLOSSARIO 296
KASPERSKY LAB 305
CONTRATTO DI LICENZA 306
INDICE 312

INFORMAZIONI SULLA GUIDA

Il Manuale dell'utente di Kaspersky PURE contiene informazioni sul funzionamento di Kaspersky PURE, sulle principali attività di protezione delle reti domestiche e sulla configurazione dell'applicazione. Il presente documento è destinato a chiunque utilizza l'applicazione Kaspersky PURE per proteggere i computer all'interno di reti domestiche.

Il Manuale dell'utente di Kaspersky PURE contiene le seguenti sezioni principali:

- Come ottenere informazioni sull'applicazione (vedere pagina 12). Questa sezione descrive varie fonti di informazioni sull'acquisto, l'installazione e l'utilizzo di Kaspersky PURE.
- Nozioni di base su Kaspersky PURE (vedere pagina 16). Questa sezione descrive le nozioni di base relative all'utilizzo delle varie funzionalità dell'applicazione per una protezione completa delle reti domestiche.
- Installazione dell'applicazione (vedere pagina 22). Questa sezione fornisce istruzioni passo passo per la corretta installazione dell'applicazione.
- Operazioni preliminari (vedere pagina 29). Questa sezione descrive le principali operazioni da eseguire dopo l'installazione dell'applicazione nel computer, allo scopo di garantire una protezione affidabile.
- Interfaccia dell'applicazione (vedere pagina 42). Questa sezione descrive l'interfaccia utente dell'applicazione, tra cui la finestra principale, il menu di scelta rapida, il servizio di notifica e altri elementi.
- Protezione del computer. Questa sezione descrive il funzionamento dei componenti di Protezione del computer progettati per assicurare la protezione del computer da varie minacce.
- Backup (vedere pagina 179). Questa sezione contiene informazioni sul backup e il ripristino dei dati dalle copie di backup.
- Parental Control (vedere pagina 185). Questa sezione contiene informazioni sulla protezione degli utenti delle reti domestiche dalle potenziali minacce durante l'utilizzo del computer o l'esplorazione di Internet, nonché sulla gestione delle impostazioni di Parental Control.
- Ottimizzazione del sistema. Questa sezione contiene informazioni sulle procedure guidate e gli strumenti che possono essere utili per una protezione avanzata.
- Tastiera virtuale (vedere pagina 204). Questa sezione descrive come utilizzare la tastiera virtuale per proteggere i dati dai keylogger.
- Crittografia dei dati (vedere pagina 205). Questa sezione descrive come utilizzare i contenitori crittografati per archiviare i dati riservati.
- Gestione delle password (vedere pagina 240). Questa sezione descrive le modalità di gestione delle password e di altri dati personali.
- Centro di controllo (vedere pagina 240). Questa sezione descrive la gestione remota della protezione delle reti domestiche.
- Configurazione di Kaspersky PURE (vedere pagina 245). Questa sezione descrive le modalità di gestione delle impostazioni dell'applicazione allo scopo di garantire una protezione flessibile ed efficiente.
- Eliminazione dei problemi (vedere pagina 265). Questa sezione descrive le azioni da intraprendere quando si verificano problemi nell'esecuzione di Kaspersky PURE.

COME OTTENERE INFORMAZIONI SULL'APPLICAZIONE

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

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

IN QUESTA SEZIONE:

Fonti di informazione per l'esecuzione di ricerche 12

Come contattare l'ufficio vendite 13

Discussioni sulle applicazioni di Kaspersky Lab nel forum Web 13

FONTI DI INFORMAZIONE PER L'ESECUZIONE DI RICERCHE

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

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

Pagina dell'applicazione nel sito Web di Kaspersky Lab

http://www.kaspersky.com/it/kaspersky-pure

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

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

http://support.kaspersky.it/pure

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

Tali articoli contengono informazioni utili, consigli e FAQ sull'acquisto, sull'installazione e sull'utilizzo dell'applicazione. Gli articoli sono ordinati per argomento. Gli articoli possono fornire risposte a domande relative non solo all'applicazione specifica, ma anche ad altri prodotti di Kaspersky Lab. Possono inoltre contenere notizie fornite dal servizio di assistenza tecnica.

Servizio di supporto FastTrack

Nella pagina di questa servizio è possibile trovare il database delle FAQ con risposte che vengono aggiornate regolarmente. Per utilizzare il servizio è necessaria una connessione a Internet.

Per accedere alla pagina del servizio, fare clic sul collegamento **Assistenza** e, nella finestra visualizzata, fare clic sul pulsante **Assistenza FastTrack**.

Guida in linea

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

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

Documentazione

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

COME CONTATTARE L'UFFICIO VENDITE

In caso di domande riguardanti la scelta o l'acquisto di Kaspersky PURE o l'estensione della licenza, è possibile contattare l'ufficio vendite di Mosca ai numeri:

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

Il servizio è disponibile in russo e in inglese.

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

DISCUSSIONI SULLE APPLICAZIONI DI KASPERSKY LAB NEL FORUM WEB

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.

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

KASPERSKY PURE

Kaspersky PURE è una nuova generazione di soluzioni di protezione per le reti domestiche.

Ciò che rende Kaspersky PURE veramente unico, anche rispetto ad altri prodotti software Kaspersky Lab, è l'approccio diversificato alla protezione delle reti domestiche.

IN QUESTA SEZIONE:

Pacchetto di distribuzione 14

Requisiti hardware e software 15

PACCHETTO DI DISTRIBUZIONE

È possibile acquistare Kaspersky PURE dai partner di Kaspersky Lab (edizione in scatola) o da un negozio online (come ad esempio http://www.kaspersky.com, sezione **eStore**).

Se è stato acquistato il prodotto in scatola, il pacchetto di distribuzione include i seguenti elementi:

- Una busta sigillata con il CD di installazione contenente i file del programma e la documentazione in formato PDF.
- La documentazione in formato stampato, ovvero il Manuale dell'utente e la Guida introduttiva.
- Il Contratto di licenza (a seconda del paese).
- La scheda di attivazione, con il codice di attivazione e le istruzioni sull'attivazione dell'applicazione (a seconda del paese).

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

Leggere con attenzione il Contratto di licenza.

Se non si accettano le condizioni del Contratto di licenza, è possibile restituire il prodotto in scatola al partner da cui è stato acquistato. In questo caso, il prodotto verrà rimborsato al prezzo di acquisto. La busta con il CD (o i dischi floppy) di installazione deve tuttavia rimanere sigillata.

Aprendo la busta con il CD (o i dischi floppy) di installazione si accettano le condizioni del Contratto di licenza.

Prima di aprire la busta con il CD (o i dischi floppy) di installazione, leggere attentamente il Contratto di licenza.

In caso di acquisto di Kaspersky PURE da eStore, il prodotto viene copiato dal sito Web di Kaspersky Lab. Il pacchetto di installazione include il prodotto stesso e il presente Contratto di licenza. Il codice di attivazione verrà inviato tramite e-mail dopo il pagamento.

REQUISITI HARDWARE E SOFTWARE

Per il corretto funzionamento di Kaspersky PURE, il computer deve soddisfare i seguenti requisiti minimi:

Requisiti generali:

- 320 MB di spazio libero su disco rigido.
- Unità CD-ROM (per l'installazione di Kaspersky PURE dal CD di installazione).
- Microsoft Internet Explorer 6.0 o versione successiva (per l'aggiornamento dei database dell'applicazione e dei moduli software via Internet).
- Microsoft Windows Installer 2.0.

Microsoft Windows XP Home Edition (Service Pack 3), Microsoft Windows XP Professional (Service Pack 3), Microsoft Windows XP Professional x64 Edition (Service Pack 3)*:*

- processore Intel Pentium da 300 MHz o superiore (o un processore equivalente compatibile);
- 256 MB di RAM.

Microsoft Windows Vista Home Basic, Microsoft Windows Vista Home Premium, Microsoft Windows Vista Business, Microsoft Windows Vista Enterprise, Microsoft Windows Vista Ultimate:

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

Microsoft Windows 7 Home Premium, Microsoft Windows 7 Professional, Microsoft Windows 7 Ultimate:

- processore Intel Pentium da 1 GHz a 32 bit (x86) / a 64 bit (x64) o superiore (o un processore equivalentecompatibile);
- 1 GB di RAM (a 32 bit); 2 GB di RAM (a 64 bit).

NOZIONI DI BASE SU KASPERSKY PURE

Kaspersky PURE è un programma progettato per garantire una protezione completa dei computer all'interno di una rete domestica. Kaspersky PURE include i seguenti moduli:

- Protezione del computer (vedere pagina 18), che assicura la protezione del computer contro le minacce conosciute e sconosciute;
- (vedere pagina 16), che consente di ripristinare velocemente le informazioni in caso di perdite di dati;
- Crittografia dei dati (vedere pagina 17), che protegge le informazioni riservate dagli accessi non autorizzati;
- (vedere pagina 17), che permette di salvaguardare bambini e adolescenti dalle potenziali minacce legate all'utilizzo del computer e di Internet;
- (vedere pagina 18), che consente di memorizzare in modo sicuro password e altri dati sugli account, garantendo la massima riservatezza durante la compilazione dei moduli di autorizzazione;
- (vedere pagina 17), che consente di gestire in remoto la protezione dei computer della rete;
- Ottimizzazione del sistema (vedere pagina 18), utilizzato per l'ottimizzazione delle impostazioni del sistema operativo e l'esecuzione di specifiche attività per la protezione del computer.

IN QUESTA SEZIONE:

Backup 16

Parental Control 17

Centro di controllo 17

Crittografia dei dati 17

Gestione delle password 18

Ottimizzazione del sistema 18

Protezione del computer 18

BACKUP

I dati memorizzati in un computer possono andare persi per diverse ragioni, come l'azione di un virus e la modifica o l'eliminazione di informazioni operata da un altro utente. Per evitare di perdere informazioni importanti, è consigliabile eseguire periodicamente il backup dei dati.

In tal modo è possibile creare copie di backup degli oggetti in uno speciale archivio nel dispositivo selezionato. A tale scopo, è necessario configurare le attività di backup. Dopo avere eseguito l'attività manualmente o automaticamente, in base a una pianificazione, le copie di backup dei file selezionati vengono create nell'archivio. Se necessario, la versione desiderata del file salvato può essere ripristinata dalla copia di backup. Un backup periodico assicura pertanto un ulteriore livello di protezione dei dati.

VEDERE ANCHE:

Backup 179

PARENTAL CONTROL

Parental Control è progettato per salvaguardare bambini e adolescenti dalle potenziali minacce legate all'utilizzo del computer e di Internet.

Parental Control consente di limitare in modo flessibile l'accesso a risorse e applicazioni per diversi utenti, a seconda dell'età e del livello di esperienza. Questa funzione consente inoltre di visualizzare rapporti statistici sulle azioni degli utenti.

Le restrizioni specificate possono essere di tre categorie:

- utilizzo di Internet;
- messaggistica immediata;
- utilizzo del computer.

VEDERE ANCHE:

Parental Control 185

CENTRO DI CONTROLLO

Le reti domestiche spesso comprendono diversi computer, che rendono più difficile gestire la protezione della rete. La vulnerabilità di un computer mette a rischio l'intera rete.

Centro di controllo offre un'area di lavoro che consente di avviare attività di scansione anti-virus e di aggiornamento per l'intera rete o per singoli computer, gestire il backup dei dati e configurare le impostazioni di Parental Control in tutti i computer della rete. Questo assicura la gestione remota della protezione in tutti i computer della rete domestica.

VEDERE ANCHE:

Centro di controllo 240

CRITTOGRAFIA DEI DATI

Le informazioni riservate salvate in formato elettronico richiedono un'ulteriore protezione dall'accesso non autorizzato. L'archiviazione dei dati in un contenitore crittografato assicura tale protezione.

La crittografia dei dati consente di creare speciali contenitori crittografati nell'unità selezionata. Nel sistema tali contenitori vengono visualizzati come unità virtuali rimovibili. Per accedere ai dati nel contenitore crittografato è necessario specificare una password.

VEDERE ANCHE:

Crittografia dei dati 205

GESTIONE DELLE PASSWORD

Al giorno d'oggi, per accedere alla maggior parte dei servizi e delle risorse occorre registrare e immettere dati sugli account per l'autenticazione. Per motivi di protezione, non è consigliabile utilizzare gli stessi account utente per differenti risorse o annotare nomi utente e password. Di conseguenza, spesso gli utenti non sono in grado di ricordare grandi quantità di dati sugli account, cosa che rende particolarmente importante la memorizzazione protetta delle password.

Gestione delle password rende possibile archiviare in formato crittografato differenti dati personali, quali nomi utente, password, indirizzi, numeri di telefono e di carta di credito. L'accesso ai dati viene protetto tramite una singola password master. Una volta immessa la password master, Gestione delle password può compilare automaticamente i campi nei vari moduli di autorizzazione. In questo modo è sufficiente ricordare una sola password master per gestire tutti i dati sugli account.

VEDERE ANCHE:

Gestione delle password 209

OTTIMIZZAZIONE DEL SISTEMA

Garantire la protezione del computer è un'attività complessa che richiede una conoscenza approfondita delle funzioni del sistema operativo e delle vulnerabilità dei software. D'altro canto, la grande quantità e varietà di informazioni sulla protezione dei sistemi ne complica l'analisi e l'elaborazione.

Per agevolare l'esecuzione di specifiche attività per la protezione del computer, Kaspersky PURE include i seguenti strumenti e procedure guidate:

La Configurazione guidata del browser (vedere pagina 196) consente di eseguire l'analisi e la valutazione delle impostazioni di Microsoft Internet Explorer, innanzitutto rispetto alla protezione.

- Il Ripristino guidato del sistema (vedere pagina 197) elimina le tracce della presenza di oggetti malware nel sistema.
- La Pulizia guidata dei dati riservati (vedere pagina 202) ricerca ed elimina le tracce delle attività di un utente nel sistema e nelle impostazioni del sistema operativo che consentono di raccogliere informazioni sulle attività dell'utente.
- Disco di ripristino (vedere pagina 198) è stato progettato per eseguire la scansione dei computer compatibili con le piattaforme x86 e per disinfettarli. È consigliabile utilizzarlo quando il livello di infezione è tale da reputare impossibile la disinfezione tramite applicazioni anti-virus o utilità di rimozione di malware.
- L'Eliminazione definitiva dei dati (vedere pagina 200) impedisce il ripristino non autorizzato dei fine eliminati.
- La Cancellazione guidata dei dati (vedere pagina 201) elimina i file temporanei e inutilizzati che richiedono un volume considerevole di spazio su disco o possono essere sfruttati dal malware.

VEDERE ANCHE:

Ottimizzazione del sistema 196

PROTEZIONE DEL COMPUTER

Protezione del computer protegge il sistema da minacce nuove o già note. Ogni tipologia di minaccia viene elaborata da un componente distinto dell'applicazione. Questa struttura del sistema di protezione consente una configurazione flessibile basata sulle esigenze specifiche personali o di un'intera azienda.

Protezione del computer include i seguenti strumenti di protezione:

- Componenti di protezione (vedere pagina 19), che garantiscono la sicurezza di:
  - file e dati personali;
  - sistema;
  - attività di rete.
- Attività di scansione anti-virus (vedere pagina 21), che consentono di esaminare singoli file, cartelle, unità o aree alla ricerca di virus o di eseguire una scansione completa del computer.
- (vedere pagina 21): garantisce che i moduli interni e i database dell'applicazione, utilizzati per ricercare i programmi dannosi, siano aggiornati.

COMPONENTI DI PROTEZIONE

I componenti di protezione seguenti offrono una difesa al computer in tempo reale:

Anti-Virus File (vedere pagina 52)

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

Anti-Virus Posta (vedere pagina 62)

Anti-Virus Posta esamina tutti i messaggi di posta elettronica in arrivo e in uscita del computer. Analizza i messaggi di posta alla ricerca di programmi dannosi. Il messaggio di posta è disponibile per il destinatario solo se non contiene oggetti pericolosi. Il componente inoltre analizza i messaggi di posta elettronica per rilevare phishing.

Anti-Virus Web (vedere pagina 69)

Anti-Virus Web intercetta e blocca gli script nei siti web se costituiscono una minaccia. Anche tutto il traffico HTTP è soggetto a un monitoraggio completo. Il componente inoltre analizza le pagine Web per rilevare phishing.

Anti-Virus IM (vedere pagina 76)

Anti-Virus IM garantisce un utilizzo sicuro dei sistemi di messaggistica immediata. Il componente protegge le informazioni che il computer riceve tramite protocolli IM. Anti-Virus IM garantisce il funzionamento sicuro della messaggistica immediata.

Controllo Applicazioni (vedere pagina 80)

Il componente Controllo Applicazioni registra le azioni eseguite dalle applicazioni nel sistema e ne gestisce le attività in base al gruppo al quale le assegna. Per ciascun gruppo di applicazioni viene definito un insieme di regole. Tali regole gestiscono l'accesso dell'applicazione a varie risorse.

Firewall (vedere pagina 94)

Il Firewall garantisce la protezione del lavoro nelle reti locali e in Internet e filtra tutte le attività di rete utilizzando regole di due tipi: *regole per le applicazioni* e *regole pacchetto*.

Difesa Proattiva (vedere pagina 101)

Difesa Proattiva consente di rilevare un nuovo programma dannoso prima che esegua la propria attività. Il componente è stato progettato per il monitoraggio e l'analisi del comportamento di tutte le applicazioni installate nel computer. In base alle azioni eseguite, Protezione del computer stabilisce se l'applicazione è potenzialmente

pericolosa. Il computer è pertanto protetto non solo dai virus noti ma anche da quelli nuovi, nonché da quelli che non sono stati ancora scoperti.

Prevenzione Intrusioni (vedere pagina 105)

Prevenzione Intrusioni si carica all'avvio del sistema operativo e tiene traccia del traffico di rete in entrata alla ricerca di attività tipiche degli attacchi di rete. In seguito all'individuazione di un tentativo di attacco al computer, Protezione del computer blocca tutte le attività di rete del computer da cui proviene l'attacco verso il computer in uso.

Anti-Spam (vedere pagina 107)

Anti-Spam si integra nel client di posta installato nel computer e monitora tutti i messaggi di posta elettronica in entrata alla ricerca di spam. Tutti i messaggi contenenti spam vengono contrassegnati con un'intestazione speciale. È inoltre possibile configurare Anti-Spam per l'elaborazione dello spam (eliminazione automatica, spostamento in una cartella speciale e così via). Il componente inoltre analizza i messaggi di posta elettronica per rilevare phishing.

Monitor di Rete (vedere pagina 21)

Il componente è stato progettato per visualizzare informazioni sulle attività di rete in modalità tempo reale.

Anti-Phishing

Il componente, integrato in Anti-Virus Web, Anti-Spam e Anti-Virus IM, consente di verificare che gli indirizzi Web non siano inclusi nell'elenco di indirizzi Web sospetti e di phishing.

Anti-Banner (vedere pagina 127)

Anti-Banner blocca le informazioni pubblicitarie contenute nei banner incorporati nelle interfacce di vari programmi installati nel computer o visualizzate online.

PROTEZIONE DI DATI E ATTIVITÀ ONLINE

Protezione del computer protegge i dati memorizzati nel computer da malware e accessi non autorizzati, garantendo un accesso sicuro alla rete locale e a Internet.

Gli oggetti protetti si suddividono in tre gruppi:

- File, dati personali, parametri di accesso a risorse diverse (nomi utente e password), dati delle carte di credito e così via. La protezione di questi oggetti viene garantita da Anti-Virus File, Controllo Applicazioni e Difesa Proattiva.
- Applicazioni installate nel computer e oggetti del sistema operativo. La protezione di questi oggetti viene garantita da Anti-Virus Posta, Anti-Virus Web, Anti-Virus IM, Controllo Applicazioni, Difesa Proattiva, Prevenzione Intrusioni e Anti-Spam.
- Attività online: utilizzo di sistemi di pagamento, protezione della posta elettronica da spam e virus e così via. La protezione di questi oggetti viene garantita da Anti-Virus Posta, Anti-Virus Web, Anti-Virus IM, Firewall, Prevenzione Intrusioni, Anti-Spam, Monitor di Rete, Anti-Banner.

CONTROLLO DELLE APPLICAZIONI E DELL'ACCESSO AI DATI

Protezione del computer impedisce che le applicazioni eseguano azioni che possono mettere a rischio il sistema, controlla l'accesso ai dati personali e consente di eseguire le applicazioni in modalità protetta. Viene eseguito con l'ausilio degli strumenti seguenti:

- **Controllo delle attività delle applicazioni** (vedere pagina 80). Il componente registra le azioni eseguite dalle applicazioni nel sistema e ne gestisce le attività in base al relativo gruppo di appartenenza. Per ciascun gruppo di applicazioni viene definito un insieme di regole. Tali regole gestiscono l'accesso dell'applicazione a varie risorse.

- **Protezione dell'identità digitale** (vedere pagina 83). Controllo Applicazioni gestisce i diritti delle applicazioni per l'esecuzione di azioni sui dati personali dell'utente. Questi ultimi includono file, cartelle e chiavi del Registro di sistema, che contengono impostazioni e dati importanti delle applicazioni di uso comune, nonché file dell'utente (cartella Documenti, cookie, informazioni sull'attività dell'utente).

- **Modalità Protetta** (vedere pagina 89). Protezione del computer garantisce la massima protezione per gli oggetti del sistema operativo e i dati personali dell'utente mediante l'esecuzione delle applicazioni sconosciute nell'ambiente virtuale protetto.

MONITOR DI RETE

Monitor di Rete è uno strumento che consente di visualizzare informazioni sulle attività di rete in tempo reale. Per eseguire Monitor di Rete, utilizzare il collegamento **Monitor di Rete** nella finestra principale di Protezione del computer.

Nella finestra visualizzata le informazioni sono raggruppate nelle schede seguenti:

- · Nella scheda *Connessioni e porte* sono elencate tutte le porte aperte e le connessioni di rete attualmente attive nel computer.

- · Nella scheda *Firewall: registro di elaborazione delle regole* vengono visualizzate informazioni sull'utilizzo delle regole di filtraggio.

- · Nella scheda *Traffico di rete* vengono visualizzate informazioni su tutte le connessioni in entrata e in uscita stabilite tra il computer e altri computer, inclusi server Web, server di posta e così via.

- · Nella scheda *Computer bloccati* sono elencati i computer bloccati.

ATTIVITÀ DI SCANSIONE ANTI-VIRUS

Oltre ad attivare una protezione costante da tutti i programmai dannosi, è estremamente importante eseguire la scansione anti-virus periodica del computer. Questa operazione è necessaria per eliminare la possibilità che si diffondano programmi dannosi non rilevati dai componenti di protezione in tempo reale, ad esempio, perché è stato impostato un livello di protezione basso.

In Protezione del computer sono incluse le seguenti attività di scansione anti-virus:

- **Scansione Personalizzata**. Scansione degli oggetti selezionati dall'utente. È possibile esaminare qualsiasi oggetto nel file system del computer.

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

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

AGGIORNAMENTI

Per bloccare gli attacchi di rete oppure eliminare un virus o un programma dannoso, è necessario aggiornare Kaspersky PURE regolarmente. Il componente **Aggiornamenti** è progettato per questo scopo. Consente infatti di gestire l'aggiornamento dei moduli e dei database utilizzati dall'applicazione.

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

INSTALLAZIONE DI KASPERSKY PURE NEL COMPUTER

Kaspersky PURE viene installato nel computer in modalità interattiva utilizzando l'Installazione guidata avviata quando si esegue il file di installazione.

Prima di iniziare l'installazione, è consigliabile chiudere tutte le applicazioni attualmente in esecuzione.

Per installare Kaspersky PURE nel computer in uso, eseguire il file di installazione, ovvero il file con estensione .exe, nel CD del prodotto. È anche possibile ricevere il pacchetto di installazione dell'applicazione via Internet.

L'installazione di Kaspersky PURE dal pacchetto di installazione scaricato via Internet è identica a quella dal CD di installazione.

Quando si apre il pacchetto di installazione, viene automaticamente eseguita una ricerca del file di installazione (con estensione *.msi). Se viene rilevato, l'applicazione cerca una versione più recente del prodotto nei server Kaspersky Lab su Internet. Se la ricerca del pacchetto di installazione non produce risultati, verrà visualizzato un messaggio in cui si propone all'utente di scaricarlo. Al termine del download, viene avviata l'installazione di Kaspersky PURE. Se il download viene annullato, l'installazione dell'applicazione proseguirà in modalità standard.

La procedura guidata è visualizzata come una sequenza di finestre (passaggi). Per semplificare la gestione del processo di installazione, ogni finestra contiene il seguente set di pulsanti:

- **Avanti** – accetta l'azione eseguita e accede al passaggio successivo della procedura di installazione.
- **Indietro** – torna al passaggio precedente della procedura di installazione.
- **Annulla** – annulla l'installazione.
- **Fine** – completa la procedura di installazione dell'applicazione.

Di seguito vengono illustrati in modo dettagliato tutti i passaggi della procedura di installazione.

IN QUESTA SEZIONE:

Passaggio 1. Verifica dei requisiti di sistema per l'installazione 23

Passaggio 2. Selezione del tipo di installazione 23

Passaggio 3. Accettazione del Contratto di licenza 23

Passaggio 4. Partecipazione al programma Kaspersky Security Network 24

Passaggio 5. Selezione della cartella di destinazione 24

Passaggio 6. Selezione dei componenti dell'applicazione per l'installazione 24

Passaggio 7. Ricerca di altre applicazioni anti-virus 25

Passaggio 8. Disabilitazione del firewall di Microsoft Windows 25

Passaggio 9. Preparazione finale per l'installazione 26

PASSAGGIO 1. VERIFICA DEI REQUISITI DI SISTEMA PER L'INSTALLAZIONE

Prima di installare Kaspersky PURE, viene eseguito un controllo dei seguenti elementi:

- se il sistema operativo e i service pack soddisfano i requisiti del programma per l'installazione;
- se il software necessario per il corretto funzionamento di Kaspersky PURE è installato nel computer;
- se l'utente dispone dei diritti per l'installazione del software.

Se il controllo viene superato, viene visualizzata la finestra dell'Installazione guidata di Kaspersky PURE.

Se una delle condizioni non è soddisfatta, viene visualizzata una notifica con la descrizione del problema. In questo caso, prima di installare l'applicazione Kaspersky Lab, è consigliabile installare tutte le applicazioni e i service pack necessari tramite il servizio Windows Update.

PASSAGGIO 2. SELEZIONE DEL TIPO DI INSTALLAZIONE

Se il computer soddisfa i requisiti di sistema, verrà visualizzata la finestra dell'Installazione guidata. Verrà richiesto di selezionare una delle seguenti modalità di installazione:

- *Installazione Express*. Se si seleziona questa opzione (la casella **Installazione personalizzata** è deselezionata), l'applicazione verrà installata completamente nel computer. Verranno applicate le impostazioni di protezione consigliate da Kaspersky Lab. Al termine dell'installazione, è possibile attivare Kaspersky PURE e configurare la protezione dell'applicazione dall'accesso non autorizzato.
- *Installazione personalizzata*. In questo caso (la casella **Installazione personalizzata** è selezionata), è possibile modificare le impostazioni di installazione predefinite. È possibile selezionare i componenti dell'applicazione da installare e specificare la cartella di installazione dell'applicazione. Le impostazioni di protezione consigliate da Kaspersky Lab verranno specificate per ogni componente selezionato. Al termine dell'installazione, è possibile attivare l'installazione e configurare la protezione dall'accesso non autorizzato.

  La modalità di installazione personalizzata è consigliata solo per gli utenti esperti.

Se si seleziona la prima opzione l'installazione guidata consentirà all'utente di visualizzare il Contratto di licenza e l'Informativa sulla raccolta dei dati di Kaspersky Security Network. Successivamente l'applicazione verrà installata nel computer.

Se si seleziona la seconda opzione, verrà richiesto di immettere o confermare determinate informazioni in ciascun passaggio dell'installazione.

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

PASSAGGIO 3. ACCETTAZIONE DEL CONTRATTO DI LICENZA

Prima di installare l'applicazione, viene offerta la possibilità di visualizzare il Contratto di licenza con l'utente finale di Kaspersky Lab. Il Contratto di licenza elenca i diritti dell'utente di utilizzare il software acquistato. Se non si accettano le condizioni del Contratto di licenza, non è possibile procedere con l'installazione dell'applicazione.

Leggere attentamente il contratto e, se si accettano le condizioni, fare clic sul pulsante **Accetto**. L'installazione dell'applicazione procede.

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

PASSAGGIO 4. PARTECIPAZIONE AL PROGRAMMA KASPERSKY SECURITY NETWORK

È possibile partecipare al programma Kaspersky Security Network. Lo scopo del programma è rivelare le nuove minacce per la protezione dei dati e migliorare la qualità dei prodotti Kaspersky Lab. A tale scopo, l'utente può fornire a Kaspersky Lab il diritto di utilizzare le informazioni sullo stato della protezione dei propri computer e sulle minacce rilevate. Per l'esecuzione dell'analisi, è inoltre possibile inviare informazioni sul sistema operativo e sull'identificatore univoco assegnato al computer da Kaspersky PURE.

Kaspersky Lab garantisce che non verrà utilizzato alcun dato personale.

Consultare le norme relative alla partecipazione al programma Kaspersky Security Network. Se si accettano tutte le condizioni, selezionare la casella ☑ **Accetto le condizioni di adesione al programma Kaspersky Security Network**.

Fare clic sul pulsante **Avanti**. L'installazione continua.

PASSAGGIO 5. SELEZIONE DELLA CARTELLA DI DESTINAZIONE

Questo passaggio è disponibile se è selezionata la selezione personalizzata di Kaspersky PURE (vedere pagina 23).

Durante questo passaggio, è possibile selezionare la cartella di destinazione in cui verrà installato Kaspersky PURE. Il percorso predefinito per l'installazione dell'applicazione è il seguente:

- **<unità> \ Programmi \ Kaspersky Lab \ Kaspersky PURE** – per i sistemi a 32 bit;
- **<unità> \ Programmi (x86) \ Kaspersky Lab \ Kaspersky PURE** – per i sistemi a 64 bit.

Per cambiare la cartella di destinazione, fare clic sul pulsante **Sfoglia** e specificare una cartella differente nella finestra visualizzata. È anche possibile specificare un nuovo percorso di installazione nel campo **Cartella di destinazione**.

Tenere presente che, se si immette manualmente il percorso completo della cartella di installazione, tale percorso non deve contenere più di 200 caratteri né includere caratteri speciali.

Fare clic sul pulsante **Avanti**. L'installazione continua.

PASSAGGIO 6. SELEZIONE DEI COMPONENTI DELL'APPLICAZIONE PER L'INSTALLAZIONE

Questo passaggio è disponibile se è selezionata la selezione personalizzata di Kaspersky PURE (vedere pagina 23).

Durante questo passaggio, è possibile selezionare i componenti dell'applicazione da installare nel computer. Per impostazione predefinita, sono selezionati tutti i componenti di protezione e il kernel del programma.

Per decidere se installare o meno un componente, è possibile visualizzare una breve descrizione del componente selezionato nella parte inferiore della finestra e determinare lo spazio libero su disco necessario per l'installazione del componente.

Per selezionare un componente per l'installazione, aprire il menu di scelta rapida facendo clic sull'icona accanto al nome del componente e selezionare la voce **La funzionalità specificata sarà installata sull'unità disco fisso locale**.

Per ottenere informazioni dettagliate sullo spazio libero su disco nel computer, fare clic sul pulsante **Volume**. Le informazioni verranno mostrate nella finestra visualizzata.

Per annullare l'installazione di un componente, selezionare l'opzione **La funzionalità specificata diventerà non disponibile** dal menu di scelta rapida. Se si annulla l'installazione di un componente, il computer non sarà protetto nei confronti di una serie di programmi che espongono il computer al rischio di infezione.

Dopo aver selezionato i componenti da installare, fare clic sul pulsante **Avanti**. Per tornare all'elenco predefinito di componenti da installare, fare clic sul pulsante **Reimposta**.

PASSAGGIO 7. RICERCA DI ALTRE APPLICAZIONI ANTI-VIRUS

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

Se nel computer sono state rilevate altre applicazioni anti-virus, queste verranno elencate sullo schermo. Verrà chiesto di disinstallarle prima di procedere all'installazione.

Per rimuovere i programmi anti-virus rilevati, utilizzare il pulsante **Rimuovi**.

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

PASSAGGIO 8. DISABILITAZIONE DEL FIREWALL DI MICROSOFT WINDOWS

Questo passaggio viene eseguito solo se Protezione del computer viene installato in un computer con Microsoft Windows Firewall abilitato e Firewall è uno dei componenti dell'applicazione che si desidera installare.

Durante questo passaggio dell'installazione di Kaspersky PURE, viene offerta la possibilità di disabilitare il firewall integrato in Microsoft Windows. Il modulo Protezione del computer include il componente Firewall, che assicura una protezione completa delle attività di rete. Di conseguenza, non è necessario utilizzare l'ulteriore protezione offerta dal sistema operativo.

Se si desidera utilizzare Firewall come strumento di protezione principale per le attività di rete, fare clic sul pulsante **Avanti**. Il firewall di Microsoft Windows verrà disabilitato automaticamente.

Se si desidera proteggere il computer con Microsoft Windows Firewall, selezionare l'opzione **Mantieni attivo il Firewall di Microsoft Windows**. In questo caso, il componente Firewall verrà installato e disabilitato per evitare conflitti nel funzionamento dell'applicazione.

PASSAGGIO 9. PREPARAZIONE FINALE PER L'INSTALLAZIONE

Questo passaggio completa la preparazione per l'installazione di Kaspersky Protezione del computer nel computer.

Durante l'installazione iniziale e personalizzata (vedere pagina 23) dell'applicazione, si consiglia di non deselezionare la casella **Proteggi il processo di installazione**. In caso di errori durante l'installazione, l'abilitazione della protezione consentirà di eseguire una procedura corretta di rollback dell'installazione. Quando si ripete l'installazione, si consiglia di deselezionare la casella.

Se l'applicazione viene installata in remoto utilizzando *Desktop remoto di Windows*, si consiglia di deselezionare la casella **Proteggi il processo di installazione**. Se si seleziona la casella, la procedura di installazione potrebbe essere eseguita in modo non corretto o non essere completata.

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

Durante l'installazione dei componenti di Kaspersky PURE, che rilevano il traffico di rete, le connessioni di rete correnti vengono interrotte. La maggior parte delle connessioni terminate sarà ripristinata dopo un breve intervallo di tempo.

La Configurazione guidata di Kaspersky PURE verrà avviata automaticamente al termine dell'installazione.

MODIFICA, RIPRISTINO E RIMOZIONE DELL'APPLICAZIONE TRAMITE L'INSTALLAZIONE GUIDATA

Il ripristino dell'applicazione può essere utile se si sono verificati errori durante l'esecuzione a causa di configurazioni errate o file danneggiati.

Modificando il set di componenti è possibile installare nuovi componenti di Kaspersky PURE o rimuovere quelli che ostacolano il proprio lavoro o che si ritengono superflui.

- *Per avviare il ripristino dello stato originale dell'applicazione, installare componenti di Kaspersky PURE non installati in precedenza o rimuovere l'applicazione:*

  1. Inserire il CD di installazione nell'unità CD/DVD-ROM se è già stato utilizzato per installare l'applicazione. Se si installa Kaspersky PURE da un'origine differente (una cartella condivisa, una cartella sul disco rigido e così via), verificare che il pacchetto di installazione sia disponibile in tale origine e accessibile.

  2. Selezionare **Start** → **Programmi** → **Protezione del computer** → **Modifica, Ripara o Rimuovi**.

Verrà avviato il programma di installazione, che opera come una procedura guidata. Di seguito è descritta in dettaglio la procedura per il ripristino dell'applicazione, la modifica del set di componenti o la rimozione dell'applicazione.

IN QUESTA SEZIONE:

Passaggio 1. Avvio del programma di installazione 27

Passaggio 2. Selezione dell'operazione 27

Passaggio 3. Completamento della modifica, del ripristino o della rimozione dell'applicazione 28

PASSAGGIO 1. AVVIO DEL PROGRAMMA DI INSTALLAZIONE

Se sono state eseguite tutte le azioni precedenti per il ripristino dell'applicazione o la modifica del set di componenti, verrà visualizzata la finestra iniziale del programma di installazione di Kaspersky PURE. Per procedere all'installazione, fare clic sul pulsante **Avanti**.

PASSAGGIO 2. SELEZIONE DELL'OPERAZIONE

Durante questo passaggio, è necessario selezionare l'azione da eseguire sull'applicazione: è possibile modificare il set di componenti dell'applicazione, ripristinare lo stato originale dei componenti installati o rimuovere alcuni componenti o l'intera applicazione. Per eseguire l'azione desiderata, fare clic sul pulsante corrispondente. I passaggi successivi del programma di installazione dipendono dall'operazione selezionata.

La modifica del set di componenti viene eseguita in modo simile all'installazione personalizzata dell'applicazione: è possibile specificare i componenti da installare e selezionare quelli da escludere.

Il ripristino dell'applicazione viene eseguito in base al set di componenti installati. L'applicazione aggiornerà i file di tutti i componenti installati e per ognuno di essi verrà impostato il livello di protezione **Consigliato**.

Durante la rimozione dell'applicazione è possibile selezionare i dati creati e utilizzati dall'applicazione che si desidera salvare sul computer. Per eliminare tutti i dati di Kaspersky PURE, selezionare l'opzione **Disinstallazione completa**. Per salvare i dati, selezionare l'opzione **Salva i dati dell'applicazione** e specificare i dati da mantenere inalterati:

- *Mantieni i dati di attivazione* – il file di chiave necessario per l'esecuzione dell'applicazione.
- *Database Anti-Spam* – il database utilizzato per il riconoscimento dei messaggi e-mail indesiderati. Questo database contiene informazioni dettagliate utilizzate per distinguere lo spam dai messaggi utili.
- *Mantieni i file di backup e quarantena*. Gli oggetti di backup sono copie di backup degli oggetti eliminati o disinfettati dall'utente. È consigliabile salvare tali oggetti in modo da poterli ripristinare in futuro. Gli oggetti in quarantena sono oggetti che potrebbero essere stati infettati da virus o dalle relative varianti. Tali oggetti contengono codice simile a quello di un virus noto, tuttavia non è possibile stabilirne inequivocabilmente la pericolosità. È consigliabile salvare tali oggetti perché potrebbero rivelarsi non infetti o perché potrebbe essere possibile eseguirne la disinfezione dopo l'aggiornamento dei database dell'applicazione.
- *Mantieni le impostazioni di protezione* – valori impostati per i parametri di tutti i componenti dell'applicazione.
- *Mantieni i dati di iSwift e iChecker* – database che contiene informazioni sugli oggetti NTFS sottoposti a scansione. Consente di velocizzare la scansione degli oggetti. Utilizzando i dati di questo database, Kaspersky PURE esamina solo gli oggetti modificati dall'ultima scansione.
- *Mantieni i dati della cartella condivisa della Modalità Protetta* – dati accessibili sia in Modalità Protetta che nella modalità di esecuzione normale.

Se è trascorso un periodo di tempo considerevole tra la rimozione di una versione precedente di Protezione del computer e l'installazione di una versione più recente, è consigliabile evitare di utilizzare il database di iSwift e iChecker salvato dall'installazione precedente dell'applicazione. Durante tale periodo di tempo, un programma dannoso potrebbe essere penetrato nel computer e avere eseguito azioni che non è possibile rilevare con questo database, causando in definitiva l'infezione del computer.

Per avviare l'operazione selezionata, fare clic sul pulsante **Avanti**. Verrà avviato il processo di copia dei file nel computer o di rimozione dei componenti e dei dati selezionati.

PASSAGGIO 3. COMPLETAMENTO DELLA MODIFICA, DEL RIPRISTINO O DELLA RIMOZIONE DELL'APPLICAZIONE

Lo stato di avanzamento del processo di ripristino, modifica o rimozione viene visualizzato sullo schermo e al termine ne viene segnalato il completamento.

In genere, la rimozione richiede il riavvio del computer per l'applicazione delle modifiche al sistema. Viene richiesto se si desidera riavviare il computer. Per riavviare immediatamente il computer, fare clic sul pulsante **Sì**. Per riavviare il computer manualmente in un secondo momento, fare clic sul pulsante **No**.

OPERAZIONI PRELIMINARI

Uno dei principali obiettivi di Kaspersky Lab nella creazione di Kaspersky PURE era assicurare una protezione completa dei computer all'interno di una rete domestica. La configurazione ottimale di tutte le impostazioni delle applicazioni consente agli utenti con qualsiasi livello di esperienza di avere la certezza della protezione del proprio computer non appena completata l'installazione del software.

Per assicurare agli utenti la massima praticità, le fasi iniziali di configurazione sono combinate nell'interfaccia della Configurazione guidata dell'applicazione (vedere la sezione "Configurazione guidata dell'applicazione" a pagina 30), avviata al termine dell'installazione. Seguendo le istruzioni della procedura guidata, è possibile attivare Kaspersky PURE, configurare le impostazioni di aggiornamento, limitare l'accesso all'applicazione tramite una password e modificare altre impostazioni.

Il computer potrebbe risultare infettato da malware prima dell'installazione di Kaspersky PURE. Per rilevare il malware sul computer, eseguire la scansione completa del computer (vedere la sezione "Scansione anti-virus del computer" a pagina 35).

A causa dell'azione del malware e di errori del sistema, le impostazioni del computer potrebbero essere danneggiate. Eseguire l'attività di scansione delle vulnerabilità (vedere la sezione "Ricerca delle vulnerabilità del computer" a pagina 35) per individuare le vulnerabilità del software installato e le anomalie delle impostazioni di sistema.

Al momento dell'installazione dell'applicazione i database inclusi nel pacchetto di installazione potrebbero inoltre diventare obsoleti. Avviare l'aggiornamento dell'applicazione (vedere pagina 35), a meno che tale operazione non sia stata già eseguita utilizzando l'Installazione guidata o automaticamente subito dopo l'installazione dell'applicazione.

Il componente Anti-Spam incluso nel pacchetto di Protezione del computer utilizza un algoritmo di autoaddestramento per rilevare i messaggi indesiderati. Eseguire l'Addestramento guidato di Anti-Spam (vedere la sezione "Addestramento con Addestramento guidato" a pagina 110) per configurare il componente per la gestione della posta.

Per ripristinare velocemente le informazioni in caso di perdite di dati, configurare l'attività di backup (vedere la sezione "Backup" a pagina 40).

Per proteggere le informazioni riservate dagli accessi non autorizzati, creare contenitori crittografati per l'archiviazione dei dati (vedere la sezione "Crittografia dei dati" a pagina 40).

Per proteggere bambini e adolescenti dalle potenziali minacce legate all'utilizzo del computer, specificare le restrizioni di Parental Control (vedere la sezione "Parental Control" a pagina 40).

Al termine di queste operazioni, Kaspersky PURE sarà pronto per l'esecuzione. Per valutare il livello di protezione del computer, utilizzare la procedura guidata per la gestione della protezione.

IN QUESTA SEZIONE:

Configurazione guidata dell'applicazione 30

Selezione del tipo di rete 34

Aggiornamento dell'applicazione 35

Scansione anti-virus del computer 35

Ricerca delle vulnerabilità del computer 35

Gestione della licenza 36

Partecipazione a Kaspersky Security Network 36

Gestione della protezione 37

Stato della protezione 39

Sospensione della protezione 39

Backup 40

Parental Control 40

Crittografia dei dati 40

Gestione delle password 41

CONFIGURAZIONE GUIDATA DELL'APPLICAZIONE

La Configurazione guidata dell'applicazione viene avviata al termine dell'installazione. Questa procedura guidata è progettata per aiutare l'utente a configurare le impostazioni iniziali di Kaspersky PURE, in base alle funzionalità e attività del computer.

L'interfaccia della Configurazione guidata dell'applicazione è costituita da una serie di passaggi in finestre tra le quali è possibile spostarsi grazie ai pulsanti **Indietro** e **Avanti** e che possono essere chiuse utilizzando il pulsante **Annulla**.

I PASSAGGI DELLA PROCEDURA GUIDATA SONO DESCRITTI DI SEGUITO

Passaggio 1. Attivazione dell'applicazione 31

Passaggio 2. Limitazione dell'accesso all'applicazione 32

Passaggio 3. Selezione della modalità di protezione 33

Passaggio 4. Configurazione dell'aggiornamento dell'applicazione 33

Passaggio 5. Selezione delle minacce da rilevare 34

Passaggio 6. Analisi delle applicazioni installate nel computer 34

Passaggio 7. Chiusura della Configurazione guidata 34

PASSAGGIO 1. ATTIVAZIONE DELL'APPLICAZIONE

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

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

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

Per attivare l'applicazione occorre una connessione a Internet.

Per ottenere un file chiave durante l'attivazione, è necessario disporre di un codice di attivazione. Il codice di attivazione viene fornito al momento dell'acquisto dell'applicazione. L'attivazione di Kaspersky PURE prevede le opzioni seguenti:

- **Attivare la versione commerciale**. Selezionare questa opzione se è stata acquistata una versione in commercio dell'applicazione ed è stato ottenuto un codice di attivazione. È possibile utilizzare questo codice per ottenere un file chiave che consente di accedere a tutte le funzionalità dell'applicazione per il periodo di validità della licenza.
- **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 in commercio. Verrà fornito un file chiave gratuito valido per un periodo specificato nel contratto di licenza della versione di prova.
- **Attivare successivamente**. Se si seleziona questa opzione, la fase di attivazione di Kaspersky PURE verrà saltata. L'applicazione verrà installata nel computer, ma non sarà possibile utilizzare determinate funzionalità, come ad esempio l'aggiornamento (sarà possibile aggiornare l'applicazione solo una volta dopo l'installazione), la creazione di contenitori crittografati, strumenti aggiuntivi e così via. L'opzione **Attivare successivamente** è disponibile solo al primo avvio dell'Attivazione guidata, in seguito all'installazione dell'applicazione.

Se Kaspersky PURE è stato installato e quindi rimosso con le informazioni sull'attivazione salvate, questo passaggio verrà ignorato. In questo caso, la Configurazione guidata riceverà automaticamente le informazioni sulla licenza esistente che verranno visualizzate nella finestra della procedura guidata.

VEDERE ANCHE:

Attivazione della versione commerciale:.....31

Attivazione della versione di prova 32

Completamento dell'attivazione.....32

ATTIVAZIONE DELLA VERSIONE COMMERCIALE:

Se si seleziona questa opzione, l'applicazione viene attivata da un server Kaspersky Lab che richiede una connessione Internet.

L'attivazione viene eseguita immettendo un codice di attivazione ricevuto tramite e-mail al momento dell'acquisto di Kaspersky PURE via Internet. Se è stata acquistata la versione in scatola dell'applicazione, il codice di attivazione è stampato all'interno della busta che contiene il CD o sotto l'adesivo di protezione all'interno della custodia del DVD.

Il codice di attivazione è una sequenza di cifre separate da trattini in quattro gruppi da cinque caratteri ciascuno, senza spazi ad esempio 11111-11111-11111-11111. Si noti che il codice deve essere inserito in caratteri dell'alfabeto latino.

L'Attivazione guidata stabilisce la connessione tramite Internet a un server di attivazione di Kaspersky Lab e invia a quest'ultimo il codice di attivazione che viene successivamente verificato. Se il codice di attivazione viene accettato, si riceve un file chiave della licenza che verrà quindi installato automaticamente. Al termine del processo di attivazione viene visualizzata una finestra contenente informazioni dettagliate sulla licenza acquistata.

Se il codice di attivazione non viene accettato, viene visualizzato il messaggio corrispondente. In questo caso, contattare il fornitore da cui è stato acquistato Kaspersky PURE.

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

Se si verificano errori durante la connessione a un server di attivazione e non è possibile ottenere un file chiave, contattare l'Assistenza tecnica.

ATTIVAZIONE DELLA VERSIONE DI PROVA

Utilizzare questa opzione di attivazione se si desidera installare una versione di prova di Kaspersky PURE prima di procedere all'acquisto di una versione commerciale. Verrà fornito un file chiave gratuito valido per un periodo specificato nel contratto di licenza della versione di prova. Una volta scaduta, la licenza di prova non può essere riattivata.

Se si verificano errori durante la connessione a un server di attivazione e non è possibile ottenere un file chiave, contattare l'Assistenza tecnica.

COMPLETAMENTO DELL'ATTIVAZIONE

L'Attivazione guidata informa l'utente che Kaspersky PURE è stato attivato correttamente. Vengono inoltre fornite informazioni sulla licenza, ovvero il tipo (commerciale, di prova), la data di scadenza e il numero di host della licenza.

PASSAGGIO 2. LIMITAZIONE DELL'ACCESSO ALL'APPLICAZIONE

Lo scopo della limitazione dell'accesso è impedire i tentativi non autorizzati di disattivare la protezione o modificare le impostazioni dei componenti integrati in Kaspersky PURE.

La limitazione dell'accesso a Kaspersky PURE tramite una password può essere utile nei seguenti casi:

- se un personal computer viene utilizzato da più persone, con differenti livelli di esperienza in ambito informatico;
- se Kaspersky PURE assicura la protezione di diversi computer di una rete domestica;
- se vi è il rischio che la protezione sia disattivata dal malware.

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

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

- **Configurazione delle impostazioni dell'applicazione** - la password verrà richiesta per salvare le modifiche alle impostazioni di Kaspersky PURE.
- **Gestione backup** – la password verrà richiesta prima di eseguire le attività di backup.
- **Gestione Parental Control** – la password verrà richiesta prima di eseguire le attività di Parental Control.
- **Gestione Centro di controllo** – la password verrà richiesta prima di modificare le impostazioni di Kaspersky PURE tramite la rete.
- **Terminazione dell'applicazione** - la password verrà richiesta quando l'utente tenta di chiudere l'applicazione.

PASSAGGIO 3. SELEZIONE DELLA MODALITA DI PROTEZIONE

Questo passaggio della Configurazione guidata dell'applicazione verrà ignorato se è stata selezionata la modalità di installazione rapida. Alle impostazioni dell'applicazione modificate in questo passaggio vengono assegnati valori predefiniti.

Selezionare la modalità di protezione fornita da Kaspersky PURE.

Sono disponibili due modalità:

- *Automatica*. In caso di eventi importanti, Kaspersky PURE eseguirà automaticamente l'azione consigliata dagli esperti di Kaspersky Lab. Una volta rilevata una minaccia, l'applicazione cerca di disinfettare l'oggetto e, se il tentativo non riesce, procede alla relativa eliminazione. Gli oggetti sospetti verranno ignorati senza essere elaborati. L'utente viene informato di nuovi eventi mediante messaggi a comparsa.

- *Interattiva*. In questa modalità, l'applicazione reagisce agli eventi nella maniera specificata. Quando si verifica un evento che richiede attenzione da parte dell'utente, l'applicazione visualizza notifiche che consentono la selezione di un'azione.

Le notifiche sul rilevamento di un'infezione attiva verranno visualizzate a prescindere dalla modalità di protezione selezionata.

PASSAGGIO 4. CONFIGURAZIONE DELL'AGGIORNAMENTO DELL'APPLICAZIONE

Questo passaggio della Configurazione guidata dell'applicazione verrà ignorato se è stata selezionata la modalità di installazione rapida. Alle impostazioni dell'applicazione modificate in questo passaggio vengono assegnati valori predefiniti.

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

- **Aggiornamenti automatici**. L'applicazione controlla la disponibilità di pacchetti di aggiornamento nella sorgente degli aggiornamenti a intervalli specificati. La frequenza della scansione può essere aumentata durante le epidemie e ridotta nei periodi più tranquilli. I nuovi aggiornamenti rilevati vengono scaricati e installati nel computer. Questa è la modalità predefinita.

- **Aggiornamenti pianificati** (l'intervallo di tempo può cambiare in base alle impostazioni dell'aggiornamento). Gli aggiornamenti vengono eseguiti automaticamente in base alla pianificazione. Le proprietà di pianificazione possono essere modificate nella finestra visualizzata facendo clic sul pulsante **Impostazioni**.

- **Aggiornamenti manuali**. Se si seleziona questa opzione, gli aggiornamenti verranno eseguiti manualmente.

Si noti che i database ed i moduli dell'applicazione in dotazione con il pacchetto di installazione potrebbero essere obsoleti al momento dell'installazione di Kaspersky PURE. È pertanto consigliabile scaricare gli aggiornamenti più recenti dell'applicazione. A tal fine, fare clic su **Aggiorna ora**. Gli aggiornamenti necessari verranno scaricati dai server degli aggiornamenti e installati nel computer.

Se i database inclusi nel pacchetto di installazione sono obsoleti, le dimensioni del pacchetto di aggiornamento possono essere piuttosto grandi e aumentare ulteriormente il traffico in Internet (fino a diverse decine di MB).

Se si desidera passare alla modifica delle impostazioni di aggiornamento (selezionare la risorsa da cui verranno scaricati gli aggiornamenti o l'account utente utilizzato per eseguire il processo di aggiornamento e così via), fare clic sul pulsante **Impostazioni**.

PASSAGGIO 5. SELEZIONE DELLE MINACCE DA RILEVARE

Questo passaggio della Configurazione guidata dell'applicazione verrà ignorato se è stata selezionata la modalità di installazione rapida. Alle impostazioni dell'applicazione modificate in questo passaggio vengono assegnati valori predefiniti.

In questo passaggio è possibile selezionare le categorie di minacce da rilevare mediante Protezione del computer. Protezione del computer rileva sempre i programmi in grado di danneggiare il computer, inclusi virus, worm e Trojan.

PASSAGGIO 6. ANALISI DELLE APPLICAZIONI INSTALLATE NEL COMPUTER

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.

Altre applicazioni sono analizzate al primo avvio dopo l'installazione di Kaspersky PURE.

PASSAGGIO 7. CHIUSURA DELLA CONFIGURAZIONE GUIDATA

L'ultima finestra della procedura guidata informa l'utente del completamento dell'installazione dell'applicazione. Per eseguire Kaspersky PURE, verificare che la casella **Esegui Kaspersky PURE** sia selezionata, quindi fare clic sul pulsante **Fine**.

SELEZIONE DEL TIPO DI RETE

Una volta installato Kaspersky PURE, il componente Firewall analizza le connessioni di rete attive del computer. A ciascuna connessione di rete viene assegnato uno stato che determina le attività di rete consentite.

Se è stata selezionata la modalità interattiva di funzionamento di Kaspersky PURE (vedere la sezione "Passaggio 3. Selezione della modalità di protezione" a pagina 33), viene visualizzata una notifica ogni volta che viene rilevata una nuova connessione di rete. È possibile selezionare lo stato della nuova rete nella finestra di notifica:

- **Rete pubblica**. Alle connessioni di rete con questo stato viene negato l'accesso al computer dall'esterno. In questo tipo di rete viene negato l'accesso alle stampanti e alle cartelle pubbliche. Si consiglia di assegnare questo stato alle connessioni alla rete Internet.

- **Rete locale**. Alle connessioni di rete con questo stato è consentito l'accesso a cartelle pubbliche e stampanti di rete. Si consiglia di assegnare questo stato alle reti locali protette, ad esempio a una rete aziendale.

- **Rete attendibile**. Le connessioni di rete con questo stato non presentano restrizioni. Si consiglia di assegnare questo stato solo ad aree assolutamente protette.

Per ogni stato di rete, Kaspersky PURE utilizza un gruppo associato di regole per la gestione dell'attività di rete. Se necessario, in una fase successiva è possibile modificare lo stato di rete di una connessione impostandone uno diverso da quello specificato inizialmente.

AGGIORNAMENTO DELL'APPLICAZIONE

Per aggiornare Kaspersky PURE, è necessario disporre di una connessione a Internet.

L'attività di protezione di Kaspersky PURE si basa sui database dell'applicazione che contengono firme delle minacce, frasi tipiche dello spam e descrizioni di attacchi di rete. Tali database potrebbero essere già obsoleti al momento dell'installazione di Kaspersky PURE in quanto insieme ai moduli dell'applicazione essi vengono aggiornati regolarmente.

Quando la configurazione guidata dell'applicazione è attiva, è possibile selezionare la modalità di avvio dell'aggiornamento (vedere la sezione "Passaggio 4. Configurazione dell'aggiornamento dell'applicazione" a pagina 33). Per impostazione predefinita, Kaspersky PURE 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 automaticamente.

Se i database inclusi nel pacchetto di installazione sono obsoleti, le dimensioni del pacchetto di aggiornamento possono essere piuttosto grandi e aumentare ulteriormente il traffico in Internet (fino a diverse decine di MB).

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

➡ *Per aggiornare manualmente Kaspersky PURE, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella parte sinistra della finestra visualizzata, selezionare la sezione **Aggiornamenti**.
3. Fare clic sul pulsante **Avvia aggiornamento**.

SCANSIONE ANTI-VIRUS DEL COMPUTER

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

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

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

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

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella parte sinistra della finestra visualizzata, selezionare la sezione **Scansione**.
3. Fare clic sul pulsante **Avvia Scansione Completa** per avviare la scansione.

RICERCA DELLE VULNERABILITÀ DEL COMPUTER

Le impostazioni del sistema operativo possono danneggiarsi in seguito a errori del sistema o attività eseguite da programmi nocivi. Le applicazioni utente installate nel computer possono inoltre presentare vulnerabilità utilizzabili dagli intrusi allo scopo di danneggiare il computer.

Per rilevare ed eliminare tali problemi, è consigliabile avviare l'attività *Scansione Vulnerabilità* (vedere pagina 140) dopo aver installato l'applicazione. Durante l'esecuzione di tale attività vengono ricercate le vulnerabilità nelle applicazioni installate, nonché i danni e le anomalie nelle impostazioni del browser e del sistema operativo.

Per avviare l'attività Scansione Vulnerabilità:

1. Aprire la finestra principaledell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella parte sinistra della finestra visualizzata, selezionare la sezione **Scansione**.
3. Fare clic sul pulsante **Apri la finestra della Scansione Vulnerabilità**.
4. Nella finestra visualizzata, fare clic sul pulsante **Avvia Scansione Vulnerabilità**.

GESTIONE DELLA LICENZA

Per poter funzionare, Kaspersky PURE necessita di una chiave valida. Un file chiave viene fornito mediante il codice di attivazione ottenuto in fase di acquisto dell'applicazione e ne garantisce il diritto di utilizzo a partire dalla data di attivazione. Il file chiave contiene informazioni sulla licenza: il tipo, la data di scadenza e il numero di host.

A meno che non sia stata attivata una versione di prova, senza un file chiave Kaspersky PURE viene eseguito con funzionalità limitate. Ad esempio, dopo l'installazione sarà possibile scaricare un solo aggiornamento, ma non gli aggiornamenti successivi. Non saranno inoltre disponibili diverse altre funzioni, come ad esempio la creazione di contenitori crittografati.

Al termine del periodo di prova, non è più possibile utilizzare la versione di prova attivata.

Anche dopo la scadenza della licenza commerciale, l'applicazione passa in modalità con funzionalità limitate, in cui Ottimizzazione del sistema e numerose altre funzionalità non sono disponibili. Resta comunque possibile eseguire la scansione del computer per identificare la presenza di eventuali virus e utilizzare i componenti di protezione, ma solo attraverso i database aggiornati fino alla scadenza della licenza. Ciò significa che la protezione dai virus diffusi dopo la scadenza della licenza dell'applicazione non può essere garantita.

Per assicurare una protezione completa, è consigliabile dunque rinnovare la licenza di Kaspersky PURE. Due settimane prima della scadenza della licenza, l'applicazione invierà un messaggio di notifica che apparirà per un determinato periodo a ogni avvio dell'applicazione.

Informazioni sulla licenza correntemente in uso sono visualizzate nella finestra **Gestione delle licenze**: tipo (commerciale, commerciale con abbonamento, commerciale con abbonamento di protezione, di prova), numero massimo di host, data di scadenza e numero di giorni che precedono la scadenza. Le informazioni sulla scadenza della licenza non verranno visualizzate se è installata la licenza commerciale con abbonamento o licenza commerciale con abbonamento protezione.

Per visualizzare il contratto di licenza dell'applicazione, fare clic sul pulsante **Visualizza il Contratto di licenza con l'utente finale**. Per eliminare il file chiave, fare clic sul pulsante ✖ a destra della licenza di cui si desidera eliminare il file chiave. Per attivare una nuova licenza, fare clic sul pulsante **Attivare una nuova licenza**.

Grazie al pulsante **Acquista la licenza** (**Rinnova la licenza**), è possibile procedere con l'acquisto (rinnovo) della licenza nel negozio online di Kaspersky Lab.

Kaspersky Lab offre prezzi speciali per l'estensione della licenza dei prodotti. Per informazioni sulle offerte speciali, visitare il sito Web di Kaspersky Lab nella sezione **Prodotti & Servizi** → **Offerte speciali**.

PARTECIPAZIONE A KASPERSKY SECURITY NETWORK

In tutto il mondo appaiono quotidianamente numerose nuove minacce. Per facilitare la raccolta di statistiche sui nuovi tipi di minaccia e sulle relative origini, nonché sviluppare i metodi da utilizzare per eliminarle, Kaspersky Lab invita gli utenti a utilizzare il servizio Kaspersky Security Network.

L'utilizzo di Kaspersky Security Network implica l'invio delle seguenti informazioni a Kaspersky Lab:

- Un identificatore univoco assegnato al computer da Kaspersky PURE, che caratterizza le impostazioni hardware del computer e non contiene informazioni.
- Informazioni sulle minacce identificate dai componenti dell'applicazione. La struttura e il contenuto delle informazioni dipendono dal tipo di minaccia rilevata.
- Informazioni sul sistema operativo: versione del sistema operativo, service pack installati, servizi e driver scaricati, versioni del browser e del client di posta elettronica, estensioni del browser, numero di versione dell'applicazione Kaspersky Lab installata.

Kaspersky Security Network raccoglie inoltre statistiche estese, tra cui informazioni relative a:

- file eseguibili e applicazioni firmate scaricate sul computer;
- applicazioni in esecuzione sul computer.

Le informazioni statistiche vengono inviate una volta completato l'aggiornamento dell'applicazione.

Kaspersky Lab garantisce che Kaspersky Security Network non raccoglie né distribuisce i dati personali degli utenti.

Per configurare le impostazioni di invio delle statistiche:

1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Selezionare la sezione **Feedback** nella parte sinistra della finestra.
3. Selezionare la casella **Accetto di partecipare al programma Kaspersky Security Network** per confermare la partecipazione al programma.

GESTIONE DELLA PROTEZIONE

I problemi di protezione del computer vengono indicati dalle variazioni del colore dell'icona che indica lo stato di protezione del computer (vedere sezione "Protezione del computer" a pagina 45) e del pannello in cui si trova l'icona stessa. Se il sistema di protezione presenta problemi, si consiglia di risolverli immediatamente.

Figura 1. Stato attuale della protezione del computer

È possibile visualizzare l'elenco dei problemi che si sono verificati, la relativa descrizione e i metodi possibili per risolverli nella scheda **Stato** (vedere la figura seguente). Per selezionarla, fare clic sull'icona di stato o sul pannello in cui si trova (vedere la figura precedente).

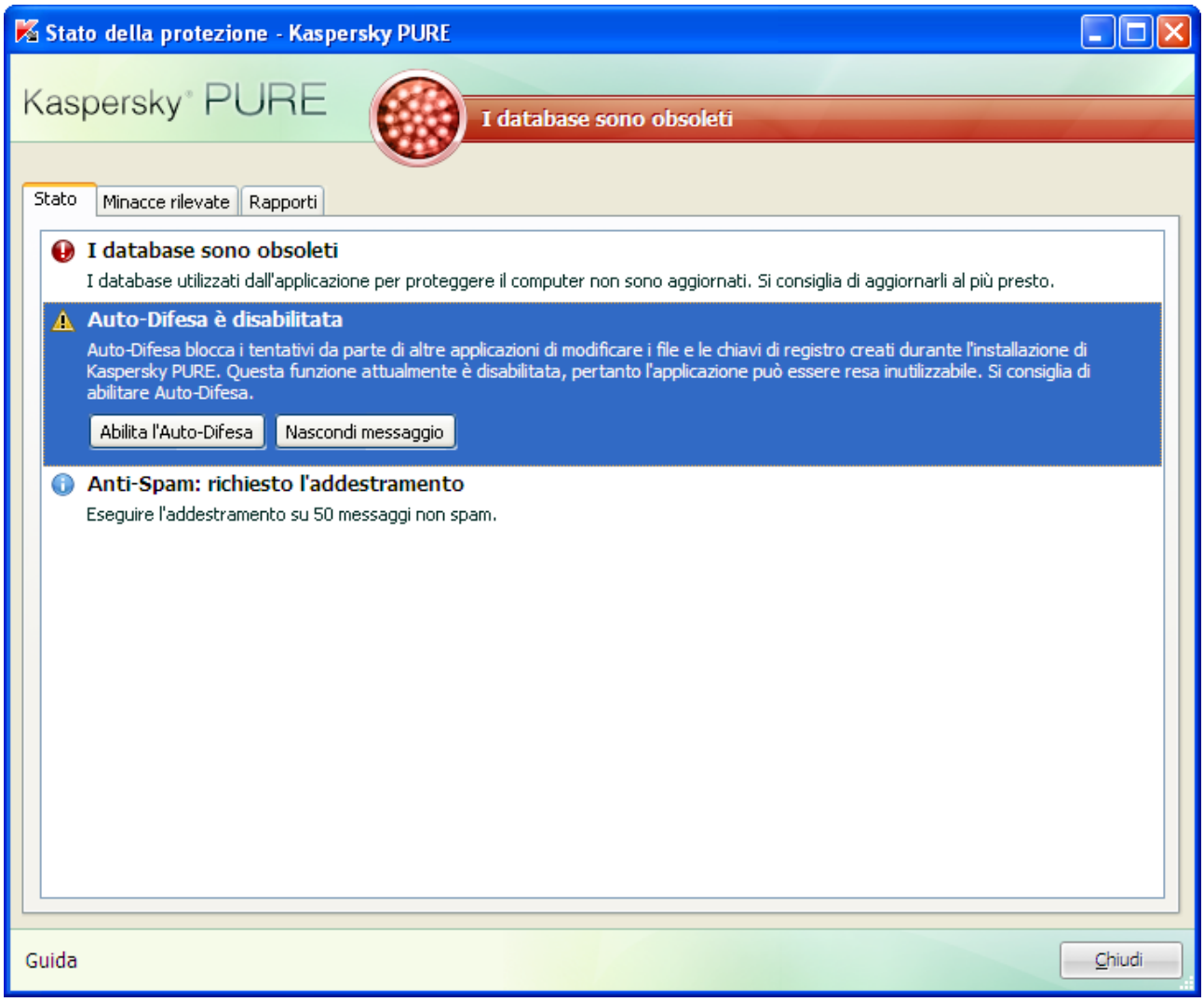


Figura 2. Risoluzione dei problemi di protezione

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

- *Eliminazione immediata*. Utilizzando i pulsanti corrispondenti, è possibile passare alla risoluzione del problema, ovvero l'azione consigliata.

- *Rimanda l'eliminazione*. Se non si riesce a eliminare il problema immediatamente, è possibile rimandare questa azione. A tale scopo, fare clic sul pulsante **Nascondi messaggio**.

  Si noti che questa opzione non è disponibile per i problemi più seri. Tali problemi comprendono ad esempio gli oggetti nocivi non disinfettati, il blocco di uno o più componenti o il danneggiamento dei file di programma.

Per visualizzare nuovamente i messaggi nascosti nell'elenco generale, selezionare la casella **Mostra messaggi nascosti**.

STATO DELLA PROTEZIONE

Le prestazioni dei componenti di Kaspersky PURE o delle attività di scansione anti-virus vengono registrate nella sezione contenente informazioni di riepilogo sullo stato di protezione del computer. Da qui è possibile controllare quanti oggetti pericolosi e sospetti sono stati rilevati dall'applicazione, quali sono stati disinfettati, eliminati o messi in quarantena.

Il rilevamento di un oggetto pericoloso da parte dell'applicazione viene notificato dallo stato di protezione del computer (vedere sezione "Protezione del computer" a pagina 45) attraverso la modifica del colore dell'icona di stato e del pannello in cui si trova. Se vengono rilevati oggetti pericolosi, il colore dell'icona e del pannello diventa rosso. In questo caso, è necessario eliminare immediatamente tutte le minacce.

- *Per visualizzare informazioni sullo stato di protezione del computer:*

  1. Aprire la finestra principale dell'applicazione e fareclic sul **Protezione del computer**.
  2. Nella finestra visualizzata fare clic sul collegamento **Rapporto**.

- *Per eliminare i problemi di protezione del computer:*

  1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
  2. Nella finestra visualizzata fare clic sul collegamento **Rapporto**.
  3. Nella finestra visualizzata, nella scheda **Stato**, eseguire le azioni richieste. Per visualizzare nuovamente i messaggi nascosti nell'elenco generale, selezionare la casella **Mostra messaggi nascosti**.

- *Per eseguire un'azione su un oggetto rilevato:*

  1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
  2. Nella finestra visualizzata fare clic sul collegamento **Rapporto**.
  3. Nella finestra visualizzata, scheda **Minacce rilevate**, selezionare l'oggetto desiderato nell'elenco di oggetti e fare clic su di esso con il pulsante destro del mouse per aprire il menu di scelta rapida.
  4. Selezionare l'azione richiesta nel menu di scelta rapida che viene visualizzata.

- *Per visualizzare il rapporto sul funzionamento del componente di protezione:*

  1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
  2. Nella finestra visualizzata fare clic sul collegamento **Rapporto**.
  3. 3. Nella finestra visualizzata selezionare la scheda **Rapporto**.

SOSPENSIONE DELLA PROTEZIONE

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

In seguito alla sospensione temporanea della protezione, tutti i componenti di protezione risulteranno sospesi, come indicato da:

icona dell'applicazione inattiva (in grigio) (vedere sezione "Icona dell'area di notifica" a pagina 42) nell'area di notifica della barra delle applicazioni;

· colore rosso dell'icona di stato e del pannello della finestra principale di Kaspersky PURE.

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

Per sospendere la protezione del computer:

1. Nel menu di scelta rapida (vedere sezione "Menu di scelta rapida" a pagina 42) dell'applicazione, selezionare **Sospendi la protezione**.

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

   - **Sospendi per <intervallo di tempo> –** la protezione verrà abilitata entro un intervallo di tempo specificato. Utilizzare il menu a discesa per selezionare il valore dell'intervallo di tempo.

   - **Sospendi fino al riavvio –** la protezione verrà abilitata dopo il riavvio dell'applicazione o dopo il riavvio del sistema (a condizione che Kaspersky PURE sia impostato per l'avvio automatico).

   - **Sospendi** – la protezione verrà abilitata solo dopo che sarà stata avviata manualmente. Per abilitare la protezione, selezionare **Riprendi la protezione** dal menu di scelta rapida dell'applicazione.

BACKUP

Il modo più comune per proteggere le informazioni importanti dalle perdite di dati è eseguirne regolarmente il backup. È consigliabile configurare attività di backup per il salvataggio periodico delle informazioni aggiornate.

Prima di iniziare, è necessario creare un archivio di backup (vedere la sezione "Creazione di un'area per l'archivio di backup" a pagina 179) nell'unità selezionata. In questo archivio verranno create le copie di backup dei file necessari. Una volta eseguita questa operazione, è possibile configurare le attività di backup (vedere la sezione "Creazione di un'attività di backup" a pagina 181) (scegliere i file per cui creare le attività di backup e configurare l'avvio automatico e altre condizioni per il backup).

PARENTAL CONTROL

Al termine dell'installazione di Kaspersky PURE, Parental Control è disattivato. Nessuna restrizione viene applicata per gli utenti. Per proteggere bambini e adolescenti dalle potenziali minacce legate all'utilizzo del computer e di Internet, è consigliabile configurare tempestivamente le impostazioni di Parental Control per tutti gli utenti.

Se non è stata attivata la protezione tramite password durante l'installazione dell'applicazione (vedere la sezione "Passaggio 2. Limitazione dell'accesso all'applicazione" a pagina 32), al primo avvio di Parental Control viene richiesto di impostare una password per la protezione delle impostazioni dalle modifiche non autorizzate. Una volta eseguita tale operazione, è possibile attivare Parental Control e configurare le restrizioni (vedere la sezione "Attivazione e configurazione di Parental Control" a pagina186) per l'utilizzo del computer e di Internet e per la messaggistica immediata per tutti gli account presenti nel computer.

CRITTOGRAFIA DEI DATI

Per proteggere le informazioni riservate dagli accessi non autorizzati, è consigliabile archiviarle in formato crittografato in uno speciale contenitore.

Prima di iniziare, è necessario creare un contenitore crittografato (vedere la sezione "Creazione del contenitore" a pagina 205), copiarvi i dati (vedere la sezione "Aggiunta di file nel contenitore" a pagina 207) come in una normale unità rimovibile e quindi disconnettere (vedere la sezione "Connessione e disconnessione del contenitore" a pagina 206) il contenitore. Sarà quindi necessario specificare una password per eseguire la connessione al contenitore e accedere ai dati.

GESTIONE DELLE PASSWORD

Gestione delle password protegge i dati personali dell'utente e ne facilita la gestione.

Una delle caratteristiche dell'applicazione è la configurazione ottimale dei parametri iniziali. Per comodità, le operazioni di configurazione iniziale sono comprese nella Configurazione guidata dell'applicazione (vedere pagina 212), che viene aperta al primo avvio dell'applicazione. Seguendo le istruzioni della procedura guidata, è possibile creare una password master e modificare le impostazioni per l'accesso all'applicazione e la protezione dei dati.

Per impedire l'accesso non autorizzato ai dati personali contenuti nel computer in assenza dell'utente, Gestione delle password blocca automaticamente il database delle password. Per utilizzare i dati personali, sbloccare Gestione delle password (vedere pagina 213).

Gestione delle password facilita l'utilizzo (vedere pagina 221) e la gestione dei dati personali. Per trovare le informazioni salvate, è possibile eseguire una ricerca tra le password (vedere pagina 222).

INTERFACCIA DELL'APPLICAZIONE

Kaspersky PURE presenta un'interfaccia di facile utilizzo. In questa sezione ne vengono descritte dettagliatamente le caratteristiche principali.

IN QUESTA SEZIONE:

Icona dell'area di notifica 42

Menu di scelta rapida 42

Finestra principale di Kaspersky PURE 44

Notifiche 48

Finestra delle impostazioni dell'applicazione 49

ICONA DELL'AREA DI NOTIFICA

Subito dopo aver installato Kaspersky PURE, la relativa icona verrà visualizzata nell'area di notifica della barra delle applicazioni di Microsoft Windows.

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

Se l'icona è attiva (colorata), la protezione è abilitata o alcuni dei rispettivi componenti sono in esecuzione. Se l'icona è inattiva (bianco e nero), tutti i componenti di protezione sono disabilitati.

L'icona di Kaspersky Pure cambia in funzione dell'operazione eseguita:

- – è in corso la scansione della posta elettronica;
- – è in corso la scansione del traffico Web;
- – è in corso l'aggiornamento dei database e dei moduli dell'applicazione;
- - per applicare gli aggiornamenti, è necessario riavviare il computer;
- – si è verificato un errore nel funzionamento di alcuni componenti dell'applicazione.

L'icona consente inoltre di accedere ai componenti di base dell'interfaccia dell'applicazione: menu di scelta rapida (vedere pagina 42) e la finestra principale (vedere pagina 44).

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

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

MENU DI SCELTA RAPIDA

Il menu di scelta rapida consente di eseguire le attività di protezione di base.

Il menu di Kaspersky PURE contiene i seguenti elementi:

- **Aggiornamenti**: avvia l'aggiornamento dei database e dei moduli dell'applicazione e installa gli aggiornamenti nel computer.
- **Scansione Completa:** avvia una scansione completa del computer per individuare eventuali oggetti malware. Durante l'operazione vengono esaminati gli oggetti di tutte le unità, inclusi i supporti rimovibili.
- **Scansione Anti-Virus:** seleziona gli oggetti e avvia la relativa scansione anti-virus. Per impostazione predefinita, l'elenco contiene diversi oggetti, tra i quali la cartella **Documenti** e le caselle di posta. È possibile ampliare l'elenco, selezionare altri oggetti per la scansione e avviare la scansione anti-virus.
- **Tastiera virtuale**: passa alla tastiera virtuale (vedere pagina 204).
- **Kaspersky PURE:** aprire la finestra principale dell'applicazione (vedere pagina 44)
- **Impostazioni**: visualizza e configura le impostazioni dell'applicazione.
- **Attivazione:** attiva Kaspersky PURE. Per ottenere lo stato di un utente registrato, è necessario attivare il programma. Questa voce di menu è disponibile solo se l'applicazione non è attivata.
- **Informazioni su:** visualizza una finestra con le informazioni sull'applicazione.
- **Sospendi la protezione / Riprendi la protezione:** disabilita o abilita temporaneamente i componenti di protezione in tempo reale. Questa voce di menu non ha effetto sull'esecuzione della scansione anti-virus o sugli aggiornamenti dell'applicazione.
- **Sospendi / Abilita Parental Control**: disabilita o abilita temporaneamente il controllo di tutti gli utenti. Questa voce di menu è disponibile solo se è installato il componente Parental Control.
- **Blocca il traffico di rete / Sblocca il traffico di rete:** blocca/sblocca temporaneamente tutte le connessioni di rete del computer.
- **Esci**: chiude Kaspersky PURE (quando viene selezionata questa opzione, l'applicazione viene scaricata dalla RAM del computer).

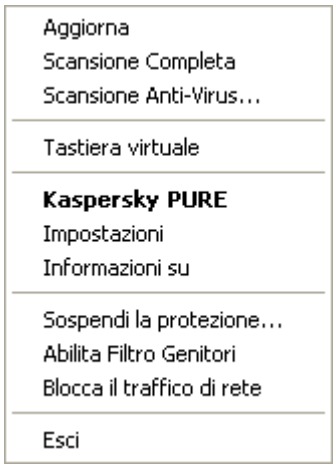


Figura 3. Menu di scelta rapida

Se è in corso un'attività di scansione anti-virus mentre si apre il menu di scelta rapida, quest'ultimo ne visualizza il nome e lo stato di avanzamento (percentuale completata). Selezionando l'attività, è possibile passare alla finestra principale contenente un rapporto sui risultati correnti della relativa esecuzione.

FINESTRA PRINCIPALE DI KASPERSKY PURE

Nella finestra principale sono disponibili le più importanti funzionalità dell'applicazione. La finestra principale può essere suddivisa in due parti.

Nella parte superiore della finestra è possibile accedere alle principali funzionalità dell'applicazione, riprendere o sospendere la protezione, eseguire una scansione anti-virus, avviare il backup dei dati e così via. I seguenti componenti di Kaspersky PURE sono disponibili nella parte superiore della finestra:

- ·**Protezione del computer** – protezione completa del computer da qualsiasi tipo di minaccia.
- ·**Backup** – creazione e archiviazione di copie di backup dei file, per assicurare il ripristino dei dati importanti in caso di perdite di dati.
- ·**Parental Control** – restrizione dell'accesso degli utenti alle risorse Web, alle applicazioni nel computer e alla messaggistica immediata.

Nella parte inferiore della finestra è possibile accedere a ulteriori funzionalità, che assicurano una protezione avanzata e ottimizzano il funzionamento del sistema. I seguenti componenti e servizi sono disponibili nella sezione **Protezione +** nella parte inferiore della finestra:

- **Ottimizzazione del sistema** – ottimizzazione del funzionamento del sistema ed esecuzione di specifiche attività per garantire la protezione del computer.
- ·**Tastiera virtuale** – prevenzione dell'intercettazione dei dati immessi tramite tastiera.
- ·**Crittografia dei dati** – prevenzione dell'accesso non autorizzato alle informazioni riservate.

- ·**Gestione delle password** – protezione di dati personali quali password, nomi utente, account di sistemi di messaggistica immediata, contatti e così via.

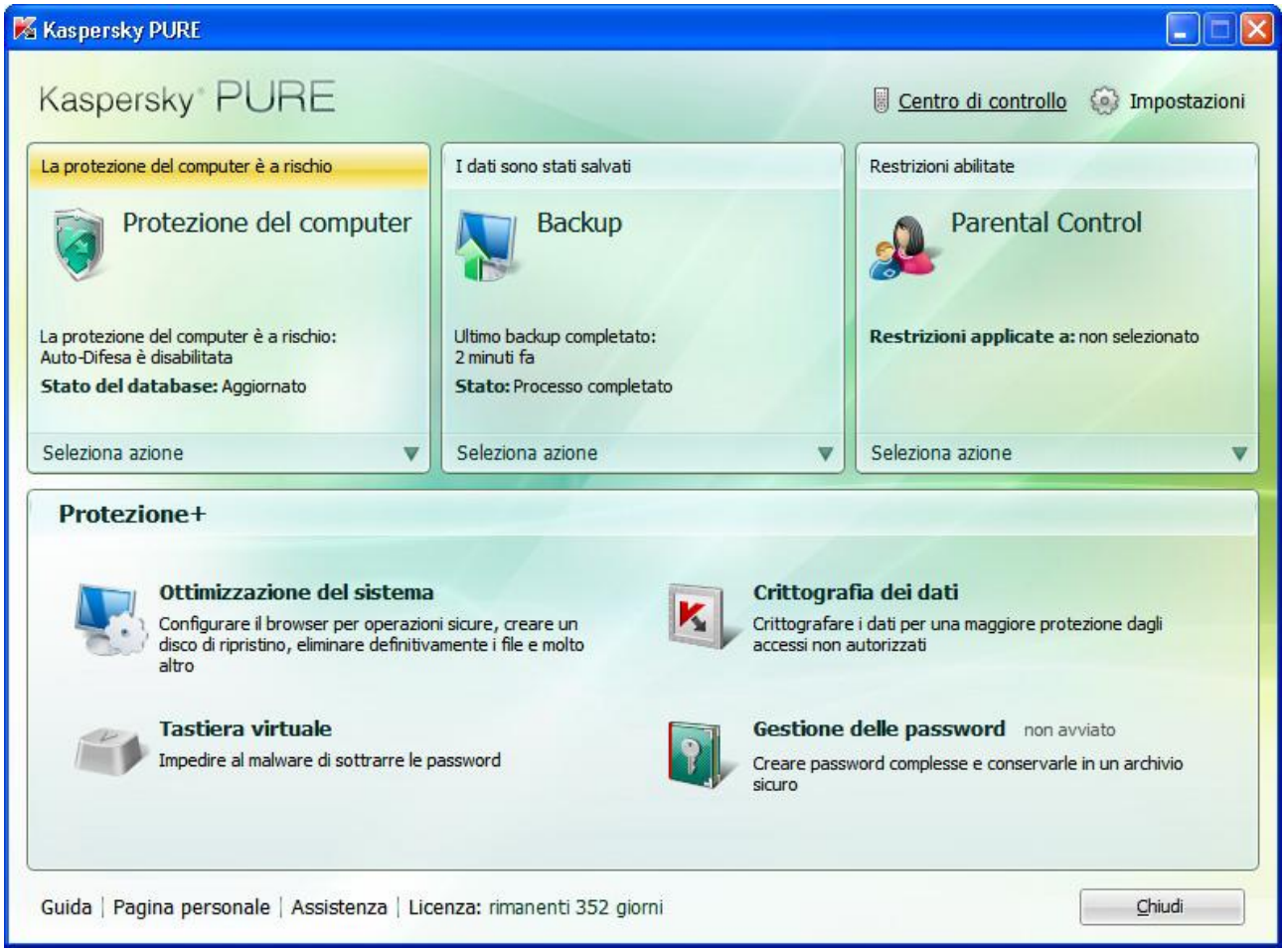


Figura 4. Finestra principale dell'applicazione

È inoltre possibile utilizzare i pulsanti e i collegamenti seguenti:

- **Centro di controllo** – amministrazione remota di Kaspersky PURE (vedere pagina 240).
- **Impostazioni** – configurazione delle impostazioni generali dell'applicazione (vedere pagina 49).
- **Guida** – visualizzazione della Guida di Kaspersky PURE.
- ·**Pagina personale** – consente di accedere alla pagina personale dell'utente (https://my.kaspersky.com/en/index.html?LANG=it) 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 del servizio di assistenza tecnica, forum).
- **Licenza** – contiene informazioni sull'attivazione e sul rinnovo della licenza di Kaspersky PURE.

È possibile modificare l'aspetto di Kaspersky PURE creando e utilizzando diversi schemi grafici e di colori.

PROTEZIONE DEL COMPUTER

La finestra principale di Protezione del computer può essere divisa in tre parti:

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

Figura 5. Stato attuale della protezione del computer

Esistono tre possibili valori per lo stato della protezione: ognuno di essi è indicato con un determinato colore, simili a quelli di un semaforo. Il verde indica che la protezione del computer è di livello adeguato, il giallo ed il rosso evidenziano la presenza di minacce alla protezione. Oltre ai programmi dannosi, le minacce comprendono il mancato aggiornamento dei database dell'applicazione obsoleti, la disabilitazione di componenti di protezione e la selezione di impostazioni di protezione minime.

Le minacce alla protezione devono essere eliminate non appena compaiono. Per informazioni dettagliate sulle minacce e su come neutralizzarle rapidamente, passare alla Gestione guidata della protezione: fare clic sull'icona di stato o sul pannello in cui si trova (vedere la figura sopra).

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

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

È inoltre possibile utilizzare i collegamenti seguenti:

- **Impostazioni**: consente di aprire la finestra delle impostazioni dell'applicazione.

- **Quarantena**: consente di lavorare con gli oggetti in quarantena.

- **Rapporto**: consente di passare all'elenco di eventi verificatisi durante il funzionamento dell'applicazione.

- **Guida**: consente di visualizzare la Guida di Kaspersky PURE.

BACKUP

La finestra principale del modulo Backup è formata da due parti:

- la parte sinistra della finestra consente di accedere alle principali funzionalità dell'applicazione, ovvero la gestione di attività di backup e archivi di copie di backup e il ripristino dei dati;

- la parte destra della finestra contiene un elenco di impostazioni relative alla funzionalità selezionata nella parte sinistra della finestra.

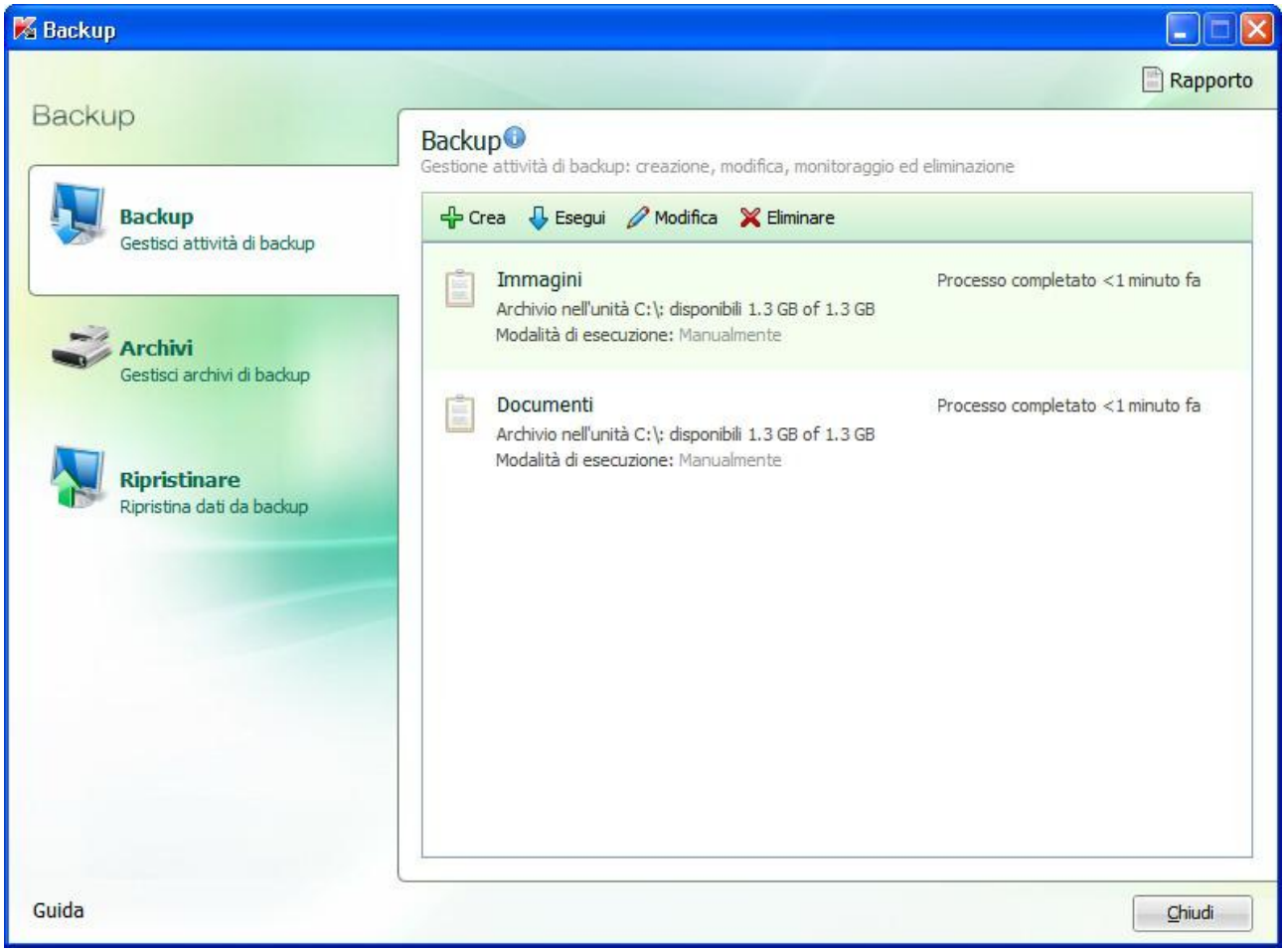


Figura 6. Finestra principale del modulo Backup

PARENTAL CONTROL

La finestra principale del modulo Parental Control è formata da due parti:

- la parte sinistra della finestra consente di accedere alle principali funzionalità dell'applicazione, ovvero la configurazione del controllo degli utenti e la visualizzazione dei rapporti;

- la parte destra della finestra contiene un elenco di impostazioni relative alla funzionalità selezionata nella parte sinistra della finestra.

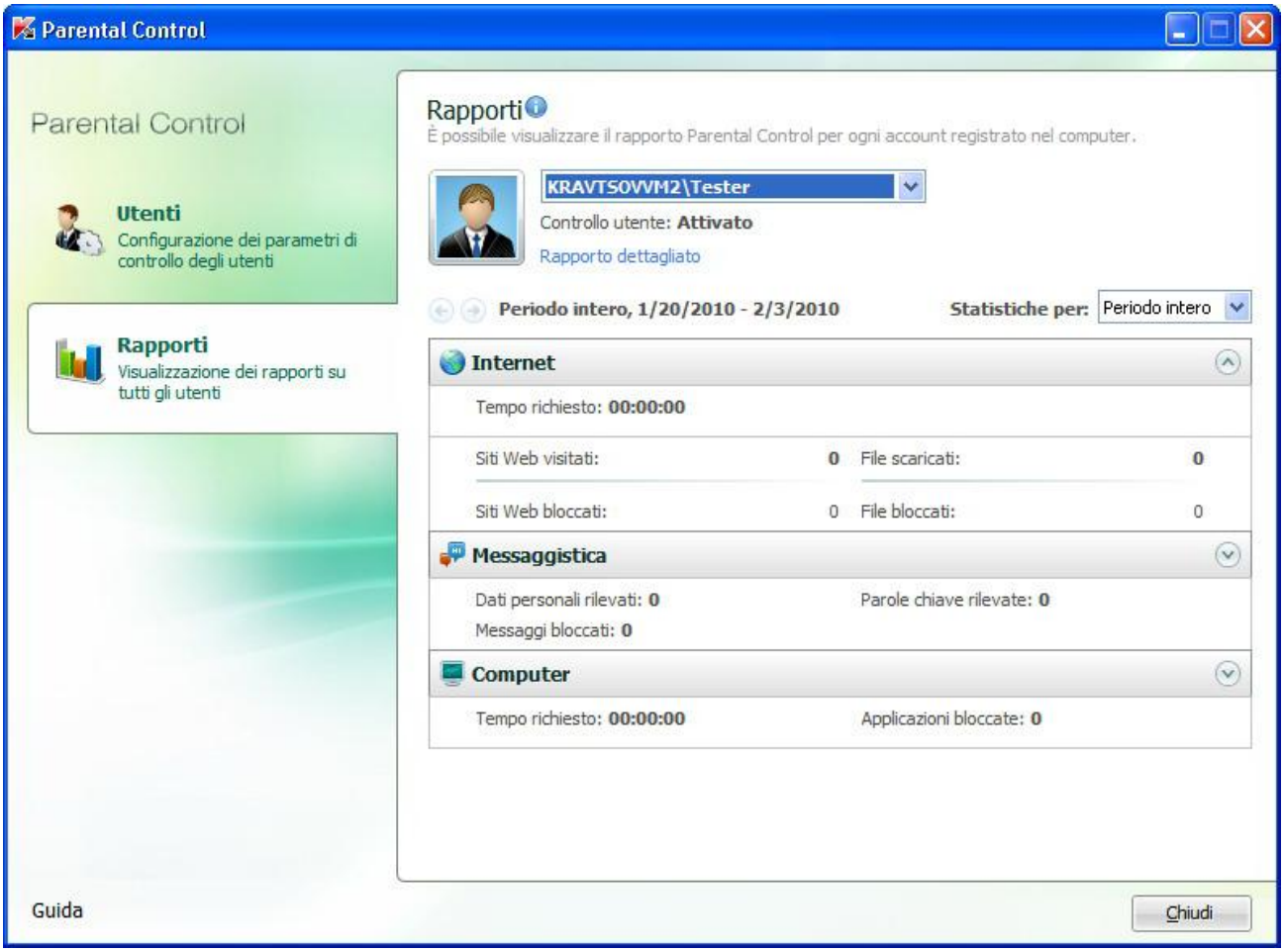


Figura 7. Finestra principale di Parental Control

NOTIFICHE

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

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

- **Allarme**. Si è verificato un evento critico, ad esempio è stato rilevato un virus o un'attività pericolosa nel sistema. È necessario decidere subito come affrontare la minaccia. Le notifiche di questo tipo sono evidenziate in rosso.
- **Attenzione**. Si è verificato un evento potenzialmente pericoloso. Ad esempio, nel sistema sono stati rilevati file potenzialmente infetti o un'attività sospetta. È necessario decidere in base al grado di pericolosità dell'evento. Le notifiche di questo tipo sono evidenziate in giallo.
- **Informazioni**. Questa notifica fornisce informazioni su eventi non critici. Questo tipo, ad esempio, include le notifiche relative al funzionamento del componente Filtro contenuti. Le notifiche informative sono evidenziate in verde.

VEDERE ANCHE:

Notifiche 256

FINESTRA DELLE IMPOSTAZIONI DELL'APPLICAZIONE

È possibile aprire la finestra delle impostazioni di Kaspersky PURE mediante la finestra principale (vedere pagina 44) oppure utilizzando il menu di scelta rapida (vedere pagina 42). Per farlo, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra principale dell'applicazione oppure selezionare l'opzione appropriata dal menu di scelta rapida dell'applicazione.

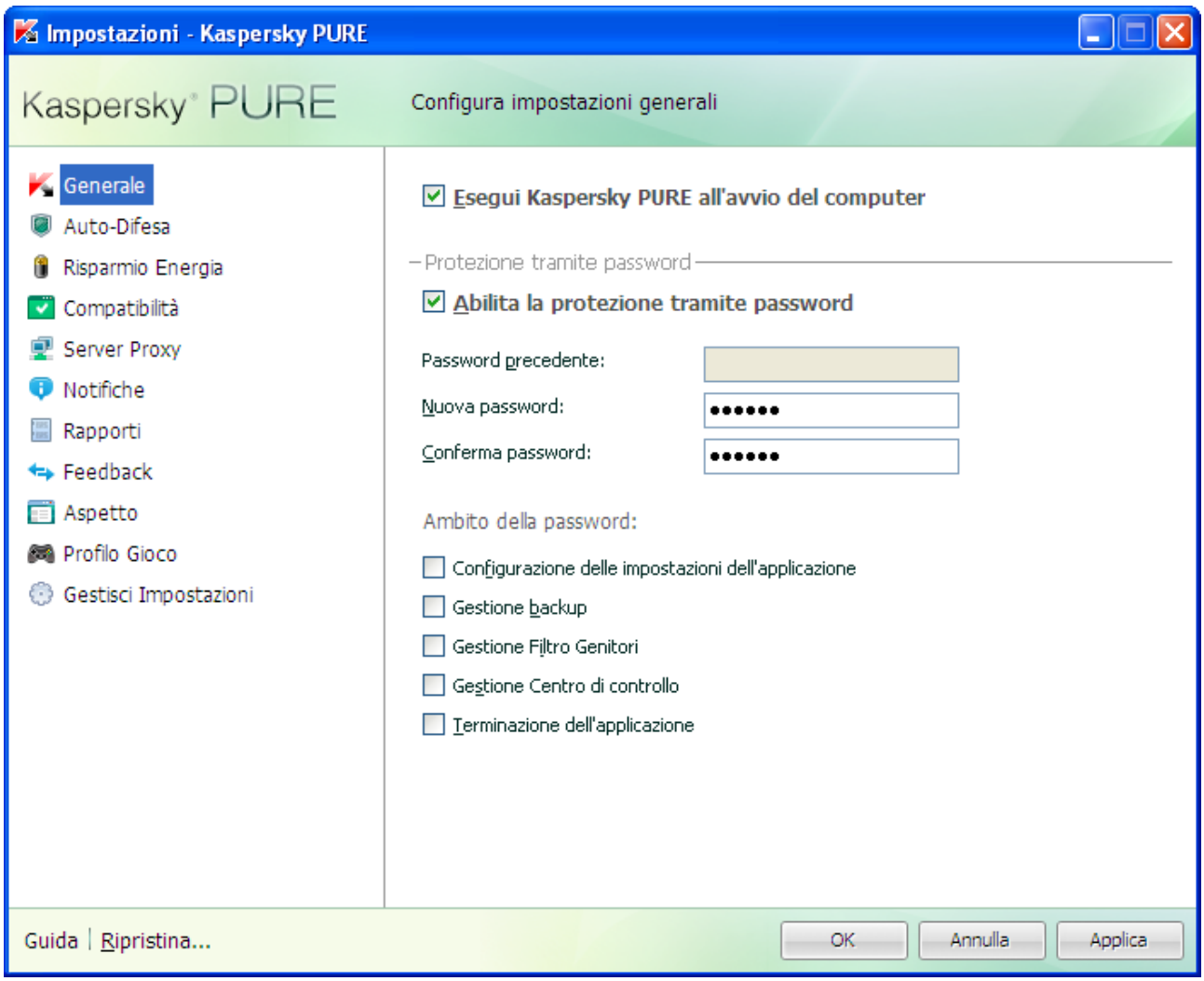


Figura 8. Configurazione Kaspersky Anti-Virus

È inoltre possibile configurare le impostazioni di Protezione del computer. A tale scopo, fare clic sul pulsante **Protezione del computer** nella finestra principale di Kaspersky PURE, quindi fare clic sul collegamento **Impostazioni** nella parte superiore della finestra visualizzata.

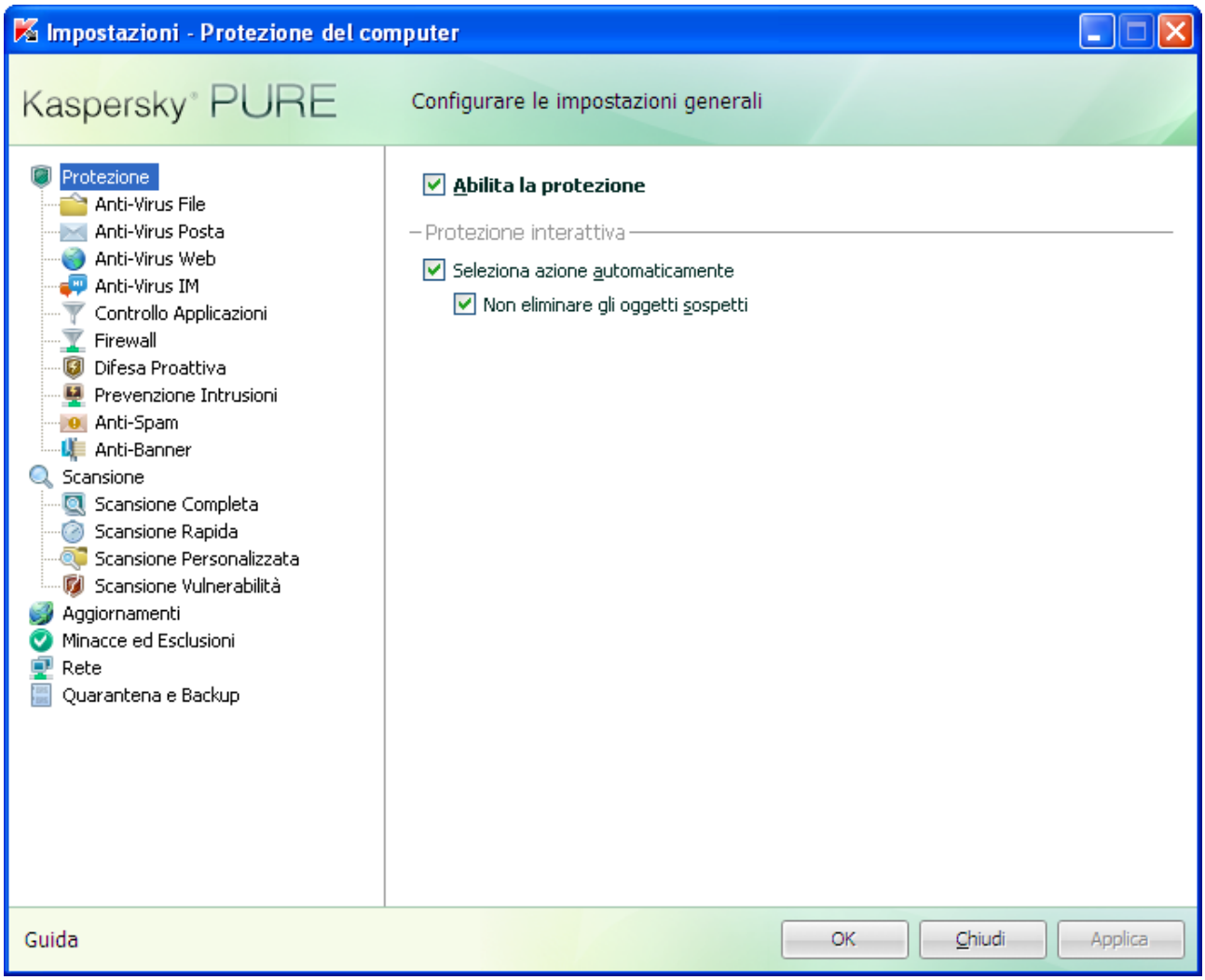


Figura 9. Configurazione Kaspersky Anti-Virus

Le finestre di configurazione delle impostazioni comprendono due parti:

- la parte sinistra della finestra consente di accedere alle attività e alle funzionalità generali di Kaspersky PURE e Protezione del computer relative all'esecuzione di tutti i componenti;
- la parte destra della finestra contiene un elenco di impostazioni relative alla funzionalità o all'attività selezionata nella parte sinistra della finestra.

PROTEZIONE DEL COMPUTER

I componenti di Protezione del computer assicurano la protezione del computer da numerose minacce, analizzano tutti gli oggetti di sistema alla ricerca di virus e vulnerabilità e aggiornano periodicamente i database anti-virus e i moduli di programma di Kaspersky PURE.

IN QUESTA SEZIONE:

Protezione del file system del computer 52

Protezione della posta 62

Protezione del traffico Web 69

Protezione del traffico dei programmi di messaggistica istantanea 76

Controllo Applicazioni 80

Modalità Protetta di esecuzione delle applicazioni 89

Firewall 94

Difesa Proattiva 101

Prevenzione Intrusioni 105

Anti-Spam 107

Anti-Banner 127

Scansione del computer 130

Aggiornamenti 144

Configurazione delle impostazioni di Protezione del computer 150

Rapporti 172

PROTEZIONE DEL FILE SYSTEM DEL COMPUTER

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

Per impostazione predefinita, Anti-Virus File esegue la scansione solo dei file nuovi o modificati. Una raccolta di impostazioni, denominata livello di protezione, determina le condizioni per la scansione dei file. Se Anti-Virus File rileva una minaccia, esegue l'azione assegnata.

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

- quelle che determinano la creazione di un ambito di protezione;
- quelle che determinano la modalità di scansione;
- quelle che determinano la modalità di scansione dei file compositi, inclusa la scansione dei file compositi di grandi dimensioni);
- quelle che determinano il modalità di scansione;
- quelle che consentono di sospendere il funzionamento del componente in base alla pianificazione o durante il funzionamento delle applicazioni selezionate.

Gli specialisti di Kaspersky Lab consigliano di non configurare manualmente le impostazioni del componente Anti-Virus File. Nella maggior parte dei casi è sufficiente modificare il livello di protezione. Per ripristinare le impostazioni predefinite di Anti-Virus File, selezionare uno dei livelli di protezione.

Per modificare le impostazioni di Anti-Virus File:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Virus File**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Apportare le modifiche richieste alle impostazioni dell'applicazione.

IN QUESTA SEZIONE:

Algoritmo di funzionamento del componente 53

Modifica del livello di protezione per i file e la memoria 54

Modifica delle azioni da eseguire sugli oggetti rilevati 54

Creazione di un ambito di protezione 55

Utilizzo dell'analisi euristica 56

Ottimizzazione della scansione 56

Scansione dei file compositi 57

Scansione dei file compositi di grandi dimensioni 57

Modifica della modalità di scansione 58

Tecnologia di scansione 58

Sospensione dell'attività del componente: creazione di una pianificazione 59

Sospensione dell'attività del componente: creazione di un elenco di applicazioni 60

Ripristino delle impostazioni di protezione predefinite 61

ALGORITMO DI FUNZIONAMENTO DEL COMPONENTE

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

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

1. Il componente intercetta gli accessi a ciascun file da parte dell'utente o di qualsiasi programma.

2. Anti-Virus File esamina i database iChecker e iSwift per informazioni sul file intercettato, quindi determina se esaminare il file sulla base delle informazioni recuperate.

Durante la scansione vengono eseguite le operazioni seguenti:

1. Il file viene esaminato alla ricerca di virus. Gli oggetti dannosi vengono riconosciuti in base ai database di Protezione del computer. Il database contiene le descrizioni di tutti i programmi dannosi e le minacce attualmente noti, nonché i metodi per elaborarli.

2. Al termine dell'analisi, è possibile eseguire una delle azioni seguenti di Protezione del computer:

    a. Se nel file viene rilevato codice dannoso, Anti-Virus File blocca il file, ne crea una copia di backup e tenta di disinfettarlo. Se il file viene disinfettato correttamente, diventa nuovamente disponibile. Se la disinfezione non riesce, il file viene eliminato.

    b. Se viene rilevato codice potenzialmente dannoso, senza alcuna garanzia dell'effettiva pericolosità, il file viene comunque disinfettato e quindi inviato in un'area di memorizzazione speciale definita Quarantena.

    c. Se nel file non viene rilevato codice dannoso, esso viene immediatamente ripristinato.

L'applicazione notifica il rilevamento di un file infetto o potenzialmente infetto.Se viene rilevato un oggetto infetto o potenzialmente infetto, sullo schermo viene visualizzato un messaggio di notifica con una richiesta di azioni ulteriori. Viene offerta la possibilità di eseguire le operazioni seguenti:

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

MODIFICA DEL LIVELLO DI PROTEZIONE PER I FILE E LA MEMORIA

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

- **Alto**. Impostare questo livello se si sospetta che la possibilità che il computer venga infettato sia alta.
- **Consigliato**. Questo livello garantisce un equilibrio ottimale tra efficienza e protezione ed è adatto nella maggior parte dei casi.
- **Basso**. Se si lavora in un ambiente protetto, ad esempio in una rete aziendale con una gestione della protezione centralizzata, il livello di protezione basso potrebbe essere appropriato. Questo livello può essere impostato anche quando si lavora con applicazioni che richiedono molte risorse.

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

Se nessuno dei livelli preimpostati soddisfa le proprie esigenze, è possibile configurare le impostazioni (vedere sezione "Protezione del file system del computer" a pagina 52) di Anti-Virus File autonomamente. Di conseguenza, il nome del livello di protezione verrà modificato in **Personalizzato**. Per ripristinare le impostazioni predefinite del componente, selezionare uno dei livelli di protezione preimpostati.

Per modificare il livello di protezione corrente per i file e la memoria, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Virus File**.
4. Impostare il livello di protezione necessario per il componente selezionato.

MODIFICA DELLE AZIONI DA ESEGUIRE SUGLI OGGETTI RILEVATI

In base ai risultati della scansione, il componente Anti-Virus File assegna uno degli stati seguenti agli oggetti rilevati:

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

Se Protezione del computer rileva oggetti infetti o potenzialmente infetti durante una scansione anti-virus, ne dà notifica all'utente. È necessario rispondere alla minaccia selezionando un'azione da eseguire sull'oggetto. Protezione del computer seleziona l'opzione **Chiedi di scegliere un'azione** come azione da eseguire su un oggetto rilevato, che rappresenta l'impostazione predefinita. È possibile modificare l'azione. Se, ad esempio, si desidera eseguire un tentativo

di disinfezione per ogni oggetto rilevato ma non si desidera selezionare l'azione **Disinfetta** ogni volta che si riceve un avviso sul rilevamento di un oggetto infetto o sospetto, è necessario selezionare l'azione: **Seleziona azione. Disinfetta.**

Prima di provare a disinfettare o eliminare un oggetto infetto, Protezione del computer ne crea una copia di backup per consentirne il ripristino o la disinfezione in un secondo momento.

Se si lavora in modalità automatica (vedere la sezione "Passaggio 3. Selezione della modalità di protezione" a pagina 33), Protezione del computer applicherà automaticamente l'azione consigliata dagli specialisti di Kaspersky Lab quando vengono rilevati oggetti pericolosi. Per gli oggetti dannosi, tale azione sarà **Disinfetta. Elimina se la disinfezione fallisce** e **ignora** per gli oggetti sospetti.

Per modificare l'azione specificata da eseguire sugli oggetti rilevati:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Virus File**.
4. Specificare l'azione necessaria per il componente selezionato.

CREAZIONE DI UN AMBITO DI PROTEZIONE

Un ambito di protezione definisce, oltre alla posizione degli oggetti da esaminare, anche il tipo di file da esaminare. Per impostazione predefinita, Protezione del computer esamina solo i file potenzialmente infettabili memorizzati in qualsiasi disco rigido, unità di rete o unità rimovibile.

È possibile espandere o restringere l'ambito di protezione aggiungendo/rimuovendo gli oggetti da esaminare oppure modificando i tipi di file da esaminare. Se ad esempio si desidera esaminare solo i file *exe* eseguiti dalle unità di rete, è necessario agire con cautela per far sì che il computer non venga esposto alla minaccia di infezioni causate dalla limitazione dell'ambito di protezione.

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

- Alcuni formati di file (ad esempio *txt*) presentano un rischio basso di contenere codice dannoso attivabile. Altri formati, al contrario, contengono o possono contenere codice eseguibile (*exe*, *dll*, *doc).* Il rischio di attivare codice dannoso in tali file è estremamente alto.
- L'intruso potrebbe inviare al computer un file con estensione *txt* che in realtà è un file eseguibile rinominato come *txt*. Selezionando l'opzione **Esamina i file per estensione**, tale file viene ignorato dalla scansione. Se si seleziona l'opzione **Esamina i file per formato**, Anti-Virus File analizza l'intestazione del file indipendentemente dall'estensione, rileva se si tratta di un file *.exe*, quindi esegue la scansione anti-virus.

Per modificare l'elenco di scansione degli oggetti:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Virus File**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra visualizzata, nella scheda **Generale**, sezione **Ambito della protezione**, fare clic sul collegamento **Aggiungi**.
6. Nella finestra **Scelta degli oggetti da esaminare** selezionare un oggetto e fare clic sul pulsante **Aggiungi**.

7. Una volta aggiunti tutti gli oggetti richiesti, fare clic sul pulsante **OK** nella finestra **Scelta degli oggetti da esaminare**.

8. Per escludere un oggetto dall'elenco di oggetti da esaminare, deselezionare la relativa casella.

Per modificare il tipo di oggetto esaminato:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.

2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.

3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Virus File**.

4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.

5. Nella finestra visualizzata, scheda **Generale**, sezione **Tipi di file**, selezionare le impostazioni richieste.

UTILIZZO DELL'ANALISI EURISTICA

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

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

Se viene rilevato un oggetto dannoso, viene visualizzato un messaggio di notifica in cui viene richiesto di eseguire un'azione.

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

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

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.

2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.

3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Virus File**.

4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.

5. Nella finestra visualizzata, nella scheda **Prestazioni**, sezione **Metodi di scansione**, selezionare la casella **Analisi euristica** e specificare il livello di dettaglio della scansione.

OTTIMIZZAZIONE DELLA SCANSIONE

Per ridurre la durata delle scansioni e aumentare la velocità delle operazioni di Protezione del computer, è possibile scegliere di sottoporre a scansione solo i file nuovi e i file modificati dopo l'ultima scansione. Questa modalità si estende ai file semplici e a quelli compositi.

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

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.

2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.

3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Virus File**.

4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.

5. Nella finestra visualizzata, nella scheda **Prestazioni**, sezione **Ottimizzazione della scansione**, selezionare la casella **Esamina solo i file nuovi e modificati**.

SCANSIONE DEI FILE COMPOSITI

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

I pacchetti di installazione e i file contenenti oggetti OLE vengono eseguiti all'apertura, risultando quindi più pericolosi degli archivi. Disabilitando la scansione degli archivi e abilitando la scansione di questi tipi di file, il computer viene protetto dall'esecuzione di codice dannoso e, al tempo stesso, la velocità di scansione aumenta.

Per impostazione predefinita, Protezione del computer esamina esclusivamente gli oggetti OLE incorporati.

Per modificare l'elenco dei file compositi esaminati:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.

2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.

3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Virus File**.

4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.

5. Nella finestra visualizzata, nella scheda **Prestazioni** della sezione **Scansione dei file compositi**, selezionare le caselle relative ai tipi di file compositi da sottoporre a scansione.

SCANSIONE DEI FILE COMPOSITI DI GRANDI DIMENSIONI

Durante la scansione di file compositi di grandi dimensioni, la decompressione preliminare può richiedere molto tempo. L'operazione può essere velocizzata se la scansione dei file viene effettuata in background. L'eventuale rilevamento di un oggetto dannoso durante l'utilizzo di file di questo tipo verrà notificato da Protezione del computer.

Per accedere più rapidamente ai file compositi, è possibile disabilitare la decompressione dei file la cui dimensione supera il valore specificato. Quando i file vengono estratti da un archivio, vengono sempre sottoposti a scansione.

Se si desidera che Protezione del computer decomprima i file di grandi dimensioni in background:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.

2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.

3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Virus File**.

4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.

5. Nella finestra visualizzata, nella scheda **Prestazioni**, sezione **Scansione dei file compositi**, fare clic sul pulsante **Avanzate**.

6. Nella finestra **File compositi**, selezionare la casella **Estrai i file compositi in background** e specificare la dimensione di file minima nel campo sottostante.

Per evitare che Protezione del computer decomprima i file compositi di grandi dimensioni:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Virus File**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra visualizzata, nella scheda **Prestazioni**, sezione **Scansione dei file compositi**, fare clic sul pulsante **Avanzate**.
6. Nella finestra **File compositi** visualizzata, selezionare la casella **Non decomprimere i file compositi di grandi dimensioni** e specificare la dimensione di file nel campo adiacente.

MODIFICA DELLA MODALITA DI SCANSIONE

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

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

Per modificare la modalità di scansione degli oggetti:

1. Aprire la finestra principale dell'applicazione e fare clic sulpulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Virus File**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra visualizzata, nella scheda **Avanzate**, sezione **Modalità di scansione**, selezionare la modalità richiesta.

TECNOLOGIA DI SCANSIONE

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

- **Tecnologia iChecker**. Questa tecnologia è in grado di aumentare la velocità di scansione escludendo determinati oggetti dalla scansione. Un oggetto viene escluso dalla scansione in base a uno speciale algoritmo che valuta la data di rilascio dei database di Protezione del computer, la data dell'ultima scansione dell'oggetto e tutte le modifiche apportate alle impostazioni di scansione.

  Si supponga, ad esempio, di disporre di un file archivio a cui dopo la scansione è stato assegnato lo stato *non infetto*. Alla scansione successiva, l'applicazione ignorerà questo archivio, a meno che non sia stato modificato o non siano state modificate le impostazioni di scansione. Se la struttura dell'archivio risulta modificata perché è stato aggiunto un nuovo oggetto oppure se le impostazioni di scansione sono state modificate o i database dell'applicazione aggiornati, il programma esaminerà nuovamente l'archivio.

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

- **Tecnologia iSwift**. Questa tecnologia è stata sviluppata a partire dalla tecnologia iChecker per i computer che utilizzano un file system di tipo NTFS. Anche iSwift presenta delle limitazioni: è associata a un percorso di file specifico nel file system e può essere applicata solo ad oggetti in NTFS.

Per cambiare tecnologia di scansione degli oggetti:

1. Aprire la finestra principaledell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Virus File**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra visualizzata, nella scheda **Avanzate**, sezione **Tecnologie di scansione**, selezionare il valore dell'impostazione richiesta.

SOSPENSIONE DELL'ATTIVITA DEL COMPONENTE: CREAZIONE DI UNA PIANIFICAZIONE

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

Figura 10. Creazione di una pianificazione

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

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Virus File**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra visualizzata, nella scheda **Avanzate** della sezione **Sospendi l'attività**, selezionare la casella **In base alla pianificazione** e fare clic sul pulsante **Pianificazione**.
6. Nella finestra **Sospensione dell'attività**, specificare la durata (in formato HH:MM) della sospensione della protezione (campi **Sospendi l'attività alle** e **Riprendi l'attività alle**).

SOSPENSIONE DELL'ATTIVITA DEL COMPONENTE: CREAZIONE DI UN ELENCO DI APPLICAZIONI

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

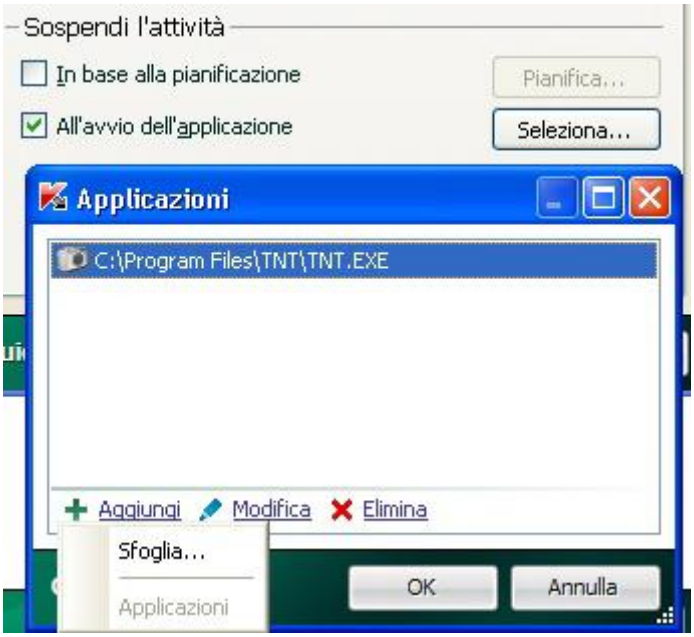


Figura 11. Creazione di un elenco di applicazioni

La configurazione della disabilitazione del componente Anti-Virus File in caso di conflitti con determinate applicazioni rappresenta una misura drastica. Se il conflitto viene generato mentre si lavora con il componente, contattare l'Assistenza tecnica Kaspersky Lab (http://support.kaspersky.com/it/). Gli specialisti dell'assistenza tecnica aiuteranno a risolvere i problemi di funzionamento di Protezione del computer in contemporanea con il software presente nel computer.

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

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Virus File**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra visualizzata, nella scheda**Avanzate**, sezione **Sospendi l'attività** selezionare la casella **All'avvio dell'applicazione** e fare clic sul pulsante **Seleziona**.
6. Nella finestra **Applicazioni**, creare un elenco di applicazioni la cui esecuzione comporta la sospensione del componente.

RIPRISTINO DELLE IMPOSTAZIONI DI PROTEZIONE PREDEFINITE

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

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

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Virus File**.
4. Nella sezione **Livello di protezione**, fare clic sul pulsante **Livello predefinito** relativo al componente selezionato.

PROTEZIONE DELLA POSTA

Anti-Virus Posta esamina i messaggi di posta elettronica in entrata e in uscita per verificare la presenza di oggetti nocivi. Viene avviato durante il caricamento del sistema operativo, si trova nella RAM del computer ed esamina tutti i messaggi di posta ricevuti tramite i protocolli POP3, SMTP, IMAP, MAPI e NNTP.

Una raccolta di impostazioni denominata livello di protezione determina la modalità di scansione del traffico. Quando viene rilevata una minaccia, Anti-Virus Posta esegue l'azione specificata dall'utente (vedere la sezione "Modifica delle azioni da eseguire sugli oggetti rilevati" a pagina 64). Le regole di scansione della posta elettronica sono definite da una serie di impostazioni. Possono essere suddivise in gruppi e determinano le funzionalità seguenti:

- ·dal flusso di posta protetto;
- ·utilizzo dei metodi di analisi euristica;
- ·scansione dei file compositi;
- ·filtraggio dei file allegati.

Kaspersky Lab consiglia di non configurare manualmente le impostazioni di Anti-Virus Posta. Nella maggior parte dei casi è sufficiente selezionare un livello di protezione diverso. È possibile ripristinare le impostazioni predefinite di Anti-Virus Posta. A tale scopo, selezionare uno dei livelli di protezione disponibili.

Per modificare le impostazioni di Anti-Virus Posta, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, selezionare il componente **Anti-Virus Posta** nella sezione **Protezione**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Apportare le modifiche richieste alle impostazioni dell'applicazione.

IN QUESTA SEZIONE:

Algoritmo di funzionamento del componente 63

Modifica del livello di protezione dei messaggi di posta elettronica 63

Modifica delle azioni da eseguire sugli oggetti rilevati 64

Creazione di un ambito di protezione 65

Scansione della posta elettronica in Microsoft Office Outlook 65

Scansione della posta elettronica in The Bat! 66

Utilizzo dell'analisi euristica 67

Scansione dei file compositi 67

Filtraggio degli allegati 67

Ripristino delle impostazioni di protezione della posta elettronica predefinite 68

ALGORITMO DI FUNZIONAMENTO DEL COMPONENTE

Protezione del computer include il componente *Anti-Virus Posta*, per l'individuazione di oggetti pericolosi nelle e-mail. Tale componente viene caricato all'avvio del sistema operativo ed è sempre in esecuzione per esaminare tutta la posta elettronica sui protocolli POP3, SMTP, IMAP, MAPI e NNTP, nonché le connessioni protette (SSL) per POP3 e IMAP.

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

Per impostazione predefinita, la posta viene protetta nel modo seguente:

1. Ogni messaggio di posta ricevuto o inviato dall'utente viene intercettato dal componente.

2. Viene quindi suddiviso nelle parti che lo compongono: l'intestazione, il corpo del testo e gli allegati.

3. Il corpo e gli allegati del messaggio (inclusi gli oggetti OLE) vengono esaminati per escludere la presenza di oggetti pericolosi. Gli oggetti dannosi vengono individuati grazie ai database utilizzati da Protezione del computer e all'algoritmo euristico. Il database contiene le descrizioni di tutti i programmi dannosi attualmente conosciuti, nonché i metodi che consentono di neutralizzarli. L'algoritmo euristico è in grado di rilevare nuovi virus non ancora inseriti nel database.

4. Dopo la scansione anti-virus, è possibile eseguire le azioni seguenti:

   - Se il corpo o gli allegati del messaggio contengono un codice dannoso, il componente Anti-Virus File blocca il messaggio, ne crea una copia di backup e cerca di disinfettare l'oggetto. Dopo aver completato la disinfezione, lo restituisce all'utente. Se la disinfezione non riesce, l'oggetto infetto viene eliminato dal messaggio. Dopo la scansione anti-virus, nella riga dell'oggetto del messaggio viene inserito un testo che indica che il messaggio è stato elaborato da Protezione del computer.

   - Se nel corpo o in un allegato viene rilevato codice potenzialmente dannoso, la cui pericolosità non è tuttavia garantita, la parte sospetta del messaggio viene spostata in un'area di memorizzazione speciale denominata Quarantena.

   - Se all'interno del messaggio non viene individuato alcun codice dannoso, il messaggio viene reso immediatamente disponibile all'utente.

Per Microsoft Office Outlook viene fornito un modulo di estensione integrato (vedere la sezione "Scansione della posta elettronica in Microsoft Office Outlook" a pagina 65) che consente di ottimizzare il client di posta.

Se si utilizza The Bat!, Protezione del computer può essere utilizzato unitamente ad altre applicazioni anti-virus. In questo caso, le regole per l'elaborazione del traffico e-mail (vedere la sezione "Scansione della posta elettronica in The Bat!" a pagina 66) vengono configurate direttamente in The Bat! e sostituiscono le impostazioni di protezione e-mail dell'applicazione.

Se si lavora con altri programmi di posta (inclusi Microsoft Outlook Express/Windows Mail, Mozilla Thunderbird, Eudora e Incredimail), Anti-Virus Posta esamina i messaggi sui protocolli SMTP, POP3, IMAP, e NNTP.

Si noti che quando si lavora con il client di posta Thunderbird, i messaggi di posta elettronica trasferiti attraverso IMAP non verranno sottoposti a una scansione anti-virus se vengono utilizzati filtri per il trasferimento dei messaggi dalla cartella **Posta in arrivo**.

MODIFICA DEL LIVELLO DI PROTEZIONE DEI MESSAGGI DI POSTA ELETTRONICA

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

- **Alto**. Se si lavora in un ambiente non protetto, è consigliabile impostare il livello massimo di protezione. Un esempio di ambiente di questo tipo è rappresentato da una connessione a un servizio di posta elettronica gratuito, da una rete priva di protezione centralizzata della posta elettronica.

- **Consigliato**. Questo livello garantisce un equilibrio ottimale tra efficienza e protezione ed è adatto nella maggior parte dei casi. Rappresenta anche l'impostazione predefinita.

- **Basso**. Se si lavora in un ambiente ben protetto, è possibile utilizzare il livello di protezione basso. Un esempio di ambiente di questo tipo è rappresentato da una rete aziendale con protezione centralizzata della posta elettronica.

Se nessuno dei livelli preimpostati soddisfa le proprie esigenze, è possibile configurare le impostazioni (vedere sezione "Protezione della posta" a pagina 62) di Anti-Virus Posta autonomamente. Di conseguenza, il nome del livello di protezione verrà modificato in **Personalizzato**. Per ripristinare le impostazioni predefinite del componente, selezionare uno dei livelli di protezione preimpostati.

Per modificare il livello di protezione della posta elettronica preimpostato:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, selezionare il componente **Anti-Virus Posta** nella sezione **Protezione**.
4. Impostare il livello di protezione necessario per il componente selezionato.

MODIFICA DELLE AZIONI DA ESEGUIRE SUGLI OGGETTI RILEVATI

Anti-Virus Posta esamina un messaggio di posta elettronica. Se la scansione indica che il messaggio o una delle sue parti (corpo, allegato) è infetto o potenzialmente infetto, le successive operazioni del componente dipendono dallo stato dell'oggetto e dall'azione selezionata.

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

- Programma dannoso, ad esempio nel caso di un *virus* o di un *Trojan*.

- *potenzialmente infetto*, quando la scansione non è in grado di determinare se l'oggetto è infetto. Ciò significa che il messaggio di posta o l'allegato contiene una sequenza di codice di un virus sconosciuto o un codice modificato di un virus conosciuto.

Se Protezione del computer rileva oggetti infetti o potenzialmente infetti durante una scansione anti-virus, ne dà notifica all'utente. È necessario rispondere alla minaccia selezionando un'azione da eseguire sull'oggetto. Protezione del computer seleziona l'opzione **Chiedi di scegliere un'azione** come azione da eseguire su un oggetto rilevato, che rappresenta l'impostazione predefinita. È possibile modificare l'azione. Se, ad esempio, si desidera eseguire un tentativo di disinfezione per ogni oggetto rilevato ma non si desidera selezionare l'azione **Disinfetta** ogni volta che si riceve un avviso sul rilevamento di un oggetto infetto o sospetto in un messaggio, è necessario selezionare l'azione: **Seleziona azione. Disinfetta.**

Prima di provare a disinfettare o eliminare un oggetto infetto, Protezione del computer ne crea una copia di backup per consentirne il ripristino o la disinfezione in un secondo momento.

Se si lavora in modalità automatica (vedere la sezione "Passaggio 3. Selezione della modalità di protezione" a pagina 33), Protezione del computer applicherà automaticamente l'azione consigliata dagli specialisti di Kaspersky Lab quando vengono rilevati oggetti pericolosi. Per gli oggetti dannosi, tale azione sarà **Disinfetta. Elimina se la disinfezione fallisce** e **ignora** per gli oggetti sospetti.

Per modificare l'azione specificata da eseguire sugli oggetti rilevati:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.

2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.

3. Nella finestra visualizzata, selezionare il componente **Anti-Virus Posta** nella sezione **Protezione**.

4. Specificare l'azione necessaria per il componente selezionato.

CREAZIONE DI UN AMBITO DI PROTEZIONE

Per ambito di protezione si intende il tipo di messaggi da esaminare. Per impostazione predefinita, Protezione del computer esamina sia i messaggi in arrivo che quelli in uscita. Se si è scelto di esaminare solo quelli in arrivo, si consiglia di esaminare anche quelli in uscita quando Protezione del computer viene utilizzato per la prima volta, in quanto è probabile che il computer contenga worm che potrebbero diffondersi tramite la posta elettronica. Questa misura precauzionale contribuirà a evitare situazioni spiacevoli spesso causate da invii non controllati di grandi quantità di messaggi di posta infetti provenienti dal proprio computer.

L'ambito di protezione include inoltre le impostazioni utilizzate per l'integrazione di Anti-Virus Posta nel sistema e i protocolli da esaminare. Per impostazione predefinita, il componente Anti-Virus Posta è integrato nei client di posta Microsoft Office Outlook e The Bat!.

- *Per disabilitare la scansione della posta in uscita, eseguire le operazioni seguenti:*

  1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.

  2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.

  3. Nella finestra visualizzata, selezionare il componente **Anti-Virus Posta** nella sezione **Protezione**.

  4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.

  5. Specificare nella finestra visualizzata i valori richiesti per le impostazioni nella scheda **Generale** della sezione **Ambito della protezione**.

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

  1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.

  2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.

  3. Nella finestra visualizzata, selezionare il componente **Anti-Virus Posta** nella sezione **Protezione**.

  4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.

  5. Nella finestra visualizzata, scheda **Avanzate**, sezione **Connettività**, selezionare le impostazioni richieste.

SCANSIONE DELLA POSTA ELETTRONICA IN MICROSOFT OFFICE OUTLOOK

Se si utilizza Microsoft Office Outlook come client di posta elettronica, è possibile configurare delle impostazioni aggiuntive per la scansione anti-virus della posta.

Durante l'installazione di Protezione del computer, in Microsoft Office Outlook viene installato uno speciale plug-in. che consente di configurare velocemente le impostazioni del componente Anti-Virus Posta e di determinare i messaggi di posta elettronica che verranno esaminati per cercare eventuali oggetti pericolosi.

Il plug-in si presenta sotto forma di una scheda speciale denominata **Anti-Virus Posta** che si trova nel menu **Strumenti** → **Opzioni**. Questa scheda consente di specificare le modalità di scansione della posta.

Per specificare condizioni di filtraggio complesse:

1. Aprire la finestra principale di Microsoft Outlook.
2. Selezionare **Strumenti** → **Opzioni** dal menu dell'applicazione.
3. Selezionare la scheda **Anti-Virus Posta** e specificare la modalità di scansione della posta desiderata.

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 moduli anti-virus installati nel computer che supportano The Bat!.

È importante ricordare che i messaggi di posta elettronica in entrata vengono esaminati prima dal componente Anti-Virus Posta e solo successivamente dal plug-in del client di posta di The Bat!. Se viene rilevato un oggetto dannoso, Protezione del computer informerà immediatamente l'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'azione **Ignora** nella finestra di notifica, l'oggetto verrà disinfettato dal plug-in The Bat!. Quando si inviano messaggi di posta elettronica, la scansione viene eseguita prima dal plug-in, quindi da Anti-Virus Posta.

È necessario decidere:

- quale flusso di messaggi di posta elettronica sarà esaminato (in entrata, in uscita).
- in che momento gli oggetti della posta elettronica saranno analizzati (all'apertura di un messaggio o prima di salvarlo su disco).
- le azioni intraprese dal client di posta quando nei messaggi di posta elettronica vengono rilevati oggetti pericolosi. È ad esempio possibile selezionare:
  - **Tenta di disinfettare le parti infette**: se questa opzione è selezionata, si tenterà di disinfettare l'oggetto infetto. Se non è possibile disinfettarlo, resterà 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.

The Bat! non assegna intestazioni speciali ai messaggi contenenti oggetti pericolosi.

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

1. Aprire la finestra principale di The Bat!.
2. Selezionare **Impostazioni** dal menu **Proprietà** del client di posta.
3. Selezionare **Protezione anti-virus** nella struttura ad albero delle impostazioni.

UTILIZZO DELL'ANALISI EURISTICA

Il metodo euristico implica l'analisi delle attività eseguite dall'oggetto nel sistema. Se tali azioni sono tipiche di oggetti dannosi, è probabile che l'oggetto venga classificato come dannoso o sospetto. In questo modo è possibile rilevare le nuove minacce prima che queste vengano studiate dagli analisti anti-virus. L'analisi euristica è abilitata per impostazione predefinita.

Protezione del computer informa l'utente della presenza di un oggetto nocivo rilevato in un messaggio. È necessario rispondere alla notifica elaborando ulteriormente il messaggio.

Inoltre, è possibile impostare il livello di dettaglio delle scansioni, **superficiale**, **media** o **approfondita**, spostando il cursore nella posizione selezionata.

- *Per abilitare/disabilitare l'analisi euristica e impostare il livello di dettaglio della scansione, eseguire le operazioni seguenti:*

  1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
  2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
  3. Nella finestra visualizzata, selezionare il componente **Anti-Virus Posta** nella sezione **Protezione**.
  4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
  5. Nella finestra visualizzata, nella scheda **Generale**, sezione **Metodi di scansione**, selezionare/deselezionare la casella **Analisi euristica** e specificare il livello di dettaglio della scansione.

SCANSIONE DEI FILE COMPOSITI

La selezione della modalità di scansione dei file compositi influisce sulle prestazioni di Protezione del computer. È possibile abilitare o disabilitare la scansione degli archivi allegati e limitare le dimensioni massime degli archivi da esaminare.

- *Per configurare le impostazioni di scansione dei file compositi:*

  1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
  2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
  3. Nella finestra visualizzata, selezionare il componente **Anti-Virus Posta** nella sezione **Protezione**.
  4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
  5. Nella finestra visualizzata, nella scheda **Generale**, selezionare la modalità di scansione dei file compositi.

FILTRAGGIO DEGLI ALLEGATI

È possibile configurare le condizioni di filtraggio per gli allegati di posta elettronica. L'uso del filtro consente di aumentare la protezione del computer, in quanto nella maggior parte dei casi i programmi dannosi si diffondono attraverso l'invio di allegati. Rinominando o eliminando determinati tipi di allegato, è possibile proteggere il computer da potenziali pericoli, ad esempio l'apertura automatica degli allegati alla ricezione di un messaggio.

Se il computer non è protetto da alcun software di rete locale e se si accede a Internet direttamente senza un server proxy o un firewall, si consiglia di non disabilitare la scansione degli archivi allegati.

- *Per configurare le impostazioni di filtraggio degli allegati:*

  1. Aprire la finestra principaledell'applicazione e fare clic sul pulsante **Protezione del computer**.

2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.

3. Nella finestra visualizzata, selezionare il componente **Anti-Virus Posta** nella sezione **Protezione**.

4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.

5. Nella finestra visualizzata, nella scheda **Filtro allegati**, specificare le condizioni di filtraggio per gli allegati di posta elettronica. Selezionando una delle ultime due modalità l'elenco di tipi di file diventa attivo e consente di specificare i tipi richiesti o di aggiungere una maschera per la selezione di un nuovo tipo.

   Se è necessario aggiungere una maschera di un nuovo tipo, fare clic sul collegamento **Aggiungi** e immettere i dati richiesti nella finestra **Maschera per il nome del file** visualizzata.

RIPRISTINO DELLE IMPOSTAZIONI DI PROTEZIONE DELLA POSTA ELETTRONICA PREDEFINITE

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

Per ripristinare le impostazioni predefinite relative alla posta, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.

2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.

3. Nella finestra visualizzata, selezionare il componente **Anti-Virus Posta** nella sezione **Protezione**.

4. Nella sezione **Livello di protezione**, fare clic sul pulsante **Livello predefinito** relativo al componente selezionato.

PROTEZIONE DEL TRAFFICO WEB

Ogni volta che si usa Internet, si espongono le informazioni memorizzate nel computer al rischio di infezione da parte di programmi pericolosi. Tali programmi possono accedere al computer durante il download di programmi gratuiti o la navigazione in siti ritenuti sicuri che di recente hanno subito attacchi di rete. Inoltre, i worm di rete possono accedere al computer ancora prima dell'apertura di una pagina Web o del download di un file, in quanto è sufficiente che il computer sia collegato a Internet.

Il componente *Anti-Virus Web* è progettato per garantire la protezione durante l'utilizzo di Internet. Esso protegge il computer dai dati che arrivano attraverso il protocollo HTTP e inoltre previene l'esecuzione di script pericolosi sul computer.

La protezione Web controlla solo il traffico HTTP che passa attraverso le porte incluse nell'elenco di porte monitorate. Nel pacchetto di installazione di Protezione del computer è incluso un elenco di porte comunemente utilizzate per la trasmissione della posta elettronica e del traffico HTTP. Se l'utente usa porte non comprese nell'elenco, dovrà aggiungerle per proteggere il traffico da esse gestito.

Se si lavora in un'area non protetta, è consigliabile utilizzare Anti-Virus Web durante la navigazione in Internet. Se il computer è inserito in una rete protetta da un firewall di filtri del traffico HTTP, Anti-Virus Web fornisce un'ulteriore protezione durante l'uso di Internet.

Una raccolta di impostazioni denominata livello di protezione determina la modalità di scansione del traffico. Se Anti-Virus Web rileva una minaccia, esegue l'azione assegnata.

Il livello di protezione del traffico Web è determinato da un insieme di impostazioni. Tali impostazioni possono essere suddivise nei gruppi seguenti:

- Impostazioni per l'ambito di protezione;
- impostazioni che determinano l'efficienza della protezione del traffico (utilizzo dell'analisi euristica, ottimizzazione della scansione).

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

Per modificare le impostazioni di Anti-Virus Web:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, selezionare il componente **Anti-Virus Web** nella sezione **Protezione**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Apportare le modifiche richieste alle impostazioni dell'applicazione.

IN QUESTA SEZIONE:

Algoritmo di funzionamento del componente 70

Modifica del livello di protezione del traffico HTTP 71

Modifica delle azioni da eseguire sugli oggetti rilevati 71

Creazione di un ambito di protezione 71

Selezione del tipo di scansione 72

Barra degli strumenti di Kaspersky 73

Utilizzo dell'analisi euristica 74

Ottimizzazione della scansione 74

Ripristino delle impostazioni di protezione Web predefinite 75

ALGORITMO DI FUNZIONAMENTO DEL COMPONENTE

Anti-Virus Web protegge il computer verificando i dati che entrano nel computer tramite HTTP e impedisce l'esecuzione di script pericolosi nel computer.

In questa sezione viene descritto in modo più dettagliato il funzionamento del componente. Il traffico HTTP viene protetto mediante l'algoritmo seguente:

1. Ogni pagina Web o file a cui l'utente o un determinato programma può accedere attraverso il protocollo HTTP viene intercettato e analizzato da Anti-Virus Web per escludere la presenza di codice dannoso. Gli oggetti dannosi vengono individuati utilizzando i database di Protezione del computer e l'algoritmo euristico. Il database contiene le descrizioni di tutti i programmi dannosi attualmente conosciuti, nonché i metodi che consentono di neutralizzarli. L'algoritmo euristico è in grado di rilevare nuovi virus non ancora inseriti nel database.

2. Dopo l'analisi è possibile agire come segue:

   - Se una pagina Web o un oggetto al quale l'utente cerca di accedere contengono codice dannoso, l'accesso a tale oggetto o pagina Web viene bloccato. Viene visualizzata una notifica relativa all'infezione dell'oggetto o della pagina richiesta.

   - Se il file o la pagina Web non contiene codice dannoso, il programma concede immediatamente l'accesso all'utente.

Gli script vengono esaminati secondo l'algoritmo seguente:

1. Ogni esecuzione di uno script su una pagina Web viene intercettata da Anti-Virus Web e analizzata per individuare eventuali codici dannosi.

2. Se lo script contiene codice dannoso, Anti-Virus Web lo blocca, informando l'utente con un apposito messaggio a comparsa.

3. Se nello script non viene rilevato alcun codice dannoso, esso viene eseguito.

Gli script vengono intercettati solo nelle pagine Web aperte in Microsoft Internet Explorer.

MODIFICA DEL LIVELLO DI PROTEZIONE DEL TRAFFICO HTTP

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

- **Alto**. Questo livello di protezione è consigliato in ambienti sensibili in cui non vengono utilizzati altri strumenti di protezione HTTP.
- **Consigliato**. Questo livello di protezione rappresenta la scelta ideale nella maggior parte delle situazioni.
- **Basso**. Utilizzare questo livello di protezione se nel computer sono installati altri strumenti di protezione del traffico HTTP.

Se nessuno dei livelli preimpostati soddisfa le proprie esigenze, è possibile configurare le impostazioni (vedere sezione "Protezione del traffico Web" a pagina 69) di Anti-Virus Web autonomamente. Di conseguenza, il nome del livello di protezione verrà modificato in **Personalizzato**. Per ripristinare le impostazioni predefinite del componente, selezionare uno dei livelli di protezione preimpostati.

Per modificare il livello di protezione preimpostato per il traffico Web:

1. Aprire la finestra principaledell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, selezionare il componente **Anti-Virus Web** nella sezione **Protezione**.
4. Impostare il livello di protezione necessario per il componente selezionato.

MODIFICA DELLE AZIONI DA ESEGUIRE SUGLI OGGETTI RILEVATI

Se l'analisi di un oggetto HTTP indica che questo contiene codice nocivo, la risposta del componente Anti-Virus Web dipende dall'azioni selezionata dall'utente.

Anti-Virus Web blocca sempre le azioni eseguite da oggetti pericolosi e genera messaggi pop-up che comunicano all'utente l'azione intrapresa. L'azione su uno script pericoloso non può essere modificata. L'unica modifica possibile è la disabilitazione del modulo di scansione dello script (vedere la sezione "Selezione del tipo di scansione" a pagina 72).

Se si lavora in modalità automatica (vedere la sezione "Passaggio 3. Selezione della modalità di protezione" a pagina 33), Protezione del computer applicherà automaticamente l'azione consigliata dagli specialisti di Kaspersky Lab quando vengono rilevati oggetti pericolosi.

Per modificare l'azione specificata da eseguire sugli oggetti rilevati:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, selezionare il componente **Anti-Virus Web** nella sezione **Protezione**.
4. Specificare l'azione necessaria per il componente selezionato.

CREAZIONE DI UN AMBITO DI PROTEZIONE

La creazione di un ambito di protezione consiste nella selezione del tipo di scansione (vedere la sezione "Selezione del tipo di scansione" a pagina 72) degli oggetti con Anti-Virus Web e nella creazione dell'elenco di indirizzi Web attendibili,

che contiene informazioni non sottoposte a scansione da parte del componente per rilevare la presenza di oggetti pericolosi.

È possibile creare un elenco di indirizzi Web attendibili i cui contenuti sono ritenuti assolutamente innocui. Anti-Virus Web non analizzerà i dati provenienti da tali indirizzi per verificare la presenza di oggetti pericolosi. Questa opzione può risultare utile nei casi ad esempio in cui Anti-Virus Web interferisce con il download di un file specifico.

Per creare l'elenco di indirizzi Web attendibili, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, selezionare il componente **Anti-Virus Web** nella sezione **Protezione**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra **Anti-Virus Web** visualizzata, sezione **Ottimizzazione della scansione**, selezionare la casella **Non esaminare il traffico HTTP per gli indirizzi attendibili** e fare clic sul pulsante **Seleziona**.
6. Nella finestra **Elenco degli indirizzi Web attendibili** visualizzata, fare clic sul collegamento **Aggiungi**.
7. Nella finestra **Maschera per l'indirizzo (URL)** visualizzata, immettere un indirizzo Web attendibile o la relativa maschera.

SELEZIONE DEL TIPO DI SCANSIONE

L'attività di creazione di un ambito di protezione (vedere pagina 71), insieme alla creazione dell'elenco di indirizzi Web attendibili, include anche la selezione del tipo di scansione del traffico eseguita da Anti-Virus Web. A seconda del tipo, la scansione viene divisa tra scansione degli script e la scansione del traffico HTTP.

Per impostazione predefinita, Anti-Virus Web esegue la scansione del traffico HTTP e degli script simultaneamente.

La scansione del traffico HTTP include non solo la scansione anti-virus ma anche la verifica dei collegamenti per controllare che non siano inclusi nell'elenco di indirizzi Web sospetti e/o nell'elenco di indirizzi Web di phishing.

Il controllo dei collegamenti per verificare che non siano inclusi nell'elenco di indirizzi Web di phishing consente di evitare attacchi di phishing che, in genere, si presentano sotto forma di messaggi di posta elettronica provenienti da sedicenti istituti finanziari e contengono collegamenti ai relativi siti Web. Il testo del messaggio induce il lettore a fare clic sul collegamento e a immettere informazioni riservate nella finestra che segue, ad esempio, un numero di carta di credito o il nome utente e la password usati per collegarsi al proprio sito di Internet banking per eseguire operazioni finanziarie.

Poiché è possibile ricevere il collegamento a un sito di phishing non solo in un messaggio di posta elettronica ma attraverso altri veicoli, ad esempio nel testo di un messaggio ICQ, il componente Anti-Virus Web tiene traccia dei tentativi di accesso a un sito di phishing a livello di scansione del traffico HTTP e li blocca.

Il controllo dei collegamenti per verificare che non siano inclusi nell'elenco di indirizzi Web sospetti consente di tenere traccia dei siti Web inclusi nell'elenco Bloccati. L'elenco viene creato dagli specialisti di Kaspersky Lab ed è integrato nel pacchetto di installazione dell'applicazione.

Per consentire la scansione degli script da parte di Anti-Virus Web, eseguire le operazioni seguenti:

1. Aprire la finestraprincipale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, selezionare il componente **Anti-Virus Web** nella sezione **Protezione**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra **Anti-Virus Web** visualizzata, nella sezione **Avanzate**, verificare che la casella **Blocca gli script pericolosi in Microsoft Internet Explorer** sia selezionata.5. Anti-Virus Web eseguirà la scansione

di tutti gli script elaborati in Microsoft Internet Explorer, nonché di qualsiasi altro script WSH (JavaScript, Visual Basic Script e così via) avviato durante l'utilizzo del computer da parte dell'utente.

È inoltre possibile utilizzare il Barra degli strumenti di Kaspersky (vedere pagina 73). A tale scopo, selezionare la casella **Segnala gli URL sospetti o di phishing in Microsoft Internet Explorer e Mozilla Firefox**. Anti-Virus Web contrassegna gli URL sospetti e di phishing di indirizzi Web rilevati nei browser (Microsoft Internet Explorer e Mozilla Firefox).

Per eseguire la scansione dei collegamenti utilizzando il database di indirizzi Web sospetti e/o di indirizzi Web di phishing, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic supulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, selezionare il componente **Anti-Virus Web** nella sezione **Protezione**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra **Anti-Virus Web** visualizzata, nella sezione **Metodi di scansione**, verificare che le caselle **Confronta gli URL con il database degli indirizzi sospetti** e/o **Confronta gli URL con il database degli indirizzi di phishing** siano selezionate.

BARRA DEGLI STRUMENTI DI KASPERSKY

Protezione del computer include il modulo di scansione degli URL gestito da Anti-Virus Web. Tale modulo verifica se i collegamenti presenti nella pagina Web appartengono all'elenco degli indirizzi Web di phishing o sospetti. È possibile creare un elenco di indirizzi Web attendibili il cui contenuto non deve essere sottoposto a scansione e un elenco di indirizzi Web il cui contenuto deve invece essere necessariamente sottoposto a scansione. Questo modulo è incorporato come plug-in nei browser Microsoft Internet Explorer e Mozilla Firefox.

Per abilitare il modulo di scansione degli URL, eseguire le operazioni seguenti:

1. Aprire la finestra principaledell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, selezionare il componente **Anti-Virus Web** nella sezione **Protezione**.
4. Nella sezione **Livello di protezione** fare clic sul pulsante **Impostazioni** per il componente selezionato.
5. Nella finestra **Anti-Virus Web** visualizzata, sezione **Avanzate**, selezionare la casella **Contrassegna URL di phishing e sospetti in Microsoft Internet Explorer e Mozilla Firefox**.

Per creare l'elenco di indirizzi Web attendibili, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, selezionare il componente **Anti-Virus Web** nella sezione **Protezione**.
4. Nella sezione **Livello di protezione** fare clic sul pulsante **Impostazioni** per il componente selezionato.
5. Nella finestra **Anti-Virus Web** visualizzata fare clic sul pulsante **Impostazioni** nella sezione **Avanzate**.
6. Nella finestra **Barra degli strumenti di Kaspersky** visualizzata, selezionare l'opzione **In tutte le pagine Web** e fare clic sul pulsante **Esclusioni**.
7. Nella finestra **Elenco degli indirizzi Web attendibili** visualizzata, fare clic sul collegamento **Aggiungi**.

8. Nella finestra **Maschera per l'indirizzo (URL)** visualizzata, immettere un indirizzo Web attendibile o la relativa maschera.

Per creare l'elenco dei siti Web il cui contenuto deve essere sottoposto a scansione:

1. Aprire la finestra principale dell'applicazione e fare clic sulpulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, selezionare il componente **Anti-Virus Web** nella sezione **Protezione**.
4. Nella sezione **Livello di protezione** fare clic sul pulsante **Impostazioni** per il componente selezionato.
5. Nella finestra **Anti-Virus Web** visualizzata fare clic sul pulsante **Impostazioni** nella sezione **Avanzate**.
6. Nella finestra **Barra degli strumenti di Kaspersky** visualizzata, selezionare l'opzione **Nelle pagine Web selezionate** e fare clic sul pulsante **Seleziona**.
7. Nella finestra **Elenco degli indirizzi Web da verificare** visualizzata, fare clic sul collegamento **Aggiungi**.
8. Nella finestra **Maschera per l'indirizzo (URL)** visualizzata, immettere un indirizzo Web o una maschera che lo rappresenti.

UTILIZZO DELL'ANALISI EURISTICA

Il metodo euristico implica l'analisi delle attività eseguite dall'oggetto nel sistema. Se tali azioni sono tipiche di oggetti dannosi, è probabile che l'oggetto venga classificato come dannoso o sospetto. In questo modo è possibile rilevare le nuove minacce prima ancora che queste vengano studiate dagli analisti anti-virus. L'analisi euristica è abilitata per impostazione predefinita.

Protezione del computer informa l'utente della presenza di un oggetto nocivo rilevato in un messaggio. È necessario rispondere alla notifica elaborando ulteriormente il messaggio.

Inoltre, è possibile impostare il livello di dettaglio delle scansioni, **superficiale**, **media** o **approfondita**, spostando il cursore nella posizione selezionata.

Per abilitare/disabilitare l'analisi euristica e impostare il livello di dettaglio della scansione, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, selezionare il componente **Anti-Virus Web** nella sezione **Protezione**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra **Anti-Virus Web** visualizzata, sezione **Metodi di scansione**, selezionare/deselezionare la casella **Analisi euristica** e specificare il livello di dettaglio della scansione in basso.

OTTIMIZZAZIONE DELLA SCANSIONE

Per rilevare il codice nocivo in modo più efficiente, il componente Anti-Virus Web memorizza nel buffer frammenti di oggetti scaricati da Internet. Quando si utilizza questo metodo, un oggetto viene esaminato solo dopo essere stato scaricato completamente. Al termine del download viene sottoposto a scansione e, in base ai risultati ottenuti, viene restituito all'utente per poter essere utilizzato o bloccato.

La memorizzazione nel buffer comporta tuttavia un aumento dei tempi di elaborazione dell'oggetto e di conseguenza dei tempi di restituzione all'utente. Questo può causare problemi durante la copia e l'elaborazione di oggetti di grandi dimensioni in quanto è possibile che la connessione al client HTTP raggiunga il timeout.

Per risolvere questo problema, si consiglia di ridurre il tempo di memorizzazione nel buffer dei frammenti di oggetti Web scaricati da Internet. Allo scadere di questo limite temporale, l'utente riceve la parte scaricata e non esaminata del file. L'oggetto viene sottoposto a una scansione anti-virus solo dopo essere stato copiato completamente. Di conseguenza, il periodo di tempo necessario per trasferire l'oggetto all'utente si riduce, eliminando del tutto il problema della disconnessione. Inoltre, il livello di protezione per l'utilizzo di Internet non subisce variazioni.

Per impostazione predefinita, il tempo di memorizzazione nel buffer dei frammenti di file è limitato a un secondo. Aumentare questo valore o rimuovere il tempo limite di memorizzazione nel buffer migliora le scansioni anti-virus, ma rallenta l'accesso all'oggetto.

Per impostare un limite temporale per la memorizzazione nel buffer dei frammenti o per rimuoverlo, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, selezionare il componente **Anti-Virus Web** nella sezione **Protezione**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra **Anti-Virus Web** visualizzata, sezione **Ottimizzazione della scansione**, selezionare/deselezionare la casella **Limita il tempo di creazione del buffer dei frammenti** e immettere il valore temporale (in secondi) nel campo a destra.

RIPRISTINO DELLE IMPOSTAZIONI DI PROTEZIONE WEB PREDEFINITE

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

Per ripristinare le impostazioni predefinite di Anti-Virus Web, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, selezionare il componente **Anti-Virus Web** nella sezione **Protezione**.
4. Nella sezione **Livello di protezione**, fare clic sul pulsante **Livello predefinito** relativo al componente selezionato.

PROTEZIONE DEL TRAFFICO DEI PROGRAMMI DI MESSAGGISTICA ISTANTANEA

Oltre alle nuove funzionalità che rendono più semplice e agevole la navigazione in Internet, la grande diffusione dei client di messaggistica istantanea (d'ora in avanti definiti *client IM*), sta generando minacce potenziali alla protezione del computer. I messaggi che contengono URL di siti Web sospetti e quelli utilizzati da utenti malintenzionati per attacchi di phishing possono essere trasferiti tramite client IM. I programmi nocivi utilizzano infatti questo tipo di client per inviare messaggi di spamming e URL di programmi, o i programmi stessi, che rubano gli ID e le password degli utenti.

Il componente *Anti-Virus IM* è progettato per garantire il funzionamento dei client IM e per proteggere le informazioni che il computer riceve tramite protocolli IM.

Il prodotto protegge numerose applicazioni di messaggistica istantanea tra cui, ad esempio ICQ, MSN, AIM, Yahoo! Messenger, Jabber, Google Talk, Mail.Ru Agent e IRC.

Le applicazioni Yahoo! Messenger e Google Talk utilizzano il protocollo SSL. Per consentire ad Anti-Virus IM di eseguire la scansione del traffico di queste applicazioni, è necessario utilizzare la scansione delle connessioni crittografate (vedere pagina 167). A tale scopo, selezionare la casella **Scansione delle connessioni crittografate** nella sezione **Rete**.

Il traffico viene analizzato in base a una determinata combinazione di impostazioni. Se in un messaggio vengono rilevate minacce, Anti-Virus IM sostituisce il messaggio con un messaggio di errore per l'utente.

Il livello di protezione del traffico IM è determinato da un insieme di impostazioni. Tali impostazioni possono essere suddivise nei gruppi seguenti:

- impostazioni che determinano la creazione di un ambito di protezione;
- impostazioni che determinano i metodi di scansione.

Per modificare le impostazioni di Anti-Virus IM, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, selezionare il componente **Anti-Virus IM** nella sezione **Protezione**.
4. Apportare le modifiche desiderate alle impostazioni del componente selezionato.

IN QUESTA SEZIONE:

Algoritmo di funzionamento del componente 76

Creazione di un ambito di protezione 77

Selezione del metodo di scansione 77

Utilizzo dell'analisi euristica 78

ALGORITMO DI FUNZIONAMENTO DEL COMPONENTE

In Protezione del computer è incluso un componente, denominato *Anti-Virus IM*, che garantisce la scansione dei messaggi trasferiti tramite client di messaggistica istantanea per l'individuazione di oggetti pericolosi. Tale componente

viene caricato all'avvio del sistema operativo ed eseguito nella RAM del computer. Esamina tutti i messaggi in entrata e in uscita.

Per impostazione predefinita, la protezione del traffico dei client di messaggistica immediata viene garantita mediante l'algoritmo descritto di seguito:

1. Ogni messaggio ricevuto o inviato dall'utente viene intercettato dal componente.

2. Anti-Virus IM esegue la scansione del messaggio per rilevare eventuali oggetti pericolosi o URL elencati nei database degli indirizzi Web sospetti e/o di phishing. Se viene individuata una minaccia, il testo del messaggio viene sostituito con un messaggio di avviso per l'utente.

3. Se non vengono individuate minacce per la protezione, il messaggio viene reso disponibile per l'utente.

I file trasferiti tramite client IM vengono esaminati dal componente Anti-Virus File (vedere la sezione "Protezione del file system del computer" a pagina 52) quando si tenta di eseguirne il salvataggio.

CREAZIONE DI UN AMBITO DI PROTEZIONE

Per ambito di protezione si intende il tipo di messaggi da esaminare:

- **Messaggi in arrivo e in uscita**. Anti-Virus IM esamina i messaggi sia in entrata che in uscita per impostazione predefinita.

- **Solo messaggi in arrivo**. Se si è certi che i messaggi inviati non contengano oggetti pericolosi, selezionare questa impostazione. Anti-Virus IM esaminerà solo i messaggi in arrivo.

Per impostazione predefinita, Protezione del computer esamina sia i messaggi in arrivo che in uscita dei client IM.

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, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.

2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.

3. Nella finestra visualizzata, selezionare il componente **Anti-Virus IM** nella sezione **Protezione**.

4. Nella sezione **Ambito della protezione**, selezionare l'opzione **Solo messaggi in arrivo** relativa al componente selezionato.

SELEZIONE DEL METODO DI SCANSIONE

I metodi di scansione consistono nella scansione degli URL nei messaggi inviati dai client di messaggistica istantanea per verificare che non siano inclusi nell'elenco di indirizzi Web sospetti e/o nell'elenco di indirizzi Web di phishing:

- **Confronta gli URL con il database degli indirizzi sospetti**. Anti-Virus IM esegue una scansione dei collegamenti all'interno dei messaggi per verificare se sono inclusi nella blacklist.

- **Confronta gli URL con il database degli indirizzi di phishing**. I database di Protezione del computer includono tutti i siti attualmente noti utilizzati per gli attacchi di phishing. Kaspersky Lab arricchisce questo elenco con gli indirizzi ottenuti da Anti-Phishing Working Group, un'organizzazione internazionale. L'elenco viene aggiornato in seguito all'aggiornamento dei database di Protezione del computer.

- *Per eseguire la scansione dei collegamenti nei messaggi utilizzando il database di indirizzi Web sospetti, eseguire le operazioni seguenti:*

  1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
  2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
  3. Nella finestra visualizzata, selezionare il componente **Anti-Virus IM** nella sezione **Protezione**.
  4. Nella sezione **Metodi di scansione**, selezionare la casella **Confronta gli URL con il database degli indirizzi sospetti** relativa al componente selezionato.

- *Per eseguire la scansione dei collegamenti nei messaggi utilizzando il database di indirizzi Web di phishing, eseguire le operazioni seguenti:*

  1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
  2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
  3. Nella finestra visualizzata, selezionare il componente **Anti-Virus IM** nella sezione **Protezione**.
  4. Nella sezione **Metodi di scansione**, selezionare la casella **Confronta gli URL con il database degli indirizzi di phishing** relativa al componente selezionato.

UTILIZZO DELL'ANALISI EURISTICA

Il metodo euristico implica l'analisi delle attività eseguite dall'oggetto nel sistema. A tale scopo, qualsiasi script incluso nel messaggio di un client IM viene eseguito nell'ambiente protetto. Se l'attività dello script è tipica di oggetti nocivi, è probabile che l'oggetto venga classificato come nocivo o sospetto. L'analisi euristica è abilitata per impostazione predefinita.

Protezione del computer informa l'utente della presenza di un oggetto nocivo rilevato in un messaggio.

Inoltre, è possibile impostare il livello di dettaglio delle scansioni, **superficiale**, **media** o **approfondita**, spostando il cursore nella posizione selezionata.

Per abilitare/disabilitare l'analisi euristica e impostare il livello di dettaglio della scansione, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, selezionare il componente **Anti-Virus IM** nella sezione **Protezione**.
4. Nella sezione **Metodi di scansione**, selezionare/deselezionare la casella **Analisi euristica** e impostare il livello di dettaglio della scansione in basso per il componente selezionato.

CONTROLLO APPLICAZIONI

Tutte le applicazioni possono essere suddivise in tre gruppi in base ai fattori del sistema di protezione:

- *Sicure*. Questo gruppo include applicazioni sviluppate da fornitori noti e dotate di firma digitale. È possibile consentire a tali applicazioni di eseguire qualsiasi azione nel sistema.
- *Pericolose*. Questo gruppo comprende le minacce attualmente note. Le attività delle applicazioni incluse in questo gruppo devono essere bloccate.
- *Sconosciute*. Questo gruppo può comprendere le applicazioni create da sviluppatori sconosciuti, sprovviste di firma digitale. Tali applicazioni potrebbero danneggiare il sistema. È possibile decidere se sia sicuro utilizzare queste applicazioni solo dopo averle eseguite e averne analizzato il comportamento. Prima di prendere una decisione in relazione all'attendibilità o meno di un'applicazione, è consigliabile limitarne l'accesso alle risorse del sistema.

Il componente Controllo Applicazioni registra le azioni eseguite dalle applicazioni nel sistema e ne gestisce le attività, in base al gruppo a cui appartengono (vedere la sezione "Gruppi di applicazioni" a pagina 82). Per ogni gruppo di applicazioni viene definito un insieme di regole (vedere la sezione "Regole di Controllo Applicazioni" a pagina 85). Tali regole gestiscono l'accesso dell'applicazione a varie risorse, quali:

- file e cartelle;
- chiavi del Registro di sistema;
- indirizzi di rete;
- ambiente di esecuzione.

Quando un'applicazione accede a una risorsa, il componente controlla se dispone dei diritti di accesso necessari ed esegue l'azione determinata dalla regola.

Per modificare le impostazioni di Controllo Applicazioni, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Controllo Applicazioni**.
4. Apportare le modifiche desiderate alle impostazioni per il componente selezionato.

Inoltre:

1. Aprire la finestra principale dell'applicazione e selezionare la sezione **Controllo Applicazioni**.
2. Nella parte destra della finestra, fare clic sul collegamento **Attività applicazioni**.
3. Nella finestra **Controllo delle attività delle applicazioni** visualizzata, apportare le modifiche necessarie.

IN QUESTA SEZIONE:

Algoritmo di funzionamento del componente 81

Creazione di un ambito di protezione 83

Regole di Controllo Applicazioni 85

ALGORITMO DI FUNZIONAMENTO DEL COMPONENTE

Al primo avvio, Controllo Applicazioni analizza un'applicazione utilizzando l'algoritmo seguente:

1. Esegue la scansione anti-virus dell'applicazione.

2. Verifica la firma digitale dell'applicazione. Se la firma digitale viene confermata, l'applicazione verrà inclusa nel gruppo **Attendibili**. Se l'applicazione non presenta una firma digitale (o se la firma digitale è danneggiata oppure inclusa nell'elenco Bloccati), il componente procederà al passaggio successivo.

3. Cerca un record dell'applicazione avviata nel database interno delle applicazioni note incluso nel pacchetto di installazione di Protezione del computer. Se nel database viene rilevato un record relativo all'applicazione avviata, questo verrà incluso nel gruppo corrispondente. In caso contrario, il componente procederà al passaggio successivo.

4. Invia informazioni relative al file eseguibile dell'applicazione al database delle applicazioni note memorizzato in un server di Kaspersky Lab. Se il database contiene già un record correlato alle informazioni inviate, l'applicazione verrà inclusa nel gruppo corrispondente. Se il database non è accessibile (ad esempio non è presente una connessione a Internet attiva), il componente procederà al passaggio successivo.

5. Calcola la classificazione della pericolosità dell'applicazione mediante l'analisi euristica. Le applicazioni con una valutazione di rischio bassa vengono inserite nel gruppo **Restrizione bassa**. Se la valutazione di rischio dell'applicazione è alta, Protezione del computer informa l'utente e offre la possibilità di selezionare un gruppo in cui inserire l'applicazione.

Al termine delle scansioni, la decisione finale sull'azione da intraprendere viene comunicata mediante una notifica. Per impostazione predefinita, la notifica è disabilitata.

Quando l'applicazione viene riavviata, Controllo Applicazioni ne verifica l'integrità. Se l'applicazione non è stata modificata, il componente vi applica la regola esistente. Se l'applicazione è stata modificata, Controllo Applicazioni la analizza utilizzando l'algoritmo descritto prima.

VEDERE ANCHE:

Privilegi di eredità 81

Classificazione della pericolosità 82

Gruppi di applicazioni 82

Sequenza di avvio dell'applicazione 83

PRIVILEGI DI EREDITA

Un aspetto importante del componente Controllo Applicazioni è il meccanismo di *ereditarietà dei privilegi di accesso*. Tale meccanismo impedisce l'utilizzo delle applicazioni attendibili da parte di un'applicazione non attendibile o di un'applicazione con diritti limitati per eseguire azioni che richiedono determinati privilegi.

Quando le applicazioni cercano di ottenere l'accesso a una risorsa monitorata, Controllo Applicazioni analizza i diritti di tutti i processi principali dell'applicazione e li confronta con i diritti richiesti per accedere a questa risorsa. Viene quindi osservata la *regola della priorità minima*: durante il confronto tra i privilegi di accesso dell'applicazione e quelli del processo principale, i privilegi di accesso con una priorità minima vengono applicati all'attività dell'applicazione.

Priorità dei privilegi di accesso:

1. **Consenti**. I dati dei privilegi di accesso hanno la priorità più elevata.

2. **Chiedi di scegliere un'azione**.

3. **Blocca**. I dati dei privilegi di accesso hanno la priorità più bassa.

Esempio:

Un Trojan tenta di utilizzare *regedit.exe* per modificare il Registro di sistema di Microsoft Windows. La regola per i programmi Trojan imposta l'azione **Blocca** come reazione al tentativo di accesso al Registro di sistema, mentre la regola per *regedit.exe* imposta l'azione **Consenti** .

Di conseguenza, le attività del file *regedit.exe* eseguite dal programma Trojan verranno bloccate in quanto i diritti di *regedit.exe* saranno ereditati dal processo principale. Questo evento attiverà la regola della priorità minima e l'azione verrà bloccata sebbene il programma *regedit.exe* disponga dei diritti necessari per consentirla.

Se le attività dell'applicazione vengono bloccate perché i diritti di un processo principale sono insufficienti, è possibile modificare le regole (vedere la sezione "Modifica di una regola di applicazione" a pagina 87).

È necessario modificare i diritti di un processo principale solo se si ha la certezza assoluta che le attività del processo non minaccino la sicurezza del sistema.

VEDERE ANCHE:

Sequenza di avvio dell'applicazione 83

CLASSIFICAZIONE DELLA PERICOLOSITÀ

Controllo Applicazioni calcola la valutazione della pericolosità per ciascuna applicazione eseguita sul computer in uso mediante l'analisi euristica. La *classificazione della pericolosità* è un indicatore del livello di rischio che l'applicazione costituisce per il sistema e viene calcolata in base a criteri di due tipi:

- statici: questi criteri includono informazioni sul file eseguibile dell'applicazione, incluse la data di creazione, la dimensione e così via;

- dinamici: questi criteri vengono utilizzati durante la simulazione del funzionamento dell'applicazione in un ambiente virtuale, mediante l'analisi delle chiamate dell'applicazione alle funzioni del sistema. L'analisi di tali criteri consente di rilevare un tipico comportamento di malware.

Controllo Applicazioni divide le applicazioni in gruppi in base ai valori della classificazione (vedere la sezione "Gruppi di applicazioni" a pagina 82). Più bassa è la classificazione della pericolosità, più operazioni potrà eseguire l'applicazione nel sistema.

GRUPPI DI APPLICAZIONI

Tutte le applicazioni dell'utente eseguite sul computer vengono suddivise da Controllo Applicazioni in gruppi in base al livello di pericolo per il sistema che, a sua volta, influisce sui privilegi di accesso dell'applicazione alle risorse del sistema.

Sono disponibili quattro gruppi predefiniti di applicazioni:

- **Attendibili**. Applicazioni con firma digitale di fornitori attendibili oppure applicazioni registrate nel database delle applicazioni attendibili. Tali applicazioni non prevedono l'applicazione di restrizioni alle azioni eseguite nel sistema. Le attività di queste applicazioni vengono monitorate da Difesa Proattiva e da Anti-Virus File.

- **Restrizione bassa**. Applicazioni prive di firma digitale di un fornitore attendibile, che non sono elencate nel database delle applicazioni attendibili. Queste applicazioni, tuttavia, hanno ricevuto un valore basso nella classificazione della pericolosità (a pagina 82). Possono eseguire alcune operazioni, quali l'accesso ad altri processi, il controllo del sistema e l'accesso a reti nascoste. Per gran parte delle operazioni è richiesto il permesso dell'utente.

- **Restrizione alta**. Applicazioni prive di firma digitale, che non sono elencate nel database delle applicazioni attendibili. Queste applicazioni hanno un valore alto di classificazione della pericolosità. Le applicazioni di questo gruppo richiedono il permesso dell'utente per la maggior parte delle azioni che influenzano il sistema. Per tali applicazioni alcune operazioni non sono consentite.

- **Non attendibili**. Applicazioni prive di firma digitale, che non sono elencate nel database delle applicazioni attendibili. Queste applicazioni hanno un valore di classificazione della pericolosità molto alto. Controllo Applicazioni blocca tutte le azioni eseguite da tali applicazioni.

Alle applicazioni inserite da Controllo Applicazioni in un determinato gruppo viene assegnato lo stato corrispondente. Le applicazioni ereditano i diritti di accesso alle risorse dalla regola del gruppo (vedere la sezione "Regole di Controllo Applicazioni" a pagina 85).

Gli esperti di Kaspersky Lab consigliano di non spostare le applicazioni da un gruppo all'altro. Se necessario, modificare i diritti dell'applicazione per l'accesso a determinate risorse del sistema (vedere la sezione "Modifica di una regola di applicazione" a pagina 87).

SEQUENZA DI AVVIO DELL'APPLICAZIONE.

L'avvio dell'applicazione può essere effettuato dall'utente o da un'altra applicazione in esecuzione.

Se l'avvio viene effettuato da un'altra applicazione, viene creata una procedura di avvio che include programmi principali e secondari. Le procedure di avvio possono essere salvate.

Durante il salvataggio di una procedura di avvio, ogni programma incluso al suo interno resta nel relativo gruppo.

VEDERE ANCHE:

Privilegi di eredità 81

CREAZIONE DI UN AMBITO DI PROTEZIONE

Controllo Applicazioni gestisce i diritti delle applicazioni utente di eseguire azioni sulle categorie di risorse seguenti:

Sistema operativo. Tale categoria include:

- chiavi di registro contenenti impostazioni di avvio;
- chiavi di registro contenenti impostazioni per l'utilizzo di Internet;
- chiavi di registro che influiscono sulla protezione del sistema;
- chiavi di registro contenenti impostazioni dei servizi di sistema;
- file e cartelle di sistema;
- cartelle di avvio.

Kaspersky Lab ha creato un elenco di impostazioni e risorse del sistema operativo che devono essere sempre protette mediante Protezione del computer. Tale elenco non può essere modificato. È tuttavia possibile rinunciare al monitoraggio di qualsiasi oggetto del sistema operativo incluso nella categoria selezionata, nonché aggiungere elementi all'elenco.

Dati identità. Tale categoria include:

- File dell'utente (cartella Documenti, file cookie, informazioni sulle attività dell'utente);

- File di registro, cartelle e chiavi contenenti impostazioni e dati importanti delle applicazioni utilizzate più di frequente: browser Internet, programmi di gestione file, client di posta, client IM e portafogli elettronici.

Kaspersky Lab ha creato un elenco di categorie di risorse che devono essere sempre protette mediante Protezione del computer. Tale elenco non può essere modificato. È tuttavia possibile rinunciare al monitoraggio di una categoria di risorse, nonché aggiungere altre categorie all'elenco.

Per aggiungere voci all'elenco di elementi dati di identità da proteggere, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Controllo Applicazioni**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra visualizzata, nella scheda **Dati identità**, elenco a discesa **Categoria**, selezionare la categoria desiderata di oggetti dati di personali e fare clic sul collegamento **Aggiungi** un oggetto o sul collegamento **Aggiungi una categoria** se si desidera aggiungere una nuova categoria di risorse da proteggere e immetterne il nome nella finestra visualizzata.
6. Nella finestra **Risorsa utente** visualizzata fare clic sul pulsante **Sfoglia** e specificare i dati richiesti, a seconda della risorsa da aggiungere:
   - **File o cartella**. Nella finestra **Seleziona un file o una cartella** visualizzata specificare un file o una cartella.
   - **Chiave di registro**. Nella finestra **Specificare un oggetto del registro** visualizzata specificare la chiave di registro da proteggere.
   - **Servizio di rete**. Nella finestra **Servizio di rete visualizzata**, specificare le impostazioni per la connessione di rete monitorata (vedere la sezione "Configurazione delle impostazioni del servizio di rete" a pagina 99).
   - **Indirizzi IP**. Specificare l'intervallo protetto di indirizzi nella finestra **Indirizzi di rete** visualizzata.

   Dopo aver aggiunto la risorsa all'ambito di protezione, è possibile modificarla o eliminarla utilizzando i collegamenti corrispondenti nella parte inferiore della scheda. Per escludere la risorsa dall'ambito di protezione, deselezionare la casella ☑ accanto a essa.

Per aggiungere voci all'elenco di impostazioni e risorse del sistema operativo da proteggere, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Controllo Applicazioni**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra visualizzata, nella scheda **Sistema operativo**, elenco a discesa **Categoria**, selezionare la categoria desiderata di oggetti del sistema operativo e fare clic sul collegamento **Aggiungi**.
6. Nella finestra **Risorsa utente** visualizzata fare clic sul pulsante **Sfoglia** e specificare i dati richiesti, a seconda della risorsa da aggiungere:
   - **File o cartella**. Nella finestra **Seleziona un file o una cartella** visualizzata specificare un file o una cartella.
   - **Chiave di registro**. Nella finestra **Specificare un oggetto del registro** visualizzata specificare la chiave di registro da proteggere.

Dopo aver aggiunto la risorsa all'ambito di protezione, è possibile modificarla o eliminarla utilizzando i collegamenti corrispondenti nella parte inferiore della scheda. Per escludere la risorsa dall'ambito di protezione, deselezionare la casella accanto a essa.

REGOLE DI CONTROLLO APPLICAZIONI

Una regola è un insieme di reazioni di Controllo Applicazioni alle azioni dell'applicazione sulle risorse monitorate (vedere la sezione "Creazione di un ambito di protezione" a pagina 83).

Tra le possibili reazioni del componente sono incluse:

- **Eredita**. Controllo Applicazioni applica all'attività di un'applicazione l'insieme di regole per il gruppo cui questa appartiene. Si tratta dell'impostazione predefinita per la reazione.
- **Consenti**. Controllo Applicazioni consente a un'applicazione di eseguire un'azione.
- **Nega**. Controllo Applicazioni non consente a un'applicazione di eseguire un'azione.
- **Chiedi di scegliere un'azione**. Controllo Applicazioni informa l'utente che l'applicazione sta cercando di eseguire un'azione e richiede all'utente di eseguire altre azioni.
- **Registra eventi**. Le informazioni sull'attività di un'applicazione e la reazione di Controllo Applicazioni verranno registrate in un rapporto. L'aggiunta di informazioni al rapporto può essere utilizzata in combinazione con altre azioni del componente.

Per impostazione predefinita, un'applicazione eredita i diritti di accesso dal gruppo al quale appartiene. È possibile modificare una regola per l'applicazione. In questo caso, le impostazioni della regola dell'applicazione avranno priorità più alta rispetto a quelle ereditate dal gruppo al quale appartiene l'applicazione.

VEDERE ANCHE:

Inserimento di applicazioni in gruppi 85

Modifica del tempo utilizzato per determinare lo stato dell'applicazione 86

Modifica di una regola di applicazione 87

Modifica di una regola per un gruppo di applicazioni 87

Creazione di una regola di rete per l'applicazione 87

Configurazione delle esclusioni 88

Eliminazione delle regole per le applicazioni 88

INSERIMENTO DI APPLICAZIONI IN GRUPPI

Le applicazioni incluse dal componente Controllo Applicazioni nel gruppo **Attendibili** (vedere la sezione "Gruppi di applicazioni" a pagina 82) non costituiscono una minaccia per il sistema.

È possibile utilizzare l'opzione che consente di specificare l'intervallo di applicazioni attendibili, le cui attività non verranno esaminate da Controllo Applicazioni. Le applicazioni attendibili possono essere applicazioni con una firma digitale o incluse nel database di Kaspersky Security Network.

Per altre applicazioni, che non rientrano nel gruppo attendibile, è possibile utilizzare l'analisi euristica per determinare un gruppo o specificare un determinato gruppo in cui l'applicazione verrà aggiunta automaticamente.

- *Se si desidera che Controllo Applicazioni consideri le applicazioni con una firma digitale e/o contenute nel database di Kaspersky Security Network come attendibili e non ne notifichi l'attività, eseguire le operazioni seguenti:*

  1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
  2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
  3. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Controllo Applicazioni**.
  4. Nella sezione **Applicazioni attendibili**, selezionare la casella **Applicazioni con firma digitale** e/o la casella **Applicazioni del database Kaspersky Security Network** relativa al componente selezionato.

- *Se si desidera che Controllo Applicazioni utilizzi l'analisi euristica per l'allocazione di applicazioni non attendibili nei gruppi:*

  1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
  2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
  3. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Controllo Applicazioni**.
  4. Selezionare l'opzione **Usa l'analisi euristica per definire il gruppo** nella sezione **Applicazioni attendibili**. Quando lo stato viene assegnato, l'applicazione verrà inserita nel gruppo corrispondente.

- *Se si desidera che Controllo Applicazioni assegni lo stato specificato automaticamente durante l'allocazione di applicazioni non attendibili ai gruppi:*

  1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
  2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
  3. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Controllo Applicazioni**.
  4. Selezionare l'opzione **Assegna il seguente gruppo automaticamente** nella sezione **Applicazioni attendibili**. Le applicazioni verranno distribuite nei gruppi corrispondenti.

MODIFICA DEL TEMPO UTILIZZATO PER DETERMINARE LO STATO DELL'APPLICAZIONE

Se l'analisi euristica viene utilizzata per determinare lo stato dell'applicazione, Controllo Applicazioni analizza il programma per 30 secondi per impostazione predefinita. Se la classificazione della pericolosità non è stata calcolata durante questo tempo, l'applicazione riceve lo stato *Restrizione bassa* e viene inserita nel gruppo corrispondente.

Il calcolo della classificazione della pericolosità continua in background. Dopo che l'applicazione è stata studiata con l'ausilio dell'analizzatore euristico, riceve lo stato in base alla classificazione della pericolosità assegnata e viene inserita nel gruppo corrispondente.

È possibile modificare il tempo allocato per l'analisi delle applicazioni. Se si ha la certezza che tutte le applicazioni avviate nel computer non costituiscano alcuna minaccia per la sicurezza, è possibile ridurre il tempo da dedicare all'analisi. Se, al contrario, si sta installando un componente software e non si ha la certezza che sia sicuro, è consigliabile aumentare il tempo da dedicare all'analisi.

- *Per modificare la quantità di tempo assegnata al controllo delle applicazioni sconosciute:*

  1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
  2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
  3. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Controllo Applicazioni**.

4. Per il componente selezionato, impostare il valore per il parametro **Tempo limite per determinare il gruppo dell'applicazione** nella sezione **Avanzate**.

MODIFICA DI UNA REGOLA DI APPLICAZIONE

Quando un'applicazione viene avviata per la prima volta, Controllo Applicazioni ne determina lo stato e la include in un determinato gruppo. Quindi, il componente registra le azioni eseguite dall'applicazione nel sistema e ne gestisce le attività in base al relativo gruppo di appartenenza (vedere la sezione "Gruppi di applicazioni" a pagina 82). Quando un'applicazione accede a una risorsa, il componente controlla se dispone dei diritti di accesso necessari ed esegue l'azione determinata dalla regola. È possibile modificare la regola creata per l'applicazione quando se ne determina lo stato e si provvede a includerla nel gruppo corrispondente.

Per modificare una regola dell'applicazione, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, selezionare la sezione **Controllo Applicazioni**.
3. Nella finestra visualizzata, nella sezione **Controllo Applicazioni**, fare clic sul collegamento **Attività applicazioni**.
4. Nella finestra **Controllo delle attività delle applicazioni** visualizzata, nell'elenco a discesa **Categoria**, selezionare la categoria desiderata.
5. Nella colonna **Stato**, fare clic sul collegamento con lo stato dell'applicazione richiesta.
6. Nel menu visualizzato, selezionare la voce **Impostazioni personalizzate**.
7. Nella finestra visualizzata, nella scheda **Regole**, modificare le regole di accesso per la categoria di risorse richiesta.

MODIFICA DI UNA REGOLA PER UN GRUPPO DI APPLICAZIONI

Quando un'applicazione viene avviata per la prima volta, Controllo Applicazioni ne determina lo stato e la include in un determinato gruppo. Quindi, il componente registra le azioni eseguite dall'applicazione nel sistema e ne gestisce le attività in base al relativo gruppo di appartenenza (vedere la sezione "Gruppi di applicazioni" a pagina 82). È possibile modificare la regola per il gruppo, se necessario.

Per modificare una regola per il gruppo, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Controllo Applicazioni**.
4. Nella sezione **Regole per i gruppi di applicazioni**, fare clic sul pulsante **Configurazione regole** per il componente selezionato.
5. Nella finestra **Impostazioni del Controllo Applicazion**i visualizzata, selezionare il gruppo desiderato.
6. Nella finestra visualizzata, nella scheda **Regole**, modificare le regole di accesso per la categoria di risorse richiesta.

CREAZIONE DI UNA REGOLA DI RETE PER L'APPLICAZIONE

Per impostazione predefinita, dopo il primo avvio di un'applicazione, Controllo Applicazioni la include in uno dei gruppi predefiniti. Un gruppo di regole gestisce l'accesso di un'applicazione a una rete con uno stato specificato. Per elaborare l'accesso di un'applicazione a determinati servizi di rete in modo speciale, è possibile creare una regola di rete.

Per creare una regola che controlla l'attività di rete dell'applicazione, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, selezionare la sezione **Controllo Applicazioni**.
3. Nella finestra visualizzata, nella sezione **Controllo Applicazioni**, fare clic sul collegamento **Attività applicazioni**.
4. Nella finestra **Controllo delle attività delle applicazioni** visualizzata, nell'elenco a discesa **Categoria**, selezionare la categoria desiderata.
5. Nella colonna **Stato**, fare clic sul collegamento con lo stato dell'applicazione richiesta.
6. Nel menu visualizzato, selezionare la voce **Impostazioni personalizzate**.
7. Nella finestra visualizzata, nella scheda **Regole**, selezionare la categoria **Regole di rete** nell'elenco a discesa e fare clic sul collegamento **Aggiungi**.
8. Nella finestra **Regola di rete** visualizzata, configurare la regola per i pacchetti.
9. Assegnare la priorità per la regola creata.

CONFIGURAZIONE DELLE ESCLUSIONI

Quando si crea una regola predefinita per un'applicazione, Protezione del computer monitorerà tutte le azioni dell'applicazione utente, tra cui l'accesso a file e cartelle, l'accesso all'ambiente di esecuzione e l'accesso alla rete. È possibile escludere determinate azioni dalla scansione.

Per escludere alcune azioni delle applicazioni utente dalla scansione:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, selezionare la sezione **Controllo Applicazioni**.
3. Nella finestra visualizzata, nella sezione **Controllo Applicazioni**, fare clic sul collegamento **Attività applicazioni**.
4. Nella finestra **Controllo delle attività delle applicazioni** visualizzata, nell'elenco a discesa **Categoria**, selezionare la categoria desiderata.
5. Nella colonna **Stato**, fare clic sul collegamento con lo stato dell'applicazione richiesta.
6. Nel menu visualizzato, selezionare la voce **Impostazioni personalizzate**.
7. Nella finestra visualizzata, nella scheda **Esclusioni**, selezionare le caselle che corrispondono alle azioni da escludere. Quando si esclude la scansione del traffico di rete dell'applicazione, configurare ulteriori impostazioni di esclusione.

   Tutte le esclusioni create nelle regole per le applicazioni utente sono accessibili nella sezione **Minacce ed Esclusioni** della finestra delle impostazioni dell'applicazione.

ELIMINAZIONE DELLE REGOLE PER LE APPLICAZIONI

È possibile utilizzare l'opzione di eliminazione delle regole per le applicazioni non avviate per diverso tempo.

Per eliminare le regole per le applicazioni non avviate per un periodo di tempo specificato:

1. Aprire la finestra principale dell'applicazione e fare clic sulpulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Controllo Applicazioni**.
4. Selezionare la casella **Elimina le regole per le applicazioni rimaste inattive per più di** relativa al componente selezionato nella sezione **Avanzate** e specificare il numero di giorni necessari nel campo a destra.

MODALITA PROTETTA DI ESECUZIONE DELLE APPLICAZIONI

La modalità protetta di esecuzione delle applicazioni non è disponibile nei computer che eseguono Microsoft Windows XP x64.

Per garantire la massima protezione degli oggetti del sistema operativo e dei dati personali degli utenti, Kaspersky Lab ha reso possibile eseguire applicazioni di terze parti in un ambiente virtuale protetto denominato *Modalità Protetta*.

La modalità protetta è consigliata per eseguire applicazioni la cui autenticità non è evidente. In questo modo si eviteranno modifiche agli oggetti del sistema operativo che potrebbero portare a un funzionamento non corretto.

Le funzionalità di alcune applicazioni in modalità protetta possono risultare ridotte in computer che eseguono Microsoft Windows Vista x64 e Microsoft Windows 7 x64. Se tali applicazioni vengono avviate, viene visualizzato il messaggio corrispondente, se sono state configurate le notifiche relative all'evento per cui le funzionalità dell'**applicazione sono limitate in modalità protetta**.

L'esecuzione dei browser Internet in un ambiente protetto garantisce protezione durante la visualizzazione delle risorse Web, inclusa la protezione da malware che si introduce nel computer e la protezione dei dati utente da tentativi di modifica ed eliminazione non autorizzati, nonché la possibilità di eliminare tutti gli oggetti accumulati durante la sessione Internet: file temporanei, cookie, cronologia delle pagine Web visitate e così via. Microsoft Internet Explorer è incluso per impostazione predefinita nell'elenco di applicazioni in esecuzione in modalità protetta.

L'Esecuzione di un'applicazione in modalità protetta viene eseguita in base alla modalità selezionata. È disponibile l'opzione per la creazione di un collegamento che consente di avviare rapidamente le applicazioni in modalità protetta.

Per rendere disponibili i file salvati o modificati in modalità protetta quando ci si trova in modalità standard, è necessario utilizzare la Cartella condivisa in Modalità Protetta creata esclusivamente per tali file e disponibile sia in modalità protetta che in modalità standard. Quando si cancellano dati in Modalità Protetta (vedere pagina 93), i file memorizzati in questa cartella non vengono eliminati.

È consigliabile utilizzare la modalità standard di Microsoft Windows per installare le applicazioni con cui si desidera lavorare in futuro in modalità protetta.

IN QUESTA SEZIONE:

Esecuzione di un'applicazione in Modalità Protetta 90

Creazione di un collegamento per l'esecuzione dei programmi 90

Creazione dell'elenco di applicazioni in esecuzione in modalità protetta 91

Selezione della modalità: esecuzione di un'applicazione 91

Selezione della modalità: cancellazione dei dati in modalità protetta 92

Utilizzo di una cartella condivisa 92

Cancellazione dei dati in modalità protetta 93

ESECUZIONE DI UN'APPLICAZIONE IN MODALITA PROTETTA

Se l'opzione **Esegui sempre in modalità protetta** non è abilitata per l'applicazione, questa può essere eseguita in modalità protetta utilizzando uno dei metodi seguenti:

- dal menu di scelta rapida di Microsoft Windows;
- dalla finestra principale di Protezione del computer (vedere la sezione "Protezione del computer" a pagina 45);
- utilizzando un collegamento esistente (vedere la sezione "Creazione di un collegamento per l'esecuzione dei programmi" a pagina 90).

Se l'opzione **Esegui sempre in modalità protetta** è selezionata per l'applicazione, questa verrà avviata in modalità protetta indipendentemente dalla modalità di esecuzione.

Le applicazioni in esecuzione in modalità protetta sono segnalate da una cornice verde intorno alla relativa finestra e risultano evidenziate in verde nell'elenco delle applicazioni monitorate da Controllo Applicazioni (vedere la sezione "Controllo Applicazioni" a pagina 80).

Per eseguire un'applicazione in modalità protetta utilizzando un collegamento, eseguire le operazioni seguenti:

1. Aprire la cartella in cui è stato creato il collegamento.
2. Avviare l'applicazione facendo doppio clic sul relativo collegamento.

Per eseguire un'applicazione in modalità protetta dalla finestra principale di Protezione del computer, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, selezionare la sezione **Controllo Applicazioni**.
3. Nella parte inferiore della finestra, selezionare l'icona dell'applicazione desiderata.
4. Fare doppio clic sull'icona per eseguire l'applicazione o aprire il menu di scelta rapida e scegliere la voce **Esegui**.

Per eseguire un'applicazione in modalità protetta dal menu di scelta rapida di Microsoft Windows, eseguire le operazioni seguenti:

1. Fare clic con il pulsante destro del mouse sul nome dell'oggetto selezionato del file eseguibile o del collegamento dell'applicazione.
2. Nel menu visualizzato, selezionare la voce **Esecuzione in Modalità Protetta**.

CREAZIONE DI UN COLLEGAMENTO PER L'ESECUZIONE DEI PROGRAMMI

Per eseguire le applicazioni rapidamente in modalità protetta, Protezione del computer consente la creazione di collegamenti. Grazie ai collegamenti l'utente può eseguire l'applicazione desiderata in modalità protetta senza aprire la finestra principale dell'applicazione o il menu di scelta rapida di Microsoft Windows.

Per creare un collegamento in modo da eseguire un'applicazione in modalità protetta, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, selezionare la sezione **Controllo Applicazioni**.

3. Nella parte inferiore della finestra, nel campo **Applicazioni in Modalità Protetta**, selezionare l'icona dell'applicazione desiderata.

4. Facendo clic con il pulsante destro del mouse, aprire il menu di scelta rapida e utilizzare la voce **Crea collegamento**.

5. Nella finestra che viene visualizzata specificare il percorso in cui salvare il collegamento. Per impostazione predefinita, verrà creato un collegamento sul *Desktop* dell'utente corrente, con il nome corrispondente al processo dell'applicazione.

CREAZIONE DELL'ELENCO DI APPLICAZIONI IN ESECUZIONE IN MODALITA PROTETTA

È possibile creare un elenco di applicazioni in esecuzione in modalità protetta nella finestra principale dell'applicazione. L'elenco viene visualizzato nella sezione **Controllo Applicazioni**.

Se si aggiunge all'elenco un'applicazione che può essere utilizzata in più istanze, come Windows Internet Explorer, tutte le nuove istanze verranno eseguite in modalità protetta. Se si aggiunge all'elenco un'applicazione che può essere utilizzata in una sola istanza, questa dovrà essere riavviata dopo l'aggiunta.

Per aggiungere un'applicazione all'elenco delle applicazioni in esecuzione in modalità protetta, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.

2. Nella finestra visualizzata, selezionare la sezione **Controllo Applicazioni**.

3. Nella parte inferiore della finestra, nel campo **Applicazioni in Modalità Protetta**, fare clic sul collegamento **Aggiungi**.

4. Nel menu visualizzato, selezionare l'applicazione desiderata. Quando si seleziona la voce **Sfoglia**, viene aperta una finestra nella quale è necessario specificare il percorso di un file eseguibile. Quando si seleziona la voce **Applicazioni**, viene aperto l'elenco di applicazioni attualmente in esecuzione. L'icona dell'applicazione selezionata viene aggiunta al campo.

   Per eliminare un'applicazione dall'elenco delle applicazioni in esecuzione in modalità protetta, selezionarla nell'elenco e fare clic sul collegamento **Elimina**.

SELEZIONE DELLA MODALITÀ: ESECUZIONE DI UN'APPLICAZIONE

Per impostazione predefinita, è possibile eseguire tutte le applicazioni installate nel computer sia in modalità standard che in modalità protetta. Quando si aggiunge un'applicazione nell'elenco di applicazioni eseguite in modalità protetta, è possibile abilitare l'opzione **Esegui sempre in modalità protetta**. In questo modo l'applicazione verrà eseguita in modalità protetta indipendentemente dalla modalità di esecuzione, sia che si utilizzino gli strumenti standard di Microsoft Windows, sia che si utilizzino gli strumenti di Protezione del computer.

È consigliabile non abilitare l'opzione **Esegui sempre in modalità protetta** per le utilità e le applicazioni del sistema onde evitare problemi di funzionamento del sistema operativo.

Per eseguire un'applicazione solo in modalità protetta indipendentemente dalla modalità di esecuzione, eseguire le operazioni seguenti:

1. Aprire la finestra principaledell'applicazione e fare clic sul pulsante **Protezione del computer**.

2. Nella finestra visualizzata, selezionare la sezione **Controllo Applicazioni**.

3. Nella parte inferiore della finestra, selezionare l'icona dell'applicazione desiderata.

4. Aprire il menu di scelta rapida facendo clic con il pulsante destro del mouse.

5. Selezionare la voce **Esegui sempre in modalità protetta**. Accanto alla voce di menu verrà visualizzato il riquadro .

   Per consentire l'esecuzione dell'applicazione in modalità standard, selezionare di nuovo la voce.

SELEZIONE DELLA MODALITA: CANCELLAZIONE DEI DATI IN MODALITA PROTETTA

Se un'applicazione viene eseguita in modalità protetta, tutte le modifiche apportate dall'applicazione verranno eseguite solo nell'ambito di tale modalità. Per impostazione predefinita, al successivo avvio dell'applicazione, tutte le modifiche apportate e i file salvati saranno disponibili durante la sessione in modalità protetta.

Se i dati in Modalità Protetta non sono più necessari, è possibile cancellarli (vedere pagina 93).

Se alla successiva esecuzione in modalità protetta non si desidera rendere disponibili per un'applicazione le modifiche apportate, è possibile abilitare la modalità **Eliminare dati esecuzione protetta all'uscita** per tale applicazione. Le modifiche apportate durante la sessione andranno perse. Le applicazioni eseguite nella modalità specificata, sono contrassegnate con l'icona.

Per cancellare i dati in modalità protetta a ogni chiusura dell'applicazione, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.

2. Nella finestra visualizzata, selezionare la sezione **Controllo Applicazioni**.

3. Nella parte inferiore della finestra, selezionare l'icona dell'applicazione desiderata.

4. Aprire il menu di scelta rapida facendo clic con il pulsante destro del mouse.

5. Selezionare la voce **Eliminare dati esecuzione protetta all'uscita**. Accanto alla voce di menu verrà visualizzato il riquadro e sull'icona dell'applicazione nell'elenco di applicazioni eseguite in modalità protetta verrà visualizzato il simbolo .

   Per disabilitare la cancellazione dei dati salvati durante una sessione dell'applicazione in modalità protetta, selezionare di nuovo questa voce.

UTILIZZO DI UNA CARTELLA CONDIVISA

Quando si lavora in modalità protetta, tutte le modifiche necessarie dovute al funzionamento dell'applicazione, vengono apportate solo in tale modalità e non influenzano la modalità standard. Pertanto, i file salvati in modalità protetta non possono essere trasferiti alla modalità standard.

Per rendere disponibili in modalità standard i file salvati o modificati in modalità protetta, è possibile utilizzare la *Cartella condivisa in Modalità Protetta* creata da Protezione del computer. Tutti i file salvati in tale cartella quando si lavora in modalità protetta saranno disponibili in modalità standard.

La cartella condivisa viene creata nel disco rigido quando si installa Protezione del computer.

La cartella condivisa viene creata nella cartella *%AllUsersProfile%\Application Data\Kaspersky Lab\SandboxShared* durante l'installazione dell'applicazione. Tale posizione non può essere modificata.

Tale cartella è indicata dall'icona di in Esplora risorse. È anche possibile accedere alla cartella dalla finestra principale di Protezione del computer.

Per aprire la cartella condivisa dalla finestra principale di Protezione del computer, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, selezionare la sezione **Controllo Applicazioni**.
3. Fare clic sul collegamento **Cartella Condivisa**. La cartella viene aperta in una finestra standard di Microsoft Windows.

CANCELLAZIONE DEI DATI IN MODALITA PROTETTA

Per eliminare i dati salvati in modalità protetta o ripristinare le impostazioni correnti di tutte le applicazioni in esecuzione in modalità standard di Microsoft Windows, è possibile cancellare i dati in modalità protetta.

Prima di cancellarli, è consigliabile verificare che tutte le informazioni che potrebbero risultare necessarie per operazioni successive siano state salvate nella cartella condivisa. In caso contrario, i dati verranno eliminati senza alcuna possibilità di ripristinarli.

Per cancellare i dati in modalità protetta, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, selezionare la sezione **Controllo Applicazioni**.
3. Nella parte inferiore della finestra, nel campo **Applicazioni in Modalità Protetta**, fare clic sul collegamento **Cancella cronologia**.
4. Nella finestra visualizzata, confermare la cancellazione dei dati utilizzando il pulsante **OK** o fare clic sul pulsante **Annulla** per annullare l'operazione.

FIREWALL

Protezione del computer contiene un componente speciale, *Firewall*, che garantisce la protezione del computer sia nelle reti locali che in Internet e filtra tutte le attività di rete utilizzando regole di due tipi: *regole per le applicazioni* e *regole pacchetto*.

Firewall analizza le impostazioni delle reti alle quali viene connesso il computer. Se l'applicazione viene eseguita in modalità interattiva (vedere la sezione "Utilizzo della modalità di protezione interattiva" a pagina 152), Firewall richiederà la specifica dello stato della rete connessa al momento della prima connessione. Se la modalità interattiva è disabilitata, Firewall determina lo stato in base al tipo di rete, agli intervalli di indirizzi e ad altre specifiche. A seconda dello stato della rete, Firewall applica regole diverse al filtraggio delle attività di rete.

Per modificare le impostazioni di Firewall:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Firewall**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra visualizzata, utilizzare le schede **Regole di filtraggio** e **Reti** per modificare le impostazioni relative al funzionamento di **Firewall**.

IN QUESTA SEZIONE:

Modifica della categoria della rete 94

Estensione dell'intervallo degli indirizzi di rete 95

Selezione della modalità di notifica delle modifiche alla rete 95

Impostazioni Firewall avanzate 96

Regole Firewall 96

MODIFICA DELLA CATEGORIA DELLA RETE

Tutte le connessioni di rete in esecuzione sul computer vengono controllate dal componente Firewall. Firewall assegna uno stato specifico a ogni connessione e applica varie regole per il filtraggio dell'attività di rete a seconda dello stato assegnato.

Quando ci si collega a una nuova rete, Firewall visualizza una notifica (vedere pagina 262) sullo schermo. Per selezionare un metodo per il filtraggio dell'attività di rete, è necessario specificare lo *stato* della rete rilevata. È possibile selezionare uno degli stati seguenti:

- **Rete pubblica (Internet)**. Questo stato è consigliato per le reti che non sono protette da alcun programma anti-virus, firewall o filtro, ad esempio per i filtri degli Internet café. Gli utenti di tali reti non potranno accedere ai file e alle stampanti disponibili nel computer o ad esso collegate. Anche se è stata creata una cartella condivisa, le informazioni nella stessa non saranno disponibili agli utenti appartenenti a reti con questo stato. Se è stato concesso l'accesso remoto al desktop, gli utenti di questa rete non potranno ottenerlo. Il filtraggio delle attività di rete di ogni applicazione viene eseguito in base alle regole dell'applicazione. Questo stato è assegnato a Internet per impostazione predefinita.
- **Rete locale**. È consigliabile assegnare questo stato alle reti degli utenti ai quali si desidera concedere l'accesso ai file e alle stampanti del proprio computer, ad esempio per la rete aziendale interna o la rete domestica.

- **Rete attendibile**. Questo stato è consigliato solo per le zone considerate sicure, nelle quali il computer non sarà soggetto ad attacchi o a tentativi di accesso non autorizzato ai dati. Se si seleziona questo stato, saranno consentite tutte le attività di rete all'interno della rete.

I tipi di attività di rete consentiti per le reti con un determinato stato dipendono dalle impostazioni delle regole pacchetto predefinite. È possibile modificare tali regole.

Lo stato della rete definisce un set di regole utilizzate per il filtraggio delle attività di rete di quella rete specifica.

Per modificare lo stato della connessione di rete:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Firewall**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra visualizzata, nella scheda **Reti**, selezionare una connessione di rete attiva e fare clic sul collegamento **Modifica**.
6. Nella finestra visualizzata, nella scheda **Proprietà**, selezionare lo stato desiderato nell'elenco a discesa.

ESTENSIONE DELL'INTERVALLO DEGLI INDIRIZZI DI RETE

Ogni rete corrisponde a uno o più intervalli di indirizzi IP. Se ci si connette a una rete, alla cui sottorete si accede mediante un router, è possibile aggiungere manualmente le sottoreti accessibili tramite la rete in questione.

Esempio: ci si connette alla rete di un ufficio dell'azienda e si desidera utilizzare le stesse regole di filtro valide per l'ufficio a cui ci si connette direttamente e per gli uffici accessibili nella rete.

Richiedere gli intervalli di indirizzi di rete per tali uffici all'amministratore della rete e aggiungerli.

Per estendere l'intervallo di indirizzi di rete:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Firewall**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra visualizzata, nella scheda **Reti**, selezionare una connessione di rete attiva e fare clic sul collegamento **Modifica**.
6. Nella finestra visualizzata, nella scheda **Proprietà**, sezione **Sottoreti aggiuntive** fare clic sul collegamento **Aggiungi**.
7. Nella finestra Indirizzo IP visualizzata, specificare un **indirizzo IP** o una maschera di indirizzo.

SELEZIONE DELLA MODALITA DI NOTIFICA DELLE MODIFICHE ALLA RETE

Le impostazioni relative alla connessione di rete possono essere modificate durante il funzionamento. È possibile ricevere notifiche quando si verificano gli eventi seguenti:

- Connessione a una rete.

- In caso di modifiche relative alla corrispondenza tra l'indirizzo MAC e l'indirizzo IP. Questa notifica viene visualizzata in seguito alla modifica dell'indirizzo IP di uno dei computer di rete.

- Quando viene visualizzato un nuovo indirizzo MAC. Questa notifica viene visualizzata in seguito all'aggiunta di un nuovo computer nella rete.

Per abilitare la notifica delle modifiche alle impostazioni della connessione di rete:

1. Aprire la finestra principale dell'applicazione e fareclic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Firewall**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra visualizzata, nella scheda **Reti**, selezionare una connessione di rete attiva e fare clic sul collegamento **Modifica**.
6. Nella finestra visualizzata, nella scheda **Avanzate**, selezionare le caselle relative agli eventi per i quali di desidera ricevere notifiche.

IMPOSTAZIONI FIREWALL AVANZATE

Le impostazioni Firewall avanzate includono:

- Autorizzazione per utilizzare la modalità FTP attiva. La modalità attiva consente di garantire la connessione tra il server e il computer client mediante una porta alla quale verrà connesso il server, a differenza di quanto avviene con la modalità passiva in cui il client viene connesso al server. Questa modalità permette di controllare esattamente quale porta verrà aperta. Il meccanismo funziona anche se è stata creata una regola di divieto. Per impostazione predefinita, la modalità FTP attivo è consentita.

- Bloccare le connessioni se la richiesta di intervento non è disponibile (interfaccia dell'applicazione non caricata). Questa impostazione consente di evitare l'interruzione del funzionamento del Firewall in caso di mancato caricamento dell'interfaccia di Protezione del computer. Rappresenta l'azione predefinita.

- Funzionamento di Firewall fino al completo arresto del sistema. Questa impostazione consente di evitare l'interruzione del funzionamento del Firewall finché il sistema non viene arrestato completamente. Rappresenta l'azione predefinita.

Per modificare le impostazioni avanzate di Firewall, eseguire le operazioni seguenti:

1. Aprire la finestraprincipale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Firewall**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra visualizzata, nella scheda **Regole di filtraggio**, fare clic sul pulsante **Avanzate**.
6. Nella finestra **Avanzate** visualizzata, assicurarsi che le caselle corrispondenti siano selezionate.

REGOLE FIREWALL

Una *regola* Firewall è un'azione eseguita dal componente Firewall in seguito al rilevamento di un tentativo di connessione con determinate impostazioni: direzione e protocollo del trasferimento dati, intervallo di indirizzi e porte alle quali viene eseguita la connessione.

Il componente Firewall opera in base a regole di due tipi:

- *Regole per i pacchetti* (vedere la sezione "Creazione di una regola per pacchetti" a pagina 97) utilizzare per imporre restrizioni sui flussi e sui pacchetti di dati indipendentemente dalle applicazioni.

- *Regole per le applicazioni* (vedere la sezione "Creazione di una regola per l'applicazione" a pagina 98) utilizzate per imporre restrizioni sull'attività di rete di una determinata applicazione. Tali regole consentono di ottimizzare il filtraggio, ad esempio quando un determinato tipo di flusso di dati è bloccato per alcune applicazioni ma consentito per altre.

Le regole pacchetto hanno una priorità maggiore rispetto alle regole per le applicazioni. Se allo stesso tipo di attività di rete sono assegnate sia regole pacchetto che regole per le applicazioni, tale attività verrà elaborata in base alle regole pacchetto.

VEDERE ANCHE:

Creazione di una regola per pacchetti 97

Creazione di una regola per l'applicazione 98

Creazione guidata regole 98

Selezione delle azioni eseguite dalla regola 99

Configurazione delle impostazioni del servizio di rete 99

Selezione dell'intervallo di indirizzi 100

CREAZIONE DI UNA REGOLA PER PACCHETTI

In genere, le regole pacchetto limitano l'attività di rete in entrata su porte TCP e UDP specificate e filtrano i messaggi ICMP.

Una regola pacchetto è composta da un insieme di condizioni e operazioni su pacchetti e flussi di dati eseguiti quando le condizioni sono soddisfatte.

Quando si creano regole pacchetto, tenere presente che sono prioritarie rispetto a quelle per le applicazioni.

Durante la creazione delle condizioni della regola è possibile specificare il servizio e l'indirizzo di rete, utilizzare un indirizzo IP come indirizzo di rete o specificare lo stato della rete. In quest'ultimo caso, gli indirizzi verranno copiati da tutte le reti connesse e presenteranno lo stato correntemente specificato.

➡ *Per creare una regola pacchetto:*

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Firewall**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra visualizzata, nella scheda **Regole di filtraggio**, selezionare la sezione **Regole per i pacchetti** e fare clic sul collegamento **Aggiungi**.
6. Nella finestra **Regola di rete** visualizzata, specificare le impostazioni delle regole.
7. Assegnare la priorità per la regola creata.

Una volta creata la regola, è possibile modificarne le impostazioni o eliminarla utilizzando i collegamenti nella parte inferiore della scheda. Per disabilitare la regola, deselezionare la casella accanto al relativo nome.

CREAZIONE DI UNA REGOLA PER L'APPLICAZIONE

Il componente Firewall analizza l'attività di tutte le applicazioni in esecuzione sul computer. A seconda della classificazione della minaccia, ogni applicazione viene inclusa in uno dei gruppi seguenti:

- **Attendibili**. Le applicazioni appartenenti a questo gruppo possono eseguire qualsiasi attività di rete indipendentemente dallo stato della rete.
- **Restrizione bassa**. Le applicazioni appartenenti a questo gruppo possono eseguire qualsiasi attività di rete in modalità non interattiva. Se si utilizza la modalità interattiva, verrà visualizzata una notifica sullo schermo con la quale sarà possibile consentire o bloccare una connessione o creare una regola di applicazione utilizzando la procedura guidata (vedere la sezione "Creazione guidata regole" a pagina 98).
- **Restrizione alta**. Le applicazioni appartenenti a questo gruppo non possono eseguire alcuna attività di rete in modalità non interattiva. Se si utilizza la modalità interattiva, verrà visualizzata una notifica sullo schermo con la quale sarà possibile consentire o bloccare una connessione o creare una regola di applicazione utilizzando la procedura guidata (vedere la sezione "Creazione guidata regole" a pagina 98).
- **Non attendibili**. Le applicazioni appartenenti a questo gruppo non possono eseguire alcuna attività di rete.

È possibile modificare regole per un intero gruppo o per una determinata applicazione in un gruppo e creare regole aggiuntive per un filtraggio più accurato dell'attività di rete.

Le regole personalizzate per singole applicazioni hanno una priorità maggiore rispetto alle regole ereditate da un gruppo.

Al termine dell'analisi dell'attività dell'applicazione, il componente Firewall crea regole che regolano l'accesso dell'applicazione alle reti con uno stato specifico. È possibile creare regole aggiuntive per una gestione più flessibile dell'attività di rete in Protezione del computer.

Per creare una regola dell'applicazione, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Firewall**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra visualizzata, nella scheda **Regole di filtraggio**, selezionare il gruppo di regole per un'applicazione e fare clic sul collegamento **Aggiungi**.
6. Nella finestra **Regola di rete** visualizzata, specificare le impostazioni delle regole.
7. Assegnare la priorità per la regola creata.

Una volta creata la regola, è possibile modificarne le impostazioni o eliminarla utilizzando i collegamenti nella parte inferiore della scheda. Per disabilitare la regola, deselezionare la casella accanto al relativo nome.

CREAZIONE GUIDATA REGOLE

Se viene attivata una regola per la quale è selezionata l'azione **Chiedi di scegliere un'azione** (per impostazione predefinita questa azione è impostata per le applicazioni incluse nel gruppo **Restrizione bassa** o **Restrizione alta** (vedere la sezione "Gruppi di applicazioni" a pagina 82)), sullo schermo viene visualizzata una notifica corrispondente (vedere pagina 261). È possibile selezionare ulteriori azioni nella finestra di notifica:

- **Consenti**.

- **Nega**.
- **Crea una regola**. Quando viene selezionata questa opzione, viene avviata la *Creazione guidata regole*, che guida l'utente nella creazione di una regola che controlla l'attività di rete dell'applicazione.

L'azione inclusa in una regola attivata può essere impostata su **Consenti** o **Nega**. Per farlo, è necessario selezionare la casella **Applica sempre per questa applicazione**.

La procedura guidata è costituita da diverse finestre di dialogo (passaggi) alle quali è possibile accedere mediante il pulsante **Indietro** e il collegamento **Avanti**. Facendo clic sul collegamento **Fine**, la procedura guidata verrà completata. Per interrompere la procedura in qualsiasi momento, utilizzare il pulsante **Annulla**.

SELEZIONE DELLE AZIONI ESEGUITE DALLA REGOLA

Quando si applica una regola, il componente Firewall esegue una delle operazioni seguenti su un pacchetto o un flusso di dati:

- **Consenti**.
- **Blocca**.
- **Elabora in base alle regole dell'applicazione**. In questo caso l'elaborazione del pacchetto o del flusso di dati con la regola pacchetto verrà interrotta. Le regole per le applicazioni vengono applicate alle connessioni.

Se si desidera registrare informazioni su un tentativo di connessione e sulle azioni di Firewall, abilitare la modalità **Registra eventi**.

Per modificare un'azione eseguita da Firewall:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Firewall**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra visualizzata, nella scheda **Regole di filtraggio**, fare clic sul collegamento **Aggiungi**.
6. Nella finestra **Regola di rete** visualizzata, selezionare l'azione nella sezione **Azione**.

CONFIGURAZIONE DELLE IMPOSTAZIONI DEL SERVIZIO DI RETE

Le impostazioni che caratterizzano l'attività della rete per la quale vengono create regole sono descritte dal *servizio di rete*. Il servizio di rete prevede le impostazioni seguenti:

- *Nome*. Questo testo viene visualizzato nell'elenco di servizi di rete disponibili che possono essere selezionati.
- *Direzione*. Il componente Firewall monitora le connessioni nelle direzioni seguenti:
  - **In entrata**. La regola viene applicata ai pacchetti di dati ricevuti dal computer in uso. Non viene invece applicata alle regole per le applicazioni.
  - **In entrata (stream)**. La regola viene applicata alle connessioni di rete aperte da un computer remoto.
  - **In entrata/In uscita**. La regola viene applicata al flusso di dati sia in entrata che in uscita, a prescindere dal computer, sia esso quello dell'utente o un computer remoto, che ha avviato la connessione di rete.
  - **In uscita**. La regola viene applicata ai pacchetti di dati trasferiti dal computer in uso. Non viene invece applicata alle regole per le applicazioni.

- **In uscita (stream)**. La regola viene applicata solo alle connessioni di rete aperte dal computer in uso.

- *Protocollo*. Il componente Firewall monitora le connessioni che utilizzano i protocolli TCP, UDP, ICMP, ICMPv6, IGMP e GRE. Se come protocollo si è selezionato ICMP o ICMPv6, è possibile specificare il tipo ed il codice del pacchetto ICMP.

Le regole dell'applicazione controllano solo le connessioni che utilizzano i protocolli TCP e UDP.

- *Porte remote e porte locali*. Per i protocolli TCP e UDP è possibile specificare le porte di connessione di un computer remoto e del computer locale che verranno monitorate dalla regola.

Protezione del computer include servizi di rete che descrivono le connessioni di rete più comuni. Quando si creano le regole per Firewall, è possibile selezionare uno dei servizi di rete preinstallati o crearne uno nuovo.

Per configurare le impostazioni della connessione di rete elaborata dalla regola:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Firewall**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra visualizzata, nella scheda **Regole di filtraggio**, fare clic sul collegamento **Aggiungi**.
6. Nella finestra **Regola di rete** visualizzata, sezione **Servizio di rete**, fare clic sul collegamento **Aggiungi**.
7. Nella finestra **Servizio di rete** visualizzata, specificare le impostazioni della connessione di rete.

SELEZIONE DELL'INTERVALLO DI INDIRIZZI

Le regole del firewall vengono applicate alle categorie seguenti di indirizzi di rete:

- **Qualsiasi indirizzo**: la regola verrà applicata a qualsiasi indirizzo IP;
- **Indirizzi di sottorete della categoria**: la regola verrà applicata agli indirizzi IP di tutte le reti connesse con lo stato specificato al momento;
- **Indirizzi del gruppo**: la regola verrà applicata agli indirizzi IP inclusi nell'intervallo specificato.

Per specificare l'intervallo di indirizzi IP ai quali verrà applicata la regola:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Firewall**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra visualizzata, nella scheda **Regole di filtraggio**, fare clic sul collegamento **Aggiungi**.
6. Nella finestra **Regola di rete** visualizzata, selezionare l'intervallo di indirizzi nella sezione **Indirizzi**:
   a. Se si preimposta l'opzione **Indirizzi di sottorete della categoria**, selezionare lo stato della rete dal menu a discesa;
   b. Selezionare uno dei gruppi esistenti di indirizzi se è stata specificata l'opzione **Indirizzi del gruppo**. Se non si desidera utilizzare un intervallo di indirizzi di alcun gruppo, crearne uno nuovo. A tale scopo, scegliere il collegamento **Aggiungi** nella parte inferiore della sezione e specificare gli indirizzi inclusi nel gruppo nella finestra **Indirizzi di rete** visualizzata.

DIFESA PROATTIVA

Protezione del computer protegge l'utente non solo dalle minacce note ma anche da quelle più recenti, per le quali non sono ancora disponibili informazioni nei database dell'applicazione. Questa funzione è garantita da un componente specifico denominato *Difesa Proattiva*.

Le tecnologie preventive offerte da Difesa Proattiva neutralizzano le nuove minacce prima che possano danneggiare il computer. A differenza delle tecnologie reattive, che analizzano il codice in base ai record contenuti nei database di Protezione del computer, le tecnologie preventive riconoscono una nuova minaccia sul 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, Protezione del computer blocca l'attività dell'applicazione.

L'analisi delle attività viene eseguita per tutte le applicazioni, incluse quelle classificate nel gruppo **Attendibili** dal componente Controllo Applicazioni (a pagina 80). Per tali applicazioni, è possibile disabilitare le notifiche di Difesa Proattiva.

Al contrario del componente Controllo Applicazioni, Difesa Proattiva reagisce immediatamente a una sequenza definita di azioni dell'applicazione.

Per modificare le impostazioni di Difesa Proattiva, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Difesa Proattiva**.
4. Apportare le modifiche desiderate alle impostazioni per il componente selezionato.

IN QUESTA SEZIONE:

Utilizzo dell'elenco di attività pericolose 101

Modifica delle regole per il monitoraggio delle attività pericolose 102

Creazione di un gruppo di applicazioni attendibili 103

Controllo degli account di sistema 103

UTILIZZO DELL'ELENCO DI ATTIVITÀ PERICOLOSE

Tenere presente che la configurazione delle impostazioni per il controllo delle attività di Protezione del computer in Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64, Microsoft Windows 7 o Microsoft Windows 7 x64 presenta alcune differenze rispetto ad altri sistemi operativi.

Specifiche per la configurazione del controllo delle attività delle applicazioni in Microsoft Windows XP

Protezione del computer controlla l'attività delle applicazioni sul computer. Difesa Proattiva reagisce immediatamente a una sequenza definita di azioni delle applicazioni. Quando, ad esempio, viene individuato un programma che esegue azioni come copiare se stesso nelle risorse di rete, nella cartella di avvio o nel Registro di sistema per poi inviare copie di se stesso, è molto probabile che si tratti di un worm. Altre sequenze di operazioni pericolose includono:

- azioni tipiche di programmi Trojan;
- tentativi di intercettazione della tastiera;

- installazione nascosta di driver;
- tentativi di modifica del kernel del sistema operativo;
- tentativi di creazione di oggetti e processi nascosti con PID negativo;
- tentativi di modifica dei file HOSTS;
- tentativi di implementazione in altri processi;
- rootkit che reindirizzano l'input/output dei dati;
- tentativi di invio di richieste DNS.

L'elenco di attività pericolose viene aggiunto automaticamente in seguito all'aggiornamento di Protezione del computer e non è modificabile. È tuttavia possibile disattivare il monitoraggio di un'attività pericolosa.

Per disattivare il monitoraggio di un'attività pericolosa:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Difesa Proattiva**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra **Difesa Proattiva** visualizzata, deselezionare la casella accanto al nome dell'attività che non si desidera monitorare.

Specifiche per la configurazione del controllo delle attività delle applicazioni in Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64, Microsoft Windows 7 o Microsoft Windows 7 x64

Se il computer è in esecuzione in uno dei sistemi operativi indicati sopra, il controllo non verrà applicato a ogni evento a causa delle caratteristiche specifiche di tali sistemi. Il controllo non verrà applicato, ad esempio, ai tipi di eventi seguenti: *invio di dati mediante applicazioni attendibili*, *attività di sistema sospette*.

MODIFICA DELLE REGOLE PER IL MONITORAGGIO DELLE ATTIVITA PERICOLOSE

L'elenco di attività pericolose viene aggiunto automaticamente in seguito all'aggiornamento di Protezione del computer e non è modificabile. È possibile:

- disattivare il monitoraggio di un'attività pericolosa (vedere pagina 101);
- modificare la regola utilizzata da Difesa Proattiva quando viene rilevata un'attività pericolosa;
- creare un elenco di esclusioni (vedere pagina 164), elencando le applicazioni la cui attività non viene considerata pericolosa.

Per modificare la regola:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Difesa Proattiva**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.

5. Nella finestra **Difesa Proattiva** selezionata, sezione **Eventi**, selezionare l'evento richiesto per il quale si desidera modificare la regola.

6. Configurare le impostazioni dell'evento selezionato utilizzando i collegamenti nella sezione di descrizione delle regole:

   - fare clic sul collegamento con l'azione preimpostata e nella finestra **Seleziona azione** visualizzata, selezionare l'azione desiderata;

   - fare clic sul collegamento con il periodo di tempo preimpostato (non per tutti i tipi di attività) e nella finestra **Rilevamento di processi nascosti** visualizzata specificare l'intervallo di scansione per i processi nascosti;

   - fare clic sul collegamento Attivato / Disattivato per indicare che è necessario creare il rapporto sull'esecuzione dell'attività.

CREAZIONE DI UN GRUPPO DI APPLICAZIONI ATTENDIBILI

Le applicazioni incluse dal componente Controllo Applicazioni nel gruppo **Attendibili** (vedere la sezione "Gruppi di applicazioni" a pagina 82) non costituiscono una minaccia per il sistema. Tuttavia, le relative attività verranno monitorate anche da Difesa Proattiva.

Utilizzare l'opzione che consente di specificare l'intervallo di applicazioni attendibili, le cui attività non verranno esaminate da Difesa Proattiva. Le applicazioni attendibili possono essere applicazioni con una firma digitale o incluse nel database di Kaspersky Security Network.

Se si desidera che Difesa Proattiva consideri le applicazioni con una firma digitale e/o contenute nel database di Kaspersky Security Network come attendibili e non ne notifichi l'attività, eseguire le operazioni seguenti:

1. Aprire la finestra principaledell'applicazione e fare clic sul pulsante **Protezione del computer**.

2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.

3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Difesa Proattiva**.

4. Nella sezione **Applicazioni attendibili**, selezionare la casella **Applicazioni con firma digitale** e/o la casella **Applicazioni del database Kaspersky Security Network** relativa al componente selezionato.

CONTROLLO DEGLI ACCOUNT DI SISTEMA

Gli account utente controllano l'accesso al sistema e identificano l'utente e il relativo ambiente di lavoro, impedendo ad altri utenti di danneggiare il sistema operativo e i dati. I processi di sistema sono processi avviati dagli account utente di sistema.

Se si desidera controllare l'attività dei processi di sistema oltre a quella dei processi utente mediante Protezione del computer, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Difesa Proattiva**.
4. Nella sezione **Avanzate**, selezionare la casella **Effettua il monitoraggio degli account utente del sistema** relativa al componente selezionato.

PREVENZIONE INTRUSIONI

Prevenzione Intrusioni si carica all'avvio del sistema operativo e tiene traccia del traffico di rete in entrata alla ricerca di attività tipiche degli attacchi di rete. In seguito all'individuazione di un tentativo di attacco al computer, Protezione del computer blocca tutte le attività di rete del computer da cui proviene l'attacco verso il computer in uso. Per impostazione predefinita, il blocco dura un'ora. Sullo schermo verrà visualizzata una notifica (vedere la sezione "Notifiche" a pagina 256) che comunica un tentativo di attacco di rete, con informazioni specifiche sul computer di origine dell'attacco.

Nei database di Protezione del computer è inclusa una descrizione degli attacchi di rete attualmente conosciuti (vedere la sezione "Tipi di attacchi di rete rilevati" a pagina 105) nonché dei metodi utilizzati per combatterli. L'elenco degli attacchi che Prevenzione Intrusioni è in grado di rilevare viene aggiornato durante l'aggiornamento dei database dell'applicazione.

IN QUESTA SEZIONE:

Blocco dei computer da cui proviene l'attacco 105

Tipi di attacchi di rete rilevati 105

BLOCCO DEI COMPUTER DA CUI PROVIENE L'ATTACCO

Per impostazione predefinita, Prevenzione Intrusioni (vedere pagina 105) blocca l'attività di un computer da cui proviene l'attacco per un'ora.

- *Per modificare la durata del blocco del computer da cui proviene l'attacco:*

  1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
  2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
  3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Prevenzione Intrusioni**.
  4. Selezionare la casella **Blocca il computer che ha originato l'attacco per** relativa al componente selezionare e immettere la durata del blocco.

- *Per sbloccare il computer da cui proviene l'attacco:*

  1. Aprire la finestra principale dell'applicazione e selezionare la sezione **Protezione**.
  2. Nella parte destra della finestra, sezione **Attività online**, fare clic sul collegamento **Monitor di Rete**.
  3. Nella finestra visualizzata, nella scheda **Computer bloccati**, selezionare il computer bloccato e fare clic sul collegamento **Sblocca**.

TIPI DI ATTACCHI DI RETE RILEVATI

Esistono attualmente numerosi attacchi di rete che sfruttano le vulnerabilità dei sistemi operativi e di altri software installati nel computer.

Per garantire la protezione del computer, è necessario conoscere i tipi di attacchi possibili. Gli attacchi di rete noti possono essere suddivisi in tre categorie principali:

1. *Scansione porte*: non si tratta di un attacco vero e proprio, bensì di una minaccia che in genere precede un attacco, in quanto rappresenta uno dei modi più comuni per ottenere informazioni su un computer remoto. Le porte UDP/TCP utilizzate dagli strumenti di rete sul computer preso di mira da un hacker, vengono esaminate al fine di rilevarne lo stato (aperta o chiusa).

   Attraverso la scansione delle porte, un hacker è in grado di individuare i tipi di attacchi più efficaci e quelli più deboli. Le informazioni ottenute (un modello del sistema) gli consentono anche di conoscere il sistema operativo utilizzato nel computer remoto, circoscrivendo ulteriormente in questo modo il numero degli attacchi possibili e, di conseguenza, il tempo necessario per realizzarli. L'ulteriore vantaggio per l'hacker è la possibilità di tentare di utilizzare le vulnerabilità specifiche di quel sistema operativo.

2. *Attacchi DoS* o attacchi Denial of Service: attacchi che causano l'instabilità o il blocco di un sistema. Gli attacchi di questo tipo possono compromettere la possibilità di utilizzare le risorse sottoposte all'attacco, ad esempio bloccare l'accesso a Internet.

   Esistono due tipi principali di attacchi DoS:

   - invio al computer bersaglio di pacchetti appositamente creati e inattesi, che determinano il riavvio o l'arresto del sistema.

   - invio al computer bersaglio di molti pacchetti in rapidissima successione, per renderne impossibile l'elaborazione, in modo da esaurire le risorse di sistema.

   Gli esempi più eclatanti di questo gruppo di attacchi sono rappresentati dai tipi seguenti:

   - *Ping of death*: consiste nell'invio di un pacchetto ICMP di dimensioni superiori al limite dei 64 KB. Questo attacco può causare il blocco di alcuni sistemi operativi.

   - *Land*: consiste nell'invio di una richiesta a una porta aperta nel computer bersaglio per stabilire una connessione. Questo manda il computer in un ciclo che intensifica il carico sul processore e può terminare con il blocco di alcuni sistemi operativi.

   - *ICMP Flood*: consiste nell'invio di un elevato numero di pacchetti ICMP al computer. Il computer tenta di rispondere a ogni pacchetto in arrivo, rallentando notevolmente il processore.

   - *SYN Flood*: consiste nell'invio di un elevato numero di query al computer remoto per stabilire una finta connessione. Il sistema riserva determinate risorse a ciascuna di queste connessioni, esaurendole quindi del tutto e il computer non reagisce più ad altri tentativi di connessione.

3. *Attacchi intrusivi*: finalizzati a controllare completamente il computer. Questo è il tipo di attacco più pericoloso che, in caso di riuscita, può determinare il controllo completo del computer da parte dell'hacker.

   Gli hacker utilizzano questo tipo di attacco per ottenere informazioni riservate da un computer remoto, ad esempio numeri di carte di credito o password, o per penetrare nel sistema al fine di utilizzarne in seguito le risorse per fini illeciti. Ad esempio, il sistema invaso viene utilizzato come componente di reti fantasma o come piattaforma per nuovi attacchi.

   Questo gruppo è il più grande in termini di numero di attacchi inclusi. Gli attacchi possono essere divisi in tre gruppi, a seconda del sistema operativo installato nel computer dell'utente: attacchi a Microsoft Windows, attacchi a Unix e il gruppo comune per i servizi di rete destinati a entrambi i sistemi operativi.

   I tipi di attacchi descritti di seguito risultano essere i più diffusi tra quelli che utilizzano le risorse di rete dei sistemi operativi:

   - *Attacchi di sovraccarico del buffer*: tipo di vulnerabilità del software determinata dall'incapacità o dalla totale assenza di controllo durante la gestione di grandi quantità di dati. Si tratta del tipo di vulnerabilità noto da più tempo e più semplice da sfruttare da parte degli hacker.

   - *Attacchi attraverso le stringhe di formato*: tipo di vulnerabilità nel software causata dal controllo insufficiente dei valori immessi per le funzioni I/O come *printf()*, *fprintf()*, *scanf()* e altre dalla libreria standard C. Se un programma presenta questa vulnerabilità, l'hacker che riesce a inviare query create con una tecnica speciale, può assumere il controllo totale del sistema.

   Il sistema Prevenzione Intrusioni analizza automaticamente e impedisce i tentativi di sfruttare queste vulnerabilità nei servizi di rete più comuni (FTP, POP3, IMAP) se sono in esecuzione nel computer dell'utente.

   Attacchi destinati ai computer con Microsoft Windows: basati sull'uso di vulnerabilità del software installato in un computer, ad esempio Microsoft SQL Server, Microsoft Internet Explorer, Messenger e componenti del sistema disponibili tramite rete come DCom, SMB, Wins, LSASS, IIS5.

   Esistono inoltre incidenti isolati di intrusioni mediante script dannosi, tra cui gli script elaborati da Microsoft Internet Explorer e i worm di tipo Helkern. Questo tipo di attacco consiste in sostanza nell'invio di uno speciale tipo di pacchetti UDP a un computer remoto in grado di eseguire codice dannoso.

ANTI-SPAM

Protezione del computer include *Anti-Spam*, un componente che consente di rilevare messaggi indesiderati (spam) e di elaborarli in base alle regole del client di posta elettronica utilizzato, risparmiando tempo durante la gestione della posta.

Anti-Spam utilizza un algoritmo di autoaddestramento (vedere la sezione "Algoritmo di funzionamento del componente" a pagina 108) grazie al quale il componente è in grado di distinguere sempre meglio la posta spam dalla posta utile con il passare del tempo. L'origine dei dati per l'algoritmo viene estrapolata dal contenuto del messaggio. Per consentire un riconoscimento efficiente della posta spam e della posta utile con Anti-Spam, il componente richiede un addestramento (vedere la sezione "Addestramento di Anti-Spam" a pagina 109).

Si consiglia di esaminare l'algoritmo di Anti-Spam in dettaglio.

Anti-Spam può essere utilizzato come plug-in dei client di posta seguenti:

- Microsoft Office Outlook (vedere la sezione "Configurazione dell'elaborazione della posta spam in Microsoft Office Outlook" a pagina 123);
- Microsoft Outlook Express (Windows Mail) (vedere la sezione "Configurazione dell'elaborazione della posta spam in Microsoft Outlook Express (Windows Mail)" a pagina 125);
- The Bat! (vedere la sezione "Configurazione dell'elaborazione della posta spam in The Bat!" a pagina 125);
- Thunderbird (vedere la sezione "Configurazione dell'elaborazione della posta spam in Thunderbird" a pagina 126).

È possibile utilizzare gli elenchi di mittenti consentiti (vedere pagina 117) e bloccati (vedere pagina 115) per specificare gli indirizzi dai quali i messaggi verranno riconosciuti come posta utile o come spam dal componente Anti-Spam. Anti-Spam può inoltre verificare la presenza in un messaggio di frasi incluse negli elenco di frasi consentite (vedere pagina 118) e bloccate (vedere pagina 116), nonché nell'elenco di espressioni oscene (vedere pagina 117).

Anti-Spam consente di visualizzare la posta sul server (vedere la sezione "Filtraggio dei messaggi di posta sul server. Gestore della posta" a pagina 122) ed eliminare quelli indesiderati senza scaricarli nel computer.

Per modificare le impostazioni di Anti-Spam:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Spam**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Apportare le modifiche richieste alle impostazioni dell'applicazione.

IN QUESTA SEZIONE:

Algoritmo di funzionamento del componente 108

Addestramento di Anti-Spam 109

Modifica del livello di protezione 113

Selezione del metodo di scansione 114

Creazione dell'elenco di URL attendibili 115

Creazione dell'elenco di mittenti bloccati 115

Creazione dell'elenco di frasi bloccate 116

Creazione dell'elenco di frasi oscene 117

Creazione dell'elenco di mittenti consentiti 117

Creazione dell'elenco di frasi consentite 118

Importazione dell'elenco di mittenti consentiti 119

Determinazione dei fattori di spam e probabile spam 119

Selezione dell'algoritmo di riconoscimento dello spam 120

Utilizzo delle funzioni avanzate di filtraggio anti-spam 121

Aggiunta di un'etichetta all'oggetto del messaggio 121

Filtraggio dei messaggi di posta sul server. Gestore della posta 122

Esclusione di messaggi di Microsoft Exchange Server dalla scansione 122

Azioni da eseguire con la posta spam 123

Ripristino delle impostazioni predefinite di Anti-Spam 126

ALGORITMO DI FUNZIONAMENTO DEL COMPONENTE

Il funzionamento di Anti-Spam può essere suddiviso in due fasi:

1. Applicazione di rigidi criteri di filtraggio a un messaggio. Tali criteri consentono di determinare con rapidità se il messaggio è spam o meno. Anti-Spam assegna al messaggio uno stato *spam* o *non spam*, la scansione viene sospesa e il messaggio viene trasferito al client di posta per l'elaborazione (vedere i passaggi da 1 a 5 descritti di seguito).

2. Ispezione dei messaggi che hanno superato rigidi criteri di selezione durante i passaggi precedenti. Tali messaggi non possono essere inequivocabilmente considerati spam. Di conseguenza, Anti-Spam deve calcolare la *probabilità* che essi appartengano alla categoria spam.

L'algoritmo di Anti-Spam è costituito dai passaggi seguenti:

1. L'indirizzo del mittente del messaggio viene controllato per verificarne la presenza nell'elenco di mittenti consentiti o bloccati.

- Se l'indirizzo di un mittente è incluso nell'elenco degli indirizzi consentiti, al messaggio viene assegnato lo stato *Non spam*.

- Se l'indirizzo di un mittente è incluso nell'elenco degli indirizzi bloccati, al messaggio viene assegnato lo stato *Spam*.

2. Se un messaggio è stato inviato tramite Microsoft Exchange Server e ne è stata disabilitata la scansione (vedere pagina 122), gli verrà assegnato lo stato *non spam*.

3. Viene eseguita l'analisi del messaggio per verificare se contiene stringhe incluse nell'elenco di frasi consentite (vedere pagina 118). Se viene trovata almeno una riga inclusa in questo elenco, al messaggio viene assegnato lo stato *non spam*. Per impostazione predefinita, questo passaggio viene ignorato.

4. Viene eseguita l'analisi del messaggio per verificare se contiene stringhe incluse nell'elenco di frasi bloccate (vedere pagina 116). Le probabilità che il messaggio sia spam aumentano se al suo interno vengono trovate parole incluse in questo elenco. Se la probabilità calcolata supera il valore specificato (vedere pagina 119) a un messaggio viene assegnato lo stato *Spam* o *Probabile spam*. Viene eseguita l'analisi del messaggio per verificare se contiene stringhe incluse nell'elenco di frasi oscene (vedere pagina 117). Per impostazione predefinita, questo passaggio viene ignorato.

5. Se il testo del messaggio contiene un indirizzo incluso nel database di indirizzi Web di phishing o sospetti (vedere pagina 114), al messaggio viene assegnato lo stato *Spam*.

6. Viene eseguita l'analisi del messaggio utilizzando le regole euristiche. Se l'analisi rileva la presenza di segni tipici di spam in un messaggio, la probabilità che tale messaggio sia di tipo spam aumenta.

7. L'applicazione analizza i messaggi di posta elettronica tramite la tecnologia GSG. Durante questa operazione, Anti-Spam analizza le immagini allegate al messaggio di posta elettronica. Se l'analisi rileva segni tipici di spam nelle immagini, la probabilità che il messaggio sia di tipo spam aumenta.

8. L'applicazione analizza i documenti in formato *.rtf* allegati al messaggio e ne esegue la scansione per verificare che non contengano segni di spam. Una volta completata l'analisi, Anti-Spam calcola quanto è aumentata la probabilità che il messaggio sia spam. Per impostazione predefinita, la tecnologia è disabilitata.

9. Essa verifica la presenza di ulteriori caratteristiche tipiche dello spam (vedere pagina 121). Ogni funzione rilevata aumenta la probabilità che il messaggio esaminato sia effettivamente spam.

10. Se Anti-Spam è stato addestrato, il messaggio viene analizzato tramite la tecnologia iBayes. L'algoritmo iBayes con autoaddestramento calcola la probabilità che un messaggio sia di tipo spam in base alla frequenza di frasi tipiche dello spam trovate nel testo del messaggio.

L'analisi del messaggio determina la probabilità che si tratti di spam. Gli autori di spam continuano a migliorare i metodi per occultare lo spam, pertanto la probabilità calcolata molto spesso non raggiunge il valore specificato (vedere la sezione "Determinazione dei fattori di spam e probabile spam" a pagina 119). Per garantire un efficiente filtraggio dei messaggi di posta elettronica, Anti-Spam utilizza due parametri:

- *Fattore di spam*: il valore della probabilità che, se superato, fa sì che il messaggio venga considerato *spam*. Se la probabilità è inferiore a tale valore, al messaggio viene assegnato lo stato di *probabile spam*.

- *Fattore di spam potenziale*: il valore della probabilità che, se superato, fa sì che il messaggio venga considerato spam potenziale. Se la probabilità è inferiore a tale valore, Anti-Spam considera il messaggio non spam.

In base ai fattori di spam e probabile spam specificati, ai messaggi viene assegnato lo stato *spam* o *probabile spam*. A seconda dello stato assegnato, ai messaggi viene inoltre assegnata l'etichetta **[!! SPAM]** o **[!! Probable Spam]** nel campo **Oggetto**. I messaggi vengono quindi elaborati in base alle regole (vedere la sezione "Azioni da eseguire con la posta spam" a pagina 123) create per il client di posta.

ADDESTRAMENTO DI ANTI-SPAM

Uno degli strumenti più potenti per il rilevamento dello spam è l'algoritmo iBayes di autoaddestramento. Tale algoritmo stabilisce quale stato assegnare a un messaggio in base alle frasi che contiene. Prima di iniziare, è necessario inoltrare all'algoritmo iBayes alcune stringhe di esempio di posta utile e di posta spam a scopo di addestramento.

Esistono diversi approcci all'addestramento di Anti-Spam:

- Utilizzando l'Addestramento guidato (vedere la sezione "Addestramento con Addestramento guidato" a pagina 110) (addestramento del pacchetto). È consigliabile eseguire l'addestramento mediante l'Addestramento guidato fin dal primo utilizzo di Anti-Spam.
- Addestramento di Anti-Spam con i messaggi in uscita (vedere la sezione "Addestramento di Anti-Spam con i messaggi in uscita" a pagina 111).
- Addestramento diretto durante l'utilizzo della posta e-mail (vedere la sezione "Addestramento tramite il client di posta" a pagina 111), utilizzando pulsanti della barra degli strumenti o voci di menu speciali.
- Addestramento durante l'utilizzo dei rapporti Anti-Spam (vedere la sezione "Addestramento con i rapporti" a pagina 113).

ADDESTRAMENTO CON ADDESTRAMENTO GUIDATO

L'Addestramento guidato consente di addestrare Anti-Spam in modalità batch. A tale scopo è necessario specificare le cartelle degli account di Microsoft Office Outlook o Microsoft Outlook Express contenenti posta spam e posta utile.

Per il corretto riconoscimento dello spam è necessario utilizzare almeno 50 messaggi utili e 50 esempi di posta indesiderata. iBayes non funzionerà finché non saranno stati completati questi passaggi.

Per risparmiare tempo, l'Addestramento guidato limita l'addestramento a 50 messaggi tra quelli presenti in ciascuna cartella selezionata.

La procedura guidata è costituita da una serie di finestre (passaggi) tra le quali è possibile spostarsi servendosi dei pulsanti **Indietro** e **Avanti**. Per chiudere la procedura guidata, utilizzare il pulsante **Fine**. Per interrompere la procedura in qualsiasi momento, utilizzare il pulsante **Annulla**.

Per avviare la procedura guidata:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Spam**.
4. Nella sezione **Addestramento Anti-Spam**, fare clic sul pulsante **Istruisci** relativo al componente selezionato.

Quando si esegue l'addestramento in base a messaggi di posta elettronica validi, gli indirizzi dei mittenti dei messaggi vengono aggiunti all'elenco dei mittenti consentiti.

Per disabilitare l'aggiunta dell'indirizzo del mittente all'elenco di mittenti consentiti, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul. pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Spam**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra visualizzata, nella scheda **Metodi esatti**, sezione **Considera il messaggio come non spam**, selezionare la casella **Se proviene da un mittente consentito** e fare clic sul pulsante **Seleziona**.
6. Nella finestra **Elenco dei mittenti consentiti** visualizzata, deselezionare la casella **Includi gli indirizzi dei mittenti consentiti nell'addestramento Anti-Spam del client di posta**.

VEDERE ANCHE:

Addestramento con i rapporti 113

Addestramento tramite il client di posta 111

Addestramento di Anti-Spam con i messaggi in uscita 111

ADDESTRAMENTO DI ANTI-SPAM: CON I MESSAGGI IN USCITA

È possibile addestrare Anti-Spam con un campione di 50 messaggi di posta in uscita. Gli indirizzi dei destinatari verranno aggiunti automaticamente all'elenco dei mittenti consentiti.

Per addestrare Anti-Spam con i messaggi in uscita:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Spam**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra visualizzata, nella scheda **Avanzate**, sezione **Messaggi in uscita**, selezionare le caselle **Addestramento sui messaggi di posta in uscita**.

Per disabilitare l'aggiunta dell'indirizzo del mittente all'elenco dei mittenti consentiti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Spam**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra visualizzata, nella scheda **Metodi esatti**, sezione **Considera il messaggio come non spam**, selezionare la casella **Se proviene da un mittente consentito** e fare clic sul pulsante **Seleziona**.
6. Nella finestra **Elenco dei mittenti consentiti** visualizzata deselezionare la casella **Includi gli indirizzi dei mittenti consentiti nell'addestramento Anti-Spam del client di posta**.

VEDERE ANCHE:

Addestramento con Addestramento guidato 110

Addestramento con i rapporti 113

Addestramento tramite il client di posta 111

ADDESTRAMENTO TRAMITE IL CLIENT DI POSTA

L'addestramento di Anti-Spam mentre si gestiscono i messaggi di posta elettronica implica l'utilizzo di elementi dell'interfaccia speciali del programma del client di posta.

I pulsanti utilizzati per l'addestramento di Anti-Spam vengono visualizzati nell'interfaccia dei client di posta di Microsoft Office Outlook e Microsoft Outlook Express (Windows Mail) solo dopo aver installato Protezione del computer.

Per addestrare Anti-Spam tramite il client di posta:

1. Avviare il client di posta.
2. Selezionare un messaggio da utilizzare per addestrare Anti-Spam.
3. A seconda del client di posta in uso, eseguire le operazioni seguenti:
   - Fare clic sul pulsante **Spam** o **Non spam** sulla barra degli strumenti di Microsoft Office Outlook.
   - Fare clic sul pulsante **Spam** o **Non spam** sulla barra degli strumenti di Microsoft Outlook Express (Windows Mail).
   - Utilizzare gli elementi speciali **Contrassegna come spam)** e **Contrassegna come non spam** del menu **Speciale** del programma del client di posta di The Bat!;
   - Utilizzare il pulsante **Spam / Non Spam** sulla barra degli strumenti di Mozilla Thunderbird.

Dopo aver selezionato un'opzione dell'elenco precedente, Anti-Spam esegue l'addestramento utilizzando il messaggio selezionato. Se si selezionano diversi messaggi, verranno utilizzati tutti per l'addestramento.

Se un messaggio viene contrassegnato come posta utile, l'indirizzo del relativo mittente verrà aggiunto all'elenco dei mittenti consentiti.

Per disabilitare l'aggiunta dell'indirizzo del mittente all'elenco dei mittenti consentiti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Spam**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra visualizzata, nella scheda **Metodi esatti**, sezione **Considera il messaggio come non spam**, selezionare la casella ☑ **Se proviene da un mittente consentito** e fare clic sul pulsante **Seleziona**.
6. Nella finestra **Elenco dei mittenti consentiti** visualizzata deselezionare la casella ☑ **Includi gli indirizzi dei mittenti consentiti nell'addestramento Anti-Spam del client di posta**.

Se è necessario selezionare diversi messaggi contemporaneamente o se si è certi che una cartella contenga messaggi di un solo gruppo (spam o non spam), è possibile adottare un approccio più complesso all'addestramento del componente utilizzando l'Addestramento guidato (vedere la sezione "Addestramento di Anti-Spam" a pagina 109).

VEDERE ANCHE:

Addestramento di Anti-Spam con i messaggi in uscita.....111

Addestramento con Addestramento guidato 110

Addestramento con i rapporti 113

ADDESTRAMENTO CON I RAPPORTI

È possibile eseguire l'addestramento di Anti-Spam utilizzandone i rapporti come origine. I rapporti del componente, infatti, consentono di valutare l'accuratezza della configurazione e, se necessario, di apportare determinate correzioni ad Anti-Spam.

Per contrassegnare un determinato messaggio come spam o non spam:

1. Aprire la finestra principale dell'applicazione.
2. Fare clic sul collegamento **Rapporto** per passare alla finestra dei rapporti di Protezione del computer.
3. Nella finestra visualizzata, nella scheda **Rapporto**, fare clic sul pulsante **Rapporto dettagliato**.
4. Per il componente **Anti-Spam**, selezionare un messaggio in base al quale si desidera effettuare un ulteriore addestramento.
5. Aprire il menu di scelta rapida relativo al messaggio e selezionare una delle azioni seguenti:
   - **Contrassegna come spam**;
   - **Contrassegna come non spam**;
   - **Aggiungi all'elenco di mittenti consentiti**;
   - **Aggiungi all'elenco di mittenti bloccati**;

VEDERE ANCHE:

Addestramento di Anti-Spam con i messaggi in uscita.....111

Addestramento con Addestramento guidato 110

Addestramento tramite il client di posta.....111

MODIFICA DEL LIVELLO DI PROTEZIONE

Per il filtraggio dei messaggi, il componente Anti-Spam utilizza due fattori:

- *Fattore di spam*: il valore della probabilità che, se superato, fa sì che il messaggio venga considerato spam. Se la probabilità è inferiore a tale valore, ai messaggi viene assegnato lo stato di *probabile spam*.
- *Fattore di spam potenziale*: il valore della probabilità che, se superato, fa sì che il messaggio venga considerato spam potenziale. Se la probabilità è inferiore a tale valore, Anti-Spam considera il messaggio non spam.

Gli specialisti di Kaspersky Lab distinguono tre livelli di protezione:

- **Alto**. Questo livello di protezione è consigliabile se si riceve spesso posta spam, ad esempio se si utilizza un servizio di posta gratuito. Quando si seleziona questo livello, la frequenza di falsi positivi aumenta, ovvero la possibilità che la posta utile venga riconosciuta spesso come spam.
- **Consigliato**. Questo livello di protezione è consigliabile nella maggior parte dei casi.
- **Basso**. Questo livello di protezione è consigliabile se si riceve solo raramente posta spam, ad esempio se si lavora in un ambiente di posta aziendale protetto. Quando si seleziona questo livello, si riduce la frequenza con cui vengono riconosciuti i messaggi di spam e di probabile spam.

Per cambiare il livello di protezione del componente Anti-Spam selezionato:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Spam**.
4. Impostare il livello di protezione necessario per il componente selezionato.

SELEZIONE DEL METODO DI SCANSIONE

I metodi di scansione consistono nella scansione degli URL contenuti nei messaggi inviati dai client di messaggistica immediata per verificare che non siano inclusi nell'elenco di indirizzi Web sospetti e/o nell'elenco di indirizzi Web di phishing.

Il controllo dei collegamenti per verificare che non siano inclusi nell'elenco di indirizzi di phishing consente di evitare attacchi di phishing, che si presentano sotto forma di messaggi di posta elettronica provenienti da sedicenti istituti finanziari e contengono collegamenti ai relativi siti Web. Il testo del messaggio induce il lettore a fare clic sul collegamento e a immettere informazioni riservate nella finestra che segue, ad esempio, un numero di carta di credito o il nome utente e la password usati per collegarsi al proprio sito di Internet banking per eseguire operazioni finanziarie.

Un attacco di phishing può essere occultato, ad esempio, sotto forma di lettera proveniente dalla propria banca con un collegamento al relativo sito Web ufficiale. Facendo clic sul collegamento, si arriva 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 in poi, tutte le operazioni eseguite nel sito possono essere ricostruite e utilizzate per prelevare denaro dal conto dell'utente.

Per eseguire la scansione dei collegamenti nei messaggi utilizzando il database di indirizzi sospetti, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Spam**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.

5. Nella finestra visualizzata, nella scheda **Metodi esatt**i, sezione **Considera il messaggio come spam**, selezionare la casella **Se contiene URL presenti nel database degli indirizzi sospetti**.

Per eseguire la scansione dei collegamenti nei messaggi utilizzando il database di indirizzi di phishing, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Spam**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra visualizzata, nella scheda **Metodi esatti**, sezione **Considera il messaggio come spam**, selezionare la casella **Se contiene URL presenti nel database degli indirizzi di phishing**.

CREAZIONE DELL'ELENCO DI URL ATTENDIBILI

È possibile creare un elenco di indirizzi attendibili. Anti-Spam verificherà che l'indirizzo del destinatario sia incluso nell'elenco.

Per creare l'elenco di indirizzi attendibili:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Spam**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra visualizzata, nella scheda **Metodi esatti**, selezionare la casella **Se non è indirizzato a me** e fare clic sul pulsante **I miei indirizzi**.
6. Nella finestra **Indirizzi e-mail personali** visualizzata, fare clic sul collegamento **Aggiungi**.
7. Specificare gli indirizzi o le maschere di indirizzi necessari nella finestra **Maschera per l'indirizzo e-mail** visualizzata.

CREAZIONE DELL'ELENCO DI MITTENTI BLOCCATI

L'elenco di mittenti bloccati contiene gli indirizzi dei mittenti dei messaggi contrassegnati come spam. Tale elenco viene compilato manualmente.

L'elenco può contenere indirizzi o maschere di indirizzi. Le maschere supportano l'utilizzo dei caratteri jolly standard ***** e **?**, dove ***** rappresenta una qualsiasi combinazione di caratteri e **?** indica un singolo carattere. Esempi di maschere di indirizzi:

- *ivanov@test.ru*. I messaggi provenienti da questo indirizzo verranno sempre classificati come spam.
- **@test.ru.* La posta proveniente da un mittente del dominio di posta *test.ru* verrà sempre considerata spam, ad esempio: *petrov@test.ru*, *sidorov@test.ru*.
- *ivanov@**. Il mittente con questo nome, indipendentemente dal dominio di posta, invia sempre spam, ad esempio: *ivanov@test.ru*, *ivanov@mail.ru*.
- **@test**. La posta proveniente da un mittente di un dominio di posta che inizia con *test* viene considerata spam, ad esempio: *ivanov@test.ru*, *petrov@test.com*.

- *ivan.*@test.???*. La posta proveniente da un mittente il cui nome inizia con *ivan.* e che proviene da un dominio di posta che inizia con *test* e termina con tre caratteri qualsiasi, è sempre considerata spam, ad esempio: *ivan.ivanov@test.com*, *ivan.petrov@test.org*.

Per creare un elenco di mittenti bloccati e utilizzarlo successivamente:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Spam**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra visualizzata, nella scheda **Metodi esatti**, sezione **Considera il messaggio come spam**, selezionare la casella **Se proviene da un mittente bloccato** e fare clic sul pulsante **Seleziona**.
6. Nella finestra **Elenco dei mittenti bloccati** visualizzata, fare clic sul collegamento **Aggiungi**.
7. Nella finestra **Maschera per l'indirizzo e-mail** visualizzata, immettere la maschera o l'indirizzo appropriato.

CREAZIONE DELL'ELENCO DI FRASI BLOCCATE

L'elenco di frasi bloccate viene utilizzato per memorizzare frammenti chiave di messaggi considerati spam. Tale elenco viene compilato manualmente.

Per definire le frasi è anche possibile utilizzare le maschere. Le maschere supportano l'utilizzo dei caratteri jolly standard ***** e **?**, dove ***** rappresenta una qualsiasi combinazione di caratteri e **?** indica un singolo carattere. Esempi di frasi e maschere di frasi:

- *Ciao Ivan!.* Un messaggio di posta contenente solo questo testo è considerato spam. L'utilizzo di righe simili alle seguenti è sconsigliato.
- *Ciao Ivan!**. Un messaggio di posta che inizia con la stringa *Ciao Ivan!* è considerato spam.
- *Ciao *! *.* Un messaggio di posta che inizia con *Ciao* e che contiene un punto esclamativo in una parte del messaggio è considerato spam.
- ** Ivan? *.* Un messaggio di posta che inizia con il nome *Ivan* seguito da un carattere è considerato spam.
- ** Ivan\? *. Un messaggio di posta che contiene la frase *Ivan?* è considerato spam.

Se in una frase sono inclusi i caratteri * e ?, è necessario farli precedere dal carattere \ per impedire che vengano interpretati erroneamente in Anti-Spam. Pertanto, al posto di un solo carattere ne vengono utilizzati due: * e \?.

Per creare l'elenco di frasi bloccate:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Spam**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra visualizzata, nella scheda **Metodi esatti**, sezione **Considera il messaggio come spam**, selezionare la casella **Se contiene frasi bloccate** e fare clic sul pulsante **Seleziona**.
6. Nella finestra **Elenco delle frasi bloccate** visualizzata, fare clic sul collegamento **Aggiungi**.

7. Nella finestra **Frase bloccata** visualizzata, immettere una frase o una maschera.

CREAZIONE DELL'ELENCO DI FRASI OSCENE

L'elenco contiene frasi oscene che con molto probabilità indicano la presenza di un messaggio spam.

L'elenco di frasi oscene incluso nel pacchetto di distribuzione di Protezione del computer è stato compilato dagli specialisti di Kaspersky Lab. L'elenco può essere modificato.

Per definire le frasi è anche possibile utilizzare le maschere. Le maschere supportano l'utilizzo dei caratteri jolly standard ***** e **?**, dove ***** rappresenta una qualsiasi combinazione di caratteri e **?** indica un singolo carattere.

Se in una frase sono inclusi i caratteri * e ?, è necessario farli precedere dal carattere \ per impedire che vengano interpretati erroneamente in Anti-Spam. Pertanto, al posto di un solo carattere ne vengono utilizzati due: * e \?.

Per modificare l'elenco di frasi oscene, eseguire le operazioni seguenti:

1. Aprire lafinestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Spam**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra visualizzata, nella scheda **Metodi esatti**, sezione **Considera il messaggio come spam**, selezionare la casella **Se contiene frasi bloccate** e fare clic sul pulsante **Seleziona**.
6. Nella finestra **Elenco delle frasi bloccate** visualizzata selezionare la casella **Considera bloccate le parole oscene** e fare clic sul collegamento **parole oscene**.
7. Leggere il testo nella finestra **Contratto** visualizzata e, se si accettano i termini e le condizioni descritte nella finestra, selezionare la casella corrispondente e fare clic sul pulsante **OK**.
8. Nella finestra **Elenco delle parole oscene** visualizzata, fare clic sul collegamento **Aggiungi**.
9. Nella finestra **Frase bloccata** visualizzata, immettere una frase o una maschera.

CREAZIONE DELL'ELENCO DI MITTENTI CONSENTITI

L'elenco di mittenti consentiti contiene gli indirizzi dei mittenti dai quali si ritiene non verrà ricevuto spam. Tale elenco viene compilato automaticamente durante l'addestramento di Anti-Spam ma può essere modificato. L'elenco può essere modificato.

L'elenco può contenere indirizzi o maschere di indirizzi. Le maschere supportano l'utilizzo dei caratteri jolly standard ***** e **?**, dove ***** rappresenta una qualsiasi combinazione di caratteri e **?** indica un singolo carattere. Esempi di maschere di indirizzi:

- *ivanov@test.ru.* I messaggi provenienti da questo indirizzo verranno sempre classificati come validi.
- **@test.ru.* La posta proveniente da un mittente del dominio di posta *test.ru* verrà sempre considerata valida, ad esempio: *petrov@test.ru*, *sidorov@test.ru*.
- *ivanov@*.* Il mittente con questo nome, indipendentemente dal dominio di posta, invia sempre posta valida, ad esempio: *ivanov@test.ru*, *ivanov@mail.ru*.
- **@test*.* La posta proveniente da un mittente di un dominio di posta che inizia con *test* viene considerata non spam, ad esempio: *ivanov@test.ru*, *petrov@test.com*.

- *ivan.*@test.???.* La posta proveniente da un mittente il cui nome inizia con *ivan.* e che proviene da un dominio di posta che inizia con *test* e termina con tre caratteri qualsiasi, è sempre valida, ad esempio: *ivan.ivanov@test.com*, *ivan.petrov@test.org*.

Per creare l'elenco di mittenti consentiti:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Spam**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra visualizzata, nella scheda **Metodi esatti**, sezione **Considera il messaggio come non spam**, selezionare la casella **Se proviene da un mittente consentito** e fare clic sul pulsante **Seleziona**.
6. Nella finestra **Elenco dei mittenti consentiti** visualizzata, fare clic sul collegamento **Aggiungi**.
7. Nella finestra **Maschera per l'indirizzo e-mail** visualizzata, immettere la maschera o l'indirizzo appropriato.

CREAZIONE DELL'ELENCO DI FRASI CONSENTITE

L'elenco di frasi consentite viene utilizzato per memorizzare frammenti chiave di messaggi contrassegnati come posta utile e può essere creato dall'utente.

Per definire le frasi è anche possibile utilizzare le maschere. Le maschere supportano l'utilizzo dei caratteri jolly standard ***** e **?**, dove ***** rappresenta una qualsiasi combinazione di caratteri e **?** indica un singolo carattere. Esempi di frasi e maschere di frasi:

- *Ciao Ivan!.* Un messaggio di posta contenente solo questo testo è considerato posta valida. L'utilizzo di righe simili alle seguenti è sconsigliato.
- *Ciao Ivan!**. Un messaggio di posta che inizia con la stringa *Ciao Ivan!* appartiene alla categoria di posta valida.
- *Ciao *! **. Un messaggio di posta che inizia con *Ciao* e che contiene un punto esclamativo in una parte del messaggio non è considerato spam.
- ** Ivan? **. Un messaggio di posta che inizia con il nome *Ivan* seguito da un carattere non è considerato spam.
- ** Ivan\? **. Un messaggio di posta che contiene la frase *Ivan?* è considerato posta valida.

Se in una frase sono inclusi i caratteri * e ?, è necessario farli precedere dal carattere \ per impedire che vengano interpretati erroneamente in Anti-Spam. Pertanto, al posto di un solo carattere ne vengono utilizzati due: * e \?.

Per creare l'elenco di frasi consentite:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Spam**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra visualizzata, nella scheda **Metodi esatti**, sezione **Considera il messaggio come spam**, selezionare la casella **Se contiene frasi consentite** e fare clic sul pulsante **Seleziona**.
6. Nella finestra **Elenco delle frasi consentite** visualizzata, fare clic sul collegamento **Aggiungi**.

7. Nella finestra **Frase consentita** visualizzata, immettere una frase o una maschera.

IMPORTAZIONE DELL'ELENCO DI MITTENTI CONSENTITI

Gli indirizzi contenuti nell'elenco di mittenti consentiti possono essere importati dai file **.txt*, **.csv* o dalla Rubrica di Microsoft Office Outlook/Microsoft Outlook Express.

Per importare l'elenco di mittenti consentiti:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Spam**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra visualizzata, nella scheda **Metodi esatti**, sezione **Considera il messaggio come non spam**, selezionare la casella **Se proviene da un mittente consentito** e fare clic sul pulsante **Seleziona**.
6. Nella finestra **Elenco dei mittenti consentiti** visualizzata, fare clic sul collegamento **Importa**.
7. Selezionare l'origine di importazione dal menu a discesa:
   - **Importa da file**. Dopo aver selezionato questa origine, viene visualizzata una finestra di dialogo di selezione file. L'applicazione supporta l'importazione dai file di tipo *.csv* o *.txt*.
   - **Importa dalla Rubrica**. Dopo aver selezionato questa origine, viene visualizzata una finestra di dialogo di selezione della Rubrica. Selezionare la rubrica desiderata da questa finestra.

DETERMINAZIONE DEI FATTORI DI SPAM E PROBABILE SPAM

Gli esperti di Kaspersky Lab lavorano per garantire la maggiore precisione possibile nel rilevamento dello spam e del probabile spam in Anti-Spam.

Il riconoscimento dello spam si basa su metodi di filtraggio moderni che consentono di addestrare Anti-Spam in modo da distinguere lo spam, il probabile spam e la posta utile. La procedura di addestramento viene implementata come analisi di un determinato numero di messaggi dell'utente.

L'addestramento dello strumento Anti-Spam può essere eseguito utilizzando l'Apprendimento guidato e sulla base dei messaggi elaborati dai client di posta elettronica. Così facendo, a ogni singolo elemento dei messaggi di posta elettronica utili o dei messaggi spam viene assegnato un fattore. Quando un messaggio di posta elettronica entra a far parte della cartella della posta in arrivo, Anti-Spam lo analizza utilizzando l'algoritmo iBayes per distinguere tra spam e messaggi validi. I fattori di ciascun elemento vengono sommati e viene quindi calcolato un fattore di spam e un fattore di probabile spam.

Il fattore di probabile spam definisce il valore che causerà l'assegnazione dello stato *Probabile spam* a un messaggio, se superato. Se si utilizza il livello **Consigliato** di Anti-Spam, qualsiasi messaggio il cui fattore di spam abbia un valore superiore al 60% verrà considerato come probabile spam. I messaggi per i quali il valore del fattore è inferiore al 60%, vengono considerati posta utile. È possibile modificare il valore specificato.

Il fattore di spam definisce il valore che causerà l'assegnazione dello stato *Spam* a un messaggio, se superato. Qualsiasi messaggio il cui fattore abbia un valore superiore a quello specificato verrà considerato spam. Per impostazione predefinita, il fattore di spam è pari al 90% per il livello **Consigliato**. Questo significa che qualsiasi messaggio il cui fattore abbia un valore superiore al 90% verrà contrassegnato come spam. È possibile modificare il valore specificato.

➡ *Per modificare i valori impostati dei fattori di spam e probabile spam, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Spam**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra visualizzata, nella scheda **Metodi avanzati**, sezione **Fattore di spam**, configurare i fattori di spam e probabile spam.

SELEZIONE DELL'ALGORITMO DI RICONOSCIMENTO DELLO SPAM

L'analisi della posta Anti-Spam si basa sugli algoritmi di riconoscimento selezionati:

- ☑ **Analisi euristica**. Anti-Spam analizza i messaggi utilizzando le regole euristiche. L'analisi euristica è sempre abilitata.
- ☑ **Riconoscimento delle immagini (tecnologia GSG)**. Anti-Spam utilizza la tecnologia GSG per rilevare lo spam grafico.
- ☑ **Analisi degli allegati in formato RTF**. Anti-Spam analizza i documenti allegati ai messaggi per verificare che non contengano segni di spam.
- ☑ **Algoritmo di riconoscimento del testo con autoistruzione (iBayes)**. L'algoritmo iBayes definisce se un messaggio è spam o non spam in base alla frequenza nel testo di parole tipiche dei messaggi spam. Prima di utilizzare l'algoritmo iBayes è necessario addestrarlo (vedere la sezione "Addestramento di Anti-Spam" a pagina 109).

- *Per abilitare/disabilitare uno specifico algoritmo di riconoscimento spam per l'analisi dei messaggi di posta elettronica, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Spam**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra visualizzata, nella scheda **Metodi avanzati**, sezione **Algoritmi di riconoscimento** selezionare/deselezionare le caselle corrispondenti ☑.

UTILIZZO DELLE FUNZIONI AVANZATE DI FILTRAGGIO ANTI-SPAM

Oltre alle proprietà di base utilizzate per filtrare i messaggi, ad esempio elenchi di mittenti consentiti e bloccati e algoritmi di riconoscimento, è possibile specificare altri elementi. In base a tali funzioni, a un messaggio verrà assegnato lo stato *spam* con un determinato grado di probabilità.

- *Per abilitare/disabilitare singole proprietà di filtraggio anti-spam aggiuntive, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Spam**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra visualizzata, nella scheda **Metodi avanzati**, fare clic sul pulsante **Avanzate**.
6. Nella finestra **Avanzate** visualizzata, selezionare/deselezionare le caselle ☑ accanto ai segni di spam desiderati.

AGGIUNTA DI UN'ETICHETTA ALL'OGGETTO DEL MESSAGGIO

È possibile aggiungere le etichette **[!! SPAM]** o **[?? Probable Spam]** al campo **Oggetto** dei messaggi in modo che vengano riconosciuti come spam o probabile spam dopo un controllo.

- *Per abilitare/disabilitare l'aggiunta delle etichette nel campo Oggetto dei messaggi, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Spam**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra **Avanzate** visualizzata, selezionare/deselezionare le caselle desiderate ☑ nella sezione **Azioni**. È possibile modificare il testo dell'etichetta.

FILTRAGGIO DEI MESSAGGI DI POSTA SUL SERVER. GESTORE DELLA POSTA

I messaggi di posta presenti sul server possono essere visualizzati anche senza essere scaricati nel computer. Questo consente di rifiutare alcuni messaggi in modo da risparmiare tempo, ridurre il traffico durante l'utilizzo della posta e diminuire inoltre il rischio di scaricare spam o virus nel computer.

Per gestire i messaggi presenti sul server viene utilizzato **il gestore della posta**. La finestra del gestore della posta viene visualizzata sempre prima del recupero della posta, a condizione che il componente sia abilitato.

Il gestore della posta si apre solo se la posta viene ricevuta tramite POP3 e non viene visualizzato se il server POP3 non supporta la visualizzazione delle intestazioni dei messaggi o se tutti i messaggi nel server provengono da indirizzi inclusi nell'elenco di mittenti consentiti.

L'elenco di messaggi presenti sul server viene visualizzato nella parte centrale della finestra del gestore. Selezionare il messaggio nell'elenco per analizzarne in modo dettagliato l'intestazione. La visualizzazione dell'intestazione può risultare utile, ad esempio, nella situazione seguente: gli spammer installano un programma dannoso nel computer del proprio collega e tale programma invia messaggi spam che includono il suo nome, utilizzando l'elenco contatti del suo client di posta. La probabilità che il proprio indirizzo sia presente nell'elenco contatti del collega è piuttosto elevata. È quasi certo dunque che la propria casella di posta verrà riempita di messaggi spam. In questi casi non è possibile stabilire se un messaggio è stato inviato dal collega o da uno spammer utilizzando solo l'indirizzo del mittente. Per questo motivo è utile controllare le intestazioni dei messaggi in modo da verificarne in particolare il mittente, la data e ora di invio nonché la dimensione. Se possibile, tenere traccia della route del messaggio dal mittente al server di posta, facendo riferimento all'intestazione. Tutte queste informazioni dovrebbero essere presenti nelle intestazioni. Grazie ai passaggi descritti sarà possibile decidere se scaricare un messaggio dal server o eliminarlo.

Per utilizzare il gestore della posta:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Spam**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra visualizzata, nella scheda **Avanzate**, sezione **Messaggi in entrata**, selezionare la casella **Apri il gestore della posta in arrivo durante la ricezione sul protocollo POP3**.

Per eliminare i messaggi dal server utilizzando il gestore della posta:

1. Selezionare la casella accanto al messaggio nella colonna **Elimina** della finestra del gestore della posta.
2. Fare clic sul pulsante **Elimina selezionati** nella parte superiore della finestra.

I messaggi verranno eliminati dal server. Si riceverà una notifica contrassegnata come **[!! SPAM]** ed elaborata in base alle regole impostate per il client di posta in uso.

ESCLUSIONE DI MESSAGGI DI MICROSOFT EXCHANGE SERVER DALLA SCANSIONE

È possibile escludere dalla scansione anti-spam i messaggi di posta elettronica provenienti dalla rete interna, ad esempio la posta aziendale. Tenere presente che tali messaggi verranno considerati come posta interna se si utilizza Microsoft Office Outlook in tutti i computer di rete e le caselle di posta degli utenti si trovano sullo stesso server di Exchange o su server collegati mediante connettori X400.

Per impostazione predefinita, il componente Anti-Spam non esamina i messaggi di Microsoft Exchange Server.

Se si desidera che Anti-Spam analizzi i messaggi:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Spam**.
4. Fare clic sul pulsante **Impostazioni** relativo al componente selezionato.
5. Nella finestra visualizzata, nella scheda **Avanzate**, sezione **Esclusioni**, deselezionare la casella **Non controllare i messaggi nativi di Microsoft Exchange Server**.

AZIONI DA ESEGUIRE CON LA POSTA SPAM

Se in seguito alla scansione vengono identificati messaggi contenenti spam o probabile spam, le azioni successive di Anti-Spam dipendono dallo stato dell'oggetto e dall'azione selezionata. Per impostazione predefinita, i messaggi di posta classificati come **spam** o probabile spam vengono modificati mediante l'aggiunta rispettivamente dell'etichetta **[!! SPAM]** o **[?? Probable Spam]** nel campo Oggetto del messaggio.

È possibile selezionare azioni supplementari da intraprendere sui messaggi classificati come spam o probabile spam. A tale scopo, nei client di Microsoft Office Outlook (vedere la sezione "Configurazione dell'elaborazione della posta spam in Microsoft Office Outlook" a pagina 123) e Microsoft Outlook Express (Windows Mail) (vedere la sezione "Configurazione dell'elaborazione della posta spam in Microsoft Outlook Express (Windows Mail)" a pagina 125) sono disponibili plug-in speciali. È inoltre possibile configurare regole di filtraggio per i client di posta The Bat! (vedere la sezione "Configurazione dell'elaborazione della posta spam in The Bat!" a pagina 125) e Thunderbird (vedere la sezione "Configurazione dell'elaborazione della posta spam in Thunderbird" a pagina 126).

VEDERE ANCHE:

Configurazione dell'elaborazione della posta spam in Microsoft Office Outlook....123

Configurazione dell'elaborazione della posta spam in Microsoft Outlook Express (Windows Mail)....125

Configurazione dell'elaborazione della posta spam in The Bat! 125

Configurazione dell'elaborazione della posta spam in Thunderbird....126

CONFIGURAZIONE DELL'ELABORAZIONE DELLA POSTA SPAM IN MICROSOFT OFFICE OUTLOOK

La finestra delle impostazioni di elaborazione dello spam si apre automaticamente alla prima esecuzione di Microsoft Outlook dopo aver installato Protezione del computer.

Per impostazione predefinita, i messaggi di posta elettronica classificati da Anti-Spam come spam o probabile spam sono segnalati da etichette speciali, **[!! SPAM]** o **[?? Probable Spam]**, nel campo **Oggetto**.

Ai messaggi classificati come spam e probabile spam è possibile assegnare le regole di elaborazione seguenti:

- **Sposta nella cartella**: il messaggio spam viene spostato nella cartella della casella di posta in arrivo specificata.
- **Copia nella cartella**: il messaggio di posta elettronica viene copiato e spostato nella cartella specificata. Il messaggio di posta elettronica originale viene salvato nella **Posta in arrivo**.
- **Elimina**: il messaggio spam viene eliminato dalla casella di posta dell'utente.
- **Ignora:** il messaggio di posta elettronica rimane nella cartella della **Posta in arrivo**.

A questo scopo, selezionare il valore appropriato nell'elenco a discesa nella sezione **Spam** o **Probabile spam**.

Quando si addestra Anti-Spam tramite il client di posta (vedere la sezione "Addestramento tramite il client di posta" a pagina 111), un messaggio contrassegnato viene inviato a Kaspersky Lab come esempio di spam. Fare clic sul collegamento **Azione aggiuntiva da eseguire dopo aver contrassegnato manualmente i messaggi come spam** per selezionare la modalità di trasferimento dell'esempio di spam nella finestra visualizzata. Fare clic sul collegamento **Azione aggiuntiva dopo aver contrassegnato manualmente i messaggi come non spam** per selezionare la modalità di invio degli esempi non di tipo spam, ovvero esempi erroneamente considerati come spam in precedenza.

È inoltre possibile selezionare l'algoritmo per il funzionamento standard di Microsoft Office Outlook e del plug-in Anti-Spam:

- **Scansione alla ricezione**. Tutti i messaggi di posta elettronica che arrivano nella cartella Posta in arrivo dell'utente vengono inizialmente elaborati in base alle regole di Microsoft Office Outlook. Al termine dell'elaborazione, i messaggi rimanenti che non rientrano in alcuna regola vengono elaborati dal plug-in Anti-Spam. In altre parole, i messaggi vengono elaborati in base alla priorità delle regole. Talvolta, la sequenza di priorità può essere ignorata se, ad esempio, nella Posta in arrivo giungono contemporaneamente molti messaggi. Di conseguenza, possono verificarsi casi in cui informazioni su un messaggio di posta elettronica elaborato da una regola di Microsoft Office Outlook vengono registrate nel rapporto Anti-Spam contrassegnato con lo stato *spam*. Per evitare che ciò accada, si consiglia di configurare il plug-in Anti-Spam come una regola di Microsoft Outlook.

- **Usa Regola di Microsoft Office Outlook**. Se si seleziona questa opzione, i messaggi in entrata vengono elaborati utilizzando la gerarchia delle regole di Microsoft Office Outlook, una delle quali deve essere una regola sull'elaborazione dei messaggi da parte di Anti-Spam. Si tratta della configurazione migliore in quanto non causa conflitti tra Microsoft Outlook e il plug-in Anti-Spam. L'unico inconveniente è la necessità di creare ed eliminare manualmente le regole di elaborazione dello spam attraverso Microsoft Office Outlook.

Per creare una regola di elaborazione dello spam:

1. Eseguire Microsoft Office Outlook e utilizzare il comando **Strumenti** → **Regole e avvisi** nel menu principale dell'applicazione. Il metodo utilizzato per accedere alla procedura guidata dipende dalla versione di Microsoft Office Outlook in uso. In questo file della Guida viene illustrato come creare una regola utilizzando Microsoft Office Outlook 2003.

2. Nella finestra **Regole e avvisi** visualizzata, nella scheda **Regole posta elettronica**, fare clic sul pulsante **Nuova regola**. Verrà avviata la Creazione guidata Regole che include i passaggi seguenti:

   a. Scegliere se creare una regola ex novo o utilizzando un modello. Selezionare l'opzione **Crea nuova regola** e selezionare la condizione di scansione **Controlla messaggi in arrivo**. Fare clic sul pulsante **Avanti**.

   b. Fare clic sul pulsante **Avanti** nella finestra di configurazione delle condizioni di filtraggio dei messaggi senza selezionare alcuna casella. Confermare nella finestra di dialogo che si desidera applicare questa regola a tutti i messaggi ricevuti.

   c. Nella finestra di selezione delle azioni da applicare ai messaggi, selezionare la casella **esegui un'azione personalizzata** nell'elenco di azioni. Nella parte inferiore della finestra, fare clic sul collegamento **un'azione personalizzata**. Selezionare Kaspersky Anti-Spam dal menu a discesa nella finestra che viene visualizzata, quindi fare clic sul pulsante **OK**.

   d. Fare clic sul pulsante **Avanti** nella finestra delle esclusioni dalla regola senza selezionare alcuna casella.

   e. Nell'ultima finestra è possibile modificare il nome delle regola (quello predefinito è Kaspersky Anti-Spam). Verificare che la casella **Attiva regola** sia selezionata e fare clic sul pulsante **Fine**.

3. Per impostazione predefinita, la nuova regola viene posizionata all'inizio dell'elenco di regole nella finestra **Regole e avvisi**. Se si desidera, è possibile spostarla alla fine dell'elenco in modo che venga applicata per ultima ai messaggi di posta elettronica.

Tutti i messaggi di posta elettronica in arrivo vengono elaborati in base a queste regole. L'ordine in cui il programma applica le regole dipende dalla priorità assegnata a ciascuna di esse. Le regole vengono applicate a partire dall'inizio dell'elenco. Ogni regola successiva viene classificata con una priorità inferiore rispetto alla precedente. È possibile modificare la priorità di applicazione delle regole ai messaggi.

Se si desidera che la regola Anti-Spam non elabori ulteriormente i messaggi dopo l'applicazione di una regola, selezionare la casella **Interrompi l'elaborazione di ulteriori regole** nelle impostazioni delle regole (vedere il passaggio 3 della procedura di creazione delle regole).

Se si ha esperienza nella creazione di regole per l'elaborazione della posta in Microsoft Outlook, è possibile creare regole personalizzate per Anti-Spam in base all'algoritmo suggerito.

Le impostazioni di elaborazione dei messaggi classificati come spam e probabile spam per Microsoft Office Outlook sono visualizzate nella speciale scheda **Anti-Spam** della voce di menu **Strumenti** →**Opzioni**.

CONFIGURAZIONE DELL'ELABORAZIONE DELLA POSTA SPAM IN MICROSOFT OUTLOOK EXPRESS (WINDOWS MAIL)

La finestra delle impostazioni di elaborazione dello spam viene aperta quando si esegue il client dopo aver installato l'applicazione.

Per impostazione predefinita, i messaggi di posta elettronica classificati da Anti-Spam come spam o probabile spam sono segnalati da etichette speciali, **[!! SPAM]** o **[?? Probable Spam]**, nel campo **Oggetto**.

Ai messaggi classificati come spam e probabile spam è possibile assegnare le regole di elaborazione seguenti:

- **Sposta nella cartella**: il messaggio spam viene spostato nella cartella della casella di posta in arrivo specificata.
- **Copia nella cartella**: il messaggio di posta elettronica viene copiato e spostato nella cartella specificata. Il messaggio di posta elettronica originale viene salvato nella **Posta in arrivo**.
- **Elimina**: il messaggio spam viene eliminato dalla casella di posta dell'utente.
- **Ignora:** il messaggio di posta elettronica rimane nella cartella della Posta in arrivo.

Per definire la regola di elaborazione necessaria, selezionare il valore appropriato nell'elenco a discesa della sezione **Spam** o **Probabile spam**.

Quando si addestra Anti-Spam tramite il client di posta (vedere la sezione "Addestramento tramite il client di posta" a pagina 111), un messaggio contrassegnato viene inviato a Kaspersky Lab come esempio di spam. Fare clic sul collegamento **Azione aggiuntiva da eseguire dopo aver contrassegnato manualmente i messaggi come spam** per selezionare la modalità di trasferimento dell'esempio di spam nella finestra visualizzata. Fare clic sul collegamento **Azione aggiuntiva dopo aver contrassegnato manualmente i messaggi come non spam** per selezionare la modalità di invio degli esempi non di tipo spam, ovvero esempi erroneamente considerati come spam in precedenza.

La finestra per la configurazione dei metodi di elaborazione dello spam può essere aperta facendo clic sul pulsante **Impostazioni** accanto ad altri pulsanti di Anti-Spam sulla barra delle applicazioni: **Spam** e **Non spam**.

CONFIGURAZIONE DELL'ELABORAZIONE DELLA POSTA SPAM IN THE BAT!

Le azioni da eseguire in caso di spam e probabile spam in The Bat! sono definite dagli strumenti del client.

Per impostare le regole di elaborazione dello spam in The Bat!, eseguire le operazioni seguenti:

1. Selezionare **Impostazioni** dal menu **Proprietà** del client di posta.
2. Selezionare **Protezione spam** nella struttura ad albero delle impostazioni.

Le impostazioni visualizzate della protezione anti-spam sono applicabili a tutti i moduli Anti-Spam installati che supportano l'integrazione con The Bat!.

È necessario definire il livello di classificazione e specificare la modalità di gestione dei messaggi con un determinato fattore (in caso di Anti-Spam, la probabilità che un messaggio sia spam):

- Eliminare i messaggi con un fattore che supera il valore specificato;
- Trasferire i messaggi di posta con un determinato fattore in una cartella destinata allo spam;
- Trasferire nella cartella dello spam i messaggi classificati come spam con intestazioni speciali;
- Lasciare lo spam nella cartella **Posta in arrivo**.

Dopo aver elaborato un messaggio, Protezione del computer assegna ad esso lo stato di spam o probabile spam in base a un fattore con valore regolabile. The Bat! dispone di un algoritmo di classificazione dei messaggi personalizzato, anch'esso basato su un fattore di spam. Per evitare discrepanze tra la classificazione dello spam in Protezione del computer e in The Bat!, a tutti i messaggi controllati in Anti-Spam viene assegnato il fattore corrispondente allo stato del messaggio: Messaggio e-mail non spam – 0%, Probabile spam – 50%, Spam – 100%. Pertanto, la classificazione della posta di The Bat! corrisponde al fattore dello stato correlato e non al fattore della posta assegnato in Anti-Spam.

Per ulteriori informazioni sulle regole di classificazione e di elaborazione dello spam, consultare la documentazione relativa a The Bat!.

CONFIGURAZIONE DELL'ELABORAZIONE DELLA POSTA SPAM IN THUNDERBIRD

Per impostazione predefinita, i messaggi di posta elettronica classificati da Anti-Spam come spam o probabile spam sono segnalati da etichette speciali, **[!! SPAM]** o **[?? Probable Spam]**, nel campo **Oggetto**. Per eseguire azioni in presenza di tali messaggi in Thunderbird, utilizzare le regole del menu **Strumenti** → **Filtri messaggi**. Per ulteriori informazioni sull'utilizzo del client di posta, vedere la Guida di Mozilla Thunderbird.

Il modulo del plug-in Anti-Spam di Thunderbird consente di eseguire l'addestramento sulla base dei messaggi ricevuti e inviati mediante l'applicazione del client di posta e la verifica della presenza di messaggi spam nella propria corrispondenza sul server. Il modulo del plug-in è integrato in Thunderbird e inoltra i messaggi al componente Anti-Spam per effettuarne la scansione quando viene eseguito il comando del menu **Tools (Strumenti)** → **Run anti-spam filters in folder (Esegui filtri anti-spam nella cartella)**. In questo modo, il controllo dei messaggi viene eseguito da Protezione del computer anziché da Thunderbird, senza tutta alterare le funzionalità di Thunderbird.

Lo stato del modulo del plug-in Anti-Spam viene visualizzato come icona nella riga di stato di Thunderbird. Il colore grigio dell'icona informa l'utente che si è verificato un problema nel funzionamento del plug-in o che il componente Anti-Spam (vedere pagina 107) è disabilitato. Facendo doppio clic sull'icona, viene aperta la finestra di configurazione delle impostazioni di Protezione del computer. Per accedere alle impostazioni di configurazione di **Anti-Spam**, fare clic sul pulsante **Impostazioni** nella sezione **Anti-Spam**.

RIPRISTINO DELLE IMPOSTAZIONI PREDEFINITE DI ANTI-SPAM

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

Per ripristinare le impostazioni predefinite di Anti-Spam, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Spam**.
4. Nella sezione **Livello di protezione**, fare clic sul pulsante **Livello predefinito** relativo al componente selezionato.

ANTI-BANNER

Anti-Banner blocca le informazioni pubblicitarie contenute nei banner incorporati nelle interfacce di vari programmi installati nel computer o visualizzate online.

I banner pubblicitari non solo sono privi di informazioni utili, ma distolgono l'utente dal lavoro e aumentano il traffico sul computer. Anti-Banner blocca i più comuni tipi di banner attualmente conosciuti tramite maschere incluse nel pacchetto di installazione di Protezione del computer. È possibile disabilitare il blocco dei banner o creare elenchi personalizzati di banner autorizzati e bloccati.

Gli specialisti di Kaspersky Lab hanno compilato un elenco di maschere di banner pubblicitari in base a una ricerca di settore e hanno incluso tale elenco nel pacchetto di installazione di Protezione del computer. I banner pubblicitari che corrispondono alle maschere incluse nell'elenco verranno bloccati da Anti-Banner, a meno che il blocco dei banner non sia disabilitato. Per bloccare i banner con maschere di indirizzi non trovate nell'elenco standard, viene utilizzata l'analisi euristica (vedere la sezione "Utilizzo dell'analisi euristica" a pagina 127).

È inoltre possibile creare liste bianche (vedere la sezione "Creazione dell'elenco di indirizzi di banner consentiti" a pagina 128) e nere (vedere la sezione "Creazione dell'elenco di indirizzi di banner bloccati" a pagina 129) di banner per stabilire se bloccare o consentire un banner.

Dopo l'installazione di Protezione del computer, Anti-Banner è disabilitato.

Per modificare le impostazioni di Anti-Banner, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Banner**.
4. Apportare le modifiche desiderate alle impostazioni per il componente selezionato.

IN QUESTA SEZIONE:

Utilizzo dell'analisi euristica 127

Impostazioni avanzate del componente 128

Creazione dell'elenco di indirizzi di banner consentiti 128

Creazione dell'elenco di indirizzi di banner bloccati 129

Esportazione/importazione degli elenchi di banner 129

UTILIZZO DELL'ANALISI EURISTICA

I banner i cui indirizzi non sono inclusi nell'elenco standard possono essere esaminati utilizzando l'analizzatore euristico. Se è in uso, Protezione del computer analizzerà le immagini scaricate per verificare la presenza di caratteristiche tipiche dei banner. In base a tale analisi, l'immagine può essere identificata come banner e quindi bloccata.

Per iniziare a utilizzare l'analizzatore euristico:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Banner**.

4. Nella sezione **Metodi di scansione**, selezionare la casella **Usa l'analisi euristica** relativa al componente selezionato.

IMPOSTAZIONI AVANZATE DEL COMPONENTE

Gli specialisti di Kaspersky Lab hanno compilato un elenco di maschere di banner pubblicitari in base a una ricerca di settore e hanno incluso tale elenco nel pacchetto di installazione di Protezione del computer. I banner pubblicitari che corrispondono alle maschere incluse nell'elenco verranno bloccati da Anti-Banner, a meno che il blocco dei banner non sia disabilitato.

Durante la creazione degli elenchi di banner consentiti/bloccati, è possibile immettere l'indirizzo IP del banner o il relativo nome di simbolo (URL). Per evitare duplicati, è possibile utilizzare un'opzione avanzata che consente di convertire gli indirizzi IP in nomi di dominio e viceversa.

- *Per disabilitare l'utilizzo dell'elenco di banner inclusi nel pacchetto di installazione di Protezione del computer:*

  1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
  2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
  3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Banner**.
  4. Nella sezione **Metodi di scansione**, deselezionare la casella **Usa l'elenco dei banner comuni** relativa al componente selezionato.

- *Per utilizzare l'opzione di conversione degli indirizzi IP dei banner in nomi di dominio o dei nomi di dominio in indirizzi IP, eseguire le operazioni seguenti:*

  1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
  2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
  3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Banner**.
  4. Nella sezione **Metodi di scansione**, selezionare la casella **Risolvi gli indirizzi IP in nomi di dominio** relativa al componente selezionato.

CREAZIONE DELL'ELENCO DI INDIRIZZI DI BANNER CONSENTITI

Se è necessario escludere dal blocco determinati banner, un utente può creare un elenco di banner consentiti durante l'utilizzo di Protezione del computer. Tale elenco contiene le maschere dei banner pubblicitari consentiti.

- *Per aggiungere una nuova maschera all'elenco dei consentiti, eseguire le operazioni seguenti:*

  1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
  2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
  3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Banner**.
  4. Nella sezione **Avanzate**, selezionare la casella **Usa l'elenco degli indirizzi consentiti** per il componente selezionato e fare clic sul pulsante **Impostazioni**.
  5. Nella finestra **Elenco consentiti** visualizzata, fare clic sul collegamento **Aggiungi**.
  6. Immettere una maschera di banner consentito nella finestra **Maschera per l'indirizzo (URL)** visualizzata. Per sospendere l'uso di una maschera creata, non occorre eliminarla dall'elenco. Per renderla inattiva è sufficiente deselezionare la casella accanto a essa.

CREAZIONE DELL'ELENCO DI INDIRIZZI DI BANNER BLOCCATI

È possibile creare un elenco di indirizzi di banner vietati, che verranno bloccati da Anti-Banner appena rilevati.

Per aggiungere una nuova maschera alla lista nera, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Banner**.
4. Nella sezione **Avanzate**, selezionare la casella **Usa l'elenco degli indirizzi bloccati** per il componente selezionato e fare clic sul pulsante **Impostazioni**.
5. Nella finestra **Elenco bloccati** visualizzata, fare clic sul collegamento **Aggiungi**.
6. Immettere una maschera di banner bloccato nella finestra **Maschera per l'indirizzo (URL)** visualizzata. Per sospendere l'uso di una maschera creata, non occorre eliminarla dall'elenco. Per renderla inattiva è sufficiente deselezionare la casella accanto a essa.

ESPORTAZIONE/IMPORTAZIONE DEGLI ELENCHI DI BANNER

È possibile copiare da un computer a un altro gli elenchi creati di banner consentiti e bloccati. Durante l'esportazione dell'elenco, è possibile copiare solo l'elemento selezionato nell'elenco o l'intero elenco. Durante l'importazione, è possibile scegliere di aggiungere nuovi indirizzi all'elenco esistente o sostituire l'elenco esistente con quello importato.

Per copiare gli elenchi creati di banner consentiti/bloccati, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Banner**.
4. Nella sezione **Avanzate**, fare clic sul pulsante **Impostazioni** relativo all'elenco da copiare per il componente selezionato.
5. Nella finestra **Elenco consentiti** (o **Elenco bloccati**) visualizzata, utilizzare i collegamenti **Importa** o **Esporta**.

SCANSIONE DEL COMPUTER

La scansione del computer per la verifica della presenza di virus e vulnerabilità è una delle attività più importanti per garantire la sicurezza del computer. La scansione anti-virus consente di rilevare la diffusione di codice dannoso che per qualche motivo non è stato rilevato dalla protezione malware. La ricerca delle vulnerabilità consente di rilevare le vulnerabilità software che gli utenti malintenzionati possono utilizzare per diffondere oggetti dannosi e ottenere l'accesso a informazioni personali.

Kaspersky Lab distingue tra le varie attività di scansione anti-virus (vedere pagina 130), inclusa la scansione delle unità rimovibili (vedere pagina 136) e la scansione della vulnerabilità del sistema e delle applicazioni (vedere pagina 140).

Per modificare le impostazioni di qualsiasi attività di scansione:

1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.

2. Nella parte sinistra della finestra, selezionare l'attività richiesta nella sezione **Scansione** (**Scansione Completa**, **Scansione Rapida**, **Scansione Personalizzata**, **Scansione Vulnerabilità**).

3. Apportare le modifiche desiderate alle impostazioni dell'attività selezionata.

IN QUESTA SEZIONE:

Scansione anti-virus 130

Scansione Vulnerabilità 140

SCANSIONE ANTI-VIRUS

Gli specialisti di Kaspersky Lab distinguono diversi tipi di attività di scansione anti-virus:

- **Scansione Personalizzata**. Gli oggetti selezionati dall'utente vengono sottoposti a scansione. È possibile eseguire la scansione di tutti gli oggetti del file system del computer. Durante questa attività è possibile configurare le impostazioni per la scansione delle unità rimovibili.

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

- **Scansione Rapida**. Viene eseguita la scansione degli oggetti di avvio del sistema operativo.

Le attività Scansione Completa e Scansione Rapida sono attività specifiche. È consigliabile non modificare l'elenco di oggetti esaminati da queste attività.

Ogni attività di scansione viene eseguita nell'area specificata e può essere avviata in base alla pianificazione creata. Un insieme di parametri delle attività di scansione anti-virus definisce il livello di protezione. Per impostazione predefinita, sono disponibili tre livelli.

Dopo l'avvio dell'attività di scansione anti-virus, lo stato di avanzamento viene visualizzato nella sezione **Scansione** della finestra principale di Protezione del computer, nel campo con il nome dell'attività avviata. In seguito al rilevamento di una minaccia, l'applicazione esegue l'azione specificata.

Durante la ricerca di minacce, le informazioni sui risultati vengono registrate in un rapporto di Protezione del computer.

Inoltre, è possibile selezionare un oggetto da esaminare con gli strumenti standard del sistema operativo Microsoft Windows, ad esempio, nella finestra del programma **Explorer** risorse o sul **Desktop**. Posizionare il cursore sul nome

dell'oggetto desiderato, fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida di Microsoft Windows e scegliere l'opzione **Scansione Anti-Virus del file**.

Figura 12. Menu di scelta rapida di Microsoft Windows

È inoltre possibile visualizzare il rapporto di scansione contenente tutte le informazioni relative agli eventi verificatisi durante l'esecuzione dell'attività.

VEDERE ANCHE:

Avvio dell'attività di scansione anti-virus 131

Creazione di un collegamento per l'esecuzione di attività 133

Creazione di un elenco di oggetti da esaminare 133

Modifica del livello di protezione 134

Modifica delle azioni da eseguire sugli oggetti rilevati 134

Modifica del tipo di oggetti da esaminare 135

Ottimizzazione della scansione 135

Scansione di unità disco rimovibili 136

Scansione dei file compositi 136

Tecnologia di scansione 137

Modifica del metodo di scansione 138

Modalità di esecuzione: creazione di una pianificazione 138

Modalità di esecuzione: specifica di un account 139

Funzionalità dell'avvio pianificato delle attività 139

Ripristino delle impostazioni di scansione predefinite 140

AVVIO DELL'ATTIVITA DI SCANSIONE ANTI-VIRUS

Un'attività di scansione anti-virus può essere avviata in uno dei modi seguenti:

- dal menu di scelta rapida di Protezione del computer (vedere la sezione "Menu di scelta rapida" a pagina 42);
- dalla finestra principale di Protezione del computer (vedere la sezione "Protezione del computer" a pagina 45);
- utilizzando un collegamento esistente (vedere pagina 133).

Le informazioni sull'esecuzione dell'attività verranno visualizzate nella finestra principale di Protezione del computer.

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

Figura 13. Menu di scelta rapida di Microsoft Windows

Per avviare l'attività utilizzando un collegamento:

1. Aprire la cartella in cui è stato creato il collegamento.
2. Avviare l'attività facendo doppio clic su un collegamento. Lo stato di avanzamento dell'esecuzione dell'attività verrà visualizzato nella finestra principale di Protezione del computer nella sezione **Scansione**.

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

1. Fare clic con il pulsante destro del mouse sull'icona nell'area di notifica della barra delle applicazioni.
2. Selezionare la voce **Scansione Anti-Virus** nel menu di scelta rapida visualizzato.
3. Nella finestra principale di Protezione del computer, nella sezione **Scansione**, fare clic sul pulsante con il nome dell'attività richiesta.

Per avviare la scansione completa del computer, selezionare la voce **Scansione Completa** dal menu di scelta rapida. Verrà avviata una scansione completa del computer Lo stato di avanzamento dell'esecuzione dell'attività verrà visualizzato nella finestra principale di Protezione del computer nella sezione **Scansione**.

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

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione**.
3. Fare clic sul pulsante che riporta il nome dell'attività richiesta.

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

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

CREAZIONE DI UN COLLEGAMENTO PER L'ESECUZIONE DI ATTIVITA

L'applicazione offre l'opportunità di creare collegamenti per avviare rapidamente attività di scansione completa e attività di scansione rapida. Ciò consente di avviare l'attività di scansione richiesta senza aprire la finestra dell'applicazione principale o il menu di scelta rapida.

Per creare un collegamento per l'avvio di un'attività di scansione, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul. collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione**.
3. Nella parte destra della finestra, nella sezione **Esecuzione rapida delle attività di scansione**, fare clic sul pulsante **Crea collegamento** accanto al nome dell'attività richiesta (**Scansione Rapida** oppure **Scansione Completa**).
4. Nella finestra che viene visualizzata specificare il percorso in cui salvare il collegamento. Per impostazione predefinita, il collegamento viene creato con il nome di un'attività nella cartella *Risorse del computer* dell'utente corrente.

CREAZIONE DI UN ELENCO DI OGGETTI DA ESAMINARE

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

Gli oggetti vengono visualizzati nell'elenco subito dopo essere stati aggiunti. Se si seleziona la casella **Includi sottocartelle** mentre si aggiunge un oggetto, la scansione verrà eseguita in modo ricorsivo.

Per eliminare un oggetto dall'elenco, selezionarlo e fare clic sul collegamento **Elimina**.

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

Oltre a eliminare gli oggetti dall'elenco, è possibile anche ignorarli temporaneamente durante l'esecuzione di una scansione. A tal fine, selezionare l'oggetto dall'elenco e deselezionare la casella a sinistra del nome dell'oggetto.

Se l'ambito di scansione è vuoto o non contiene oggetti selezionati, l'attività di scansione manuale non può essere avviata.

Per creare l'elenco di oggetti per un'attività di scansione oggetti, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione**.
3. Fare clic sul collegamento **Aggiungi**.
4. Nella finestra **Scelta degli oggetti da esaminare** visualizzata, selezionare un oggetto e fare clic sul pulsante **Aggiungi**. Fare clic sul pulsante **OK** dopo aver aggiunto tutti gli oggetti necessari. Per escludere un oggetto dall'elenco di oggetti da esaminare, deselezionare la relativa casella.

Per creare l'elenco di oggetti da sottoporre a scansione rapida o completa, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Impostazioni** nella parte superiore.
2. Nella parte sinistra della finestra selezionare l'attività **Scansione Completa** (**Scansione Rapida**).
3. Nella sezione **Ambito della scansione**, fare clic sul pulsante **Impostazioni** per l'attività selezionata.

4. Nella finestra **<Nome attività scansione>: elenco di oggetti** visualizzata, creare l'elenco utilizzando i collegamenti **Aggiungi**, **Modifica**, **Elimina**. Per escludere un oggetto dall'elenco di oggetti da esaminare, deselezionare la relativa casella.

MODIFICA DEL LIVELLO DI PROTEZIONE

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

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

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

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

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella parte sinistra della finestra, selezionare l'attività richiesta nella sezione **Scansione** (**Scansione Completa**, **Scansione Rapida**, **Scansione Personalizzata**).
4. Nella sezione **Livello di protezione**, impostare il livello di protezione necessario per l'attività selezionata.

MODIFICA DELLE AZIONI DA ESEGUIRE SUGLI OGGETTI RILEVATI

Alle minacce appena rilevate Protezione del computer assegna uno degli stati seguenti:

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

Se Protezione del computer rileva oggetti infetti o potenzialmente infetti durante una scansione anti-virus, ne dà notifica all'utente. È necessario rispondere alla minaccia incombente selezionando un'azione da eseguire sull'oggetto. Protezione del computer seleziona l'opzione **Chiedi di scegliere un'azione** come azione da eseguire su un oggetto rilevato, che rappresenta l'impostazione predefinita. È possibile modificare l'azione. Se, ad esempio, si desidera eseguire un tentativo di disinfezione per ogni oggetto rilevato ma non si desidera selezionare l'azione **Disinfetta** ogni volta che si riceve un avviso sul rilevamento di un oggetto infetto o sospetto, è necessario selezionare l'azione: **Seleziona azione. Disinfetta.**

Prima di provare a disinfettare o eliminare un oggetto infetto, Protezione del computer ne crea una copia di backup per consentirne il ripristino o la disinfezione in un secondo momento.

Se si lavora in modalità automatica (vedere la sezione "Passaggio 3. Selezione della modalità di protezione" a pagina 33), Protezione del computer applicherà automaticamente l'azione consigliata dagli specialisti di Kaspersky Lab quando vengono rilevati oggetti pericolosi. Per gli oggetti dannosi, tale azione sarà **Disinfetta. Elimina se la disinfezione fallisce** e **ignora** per gli oggetti sospetti.

Per modificare l'azione specificata da eseguire sugli oggetti rilevati:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella parte sinistra della finestra, selezionare l'attività richiesta nella sezione **Scansione** (**Scansione Completa**, **Scansione Rapida**, **Scansione Personalizzata**).
4. Nella sezione **Azione** specificare l'azione richiesta per l'attività selezionata.

MODIFICA DEL TIPO DI OGGETTI DA ESAMINARE

Quando si specifica il tipo di oggetti da esaminare, vengono definiti il formato e le dimensioni dei file su cui verrà eseguita l'attività di scansione selezionata.

Quando si seleziona il tipo di file, è necessario tenere presente quanto segue:

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

Per modificare il tipo di oggetto esaminato:

1. Aprire la finestra principaledell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella parte sinistra della finestra, selezionare l'attività richiesta nella sezione **Scansione** (**Scansione Completa**, **Scansione Rapida**, **Scansione Personalizzata**).
4. Nella sezione **Livello di protezione**, fare clic sul pulsante **Impostazioni** per l'attività selezionata.
5. Nella finestra visualizzata, scheda **Ambito**, sezione **Tipi di file**, selezionare le impostazioni richieste.

OTTIMIZZAZIONE DELLA SCANSIONE

È possibile ridurre il tempo di scansione e velocizzare le operazioni di Protezione del computer. Per ottenere questo risultato, è necessario eseguire la scansione solo dei file nuovi e dei file stati modificati dopo l'ultima scansione. Questa modalità si applica sia ai file semplici che compositi.

È inoltre possibile limitare la durata della scansione per un file. Una volta scaduto il tempo specificato, la scansione viene arrestata.

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

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella parte sinistra della finestra, selezionare l'attività richiesta nella sezione **Scansione** (**Scansione Completa**, **Scansione Rapida**, **Scansione Personalizzata**).
4. Nella sezione **Livello di protezione**, fare clic sul pulsante **Impostazioni** per l'attività selezionata.

5. Nella finestra visualizzata, nella scheda **Ambito**, sezione **Ottimizzazione della scansione**, selezionare la casella **Esamina solo i file nuovi e modificati**.

Per imporre una restrizione temporale alla durata della scansione:

1. Aprire la finestra principaledell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella parte sinistra della finestra, selezionare l'attività richiesta nella sezione **Scansione** (**Scansione Completa**, **Scansione Rapida**, **Scansione Personalizzata**).
4. Nella sezione **Livello di protezione**, fare clic sul pulsante **Impostazioni** per l'attività selezionata.
5. Nella finestra visualizzata, scheda **Ambito**, sezione **Ottimizzazione della scansione**, selezionare la casella **Ignora i file esaminati per più di** e specificare la durata della scansione nel campo corrispondente.

SCANSIONE DI UNITA DISCO RIMOVIBILI

Gli oggetti dannosi che utilizzano le vulnerabilità del sistema operativo per replicarsi tramite reti e supporti rimovibili si stanno diffondendo sempre di più.

Utilizzare l'opzione che consente di eseguire la scansione delle unità rimovibili nel momento in cui vengono collegate al computer. A tale scopo, è necessario selezionare una delle azioni da eseguire con Protezione del computer:

- **Non eseguire scansione**. Le unità disco rimovibili vengono esaminate automaticamente durante la connessione a un computer.
- **Chiedi all'utente**. Per impostazione predefinita, Protezione del computer richiede all'utente di eseguire altre azioni quando viene connessa un'unità rimovibile.
- **Scansione Completa**. Durante il collegamento di unità rimovibili, l'applicazione esegue una scansione completa dei file memorizzati al suo interno, in base alle impostazioni dell'attività Scansione Completa.
- **Scansione Rapida**. Durante il collegamento di unità rimovibili, l'applicazione esegue una scansione di tutti i file, in base alle impostazioni dell'attività Scansione Rapida.

Per utilizzare la funzionalità di scansione dei supporti rimovibili al momento della connessione, eseguire la procedura seguente:

1. Aprire la finestraAprire la finestra principale dell'applicazione e fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione**.
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.

SCANSIONE DEI FILE COMPOSITI

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

Per ogni tipo di file composito, è possibile scegliere di analizzare tutti i file oppure solo quelli nuovi. Per farlo, utilizzare il collegamento accanto al nome dell'oggetto. Il relativo valore verrà modificato quando si fa clic con il pulsante sinistro del mouse su di esso. Se si seleziona la modalità di scansione dei soli file nuovi e modificati (vedere pagina 135), non sarà possibile selezionare i tipi di file compositi da sottoporre a scansione.

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

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

Per modificare l'elenco dei file compositi esaminati:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella parte sinistra della finestra, selezionare l'attività richiesta nella sezione **Scansione** (**Scansione Completa**, **Scansione Rapida**, **Scansione Personalizzata**).
4. Nella sezione **Livello di protezione**, fare clic sul pulsante **Impostazioni** per l'attività selezionata.
5. Nella finestra visualizzata, nella scheda **Ambito**, sezione **Scansione dei file compositi**, selezionare il tipo di file compositi richiesto da esaminare.

Per impostare la dimensione massima dei file compositi da esaminare:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella parte sinistra della finestra, selezionare l'attività richiesta nella sezione **Scansione** (**Scansione Completa**, **Scansione Rapida**, **Scansione Personalizzata**).
4. Nella sezione **Livello di protezione**, fare clic sul pulsante **Impostazioni** per l'attività selezionata.
5. Nella finestra visualizzata, nella scheda **Ambito**, sezione **Scansione dei file compositi**, fare clic sul pulsante **Avanzate**.
6. Nella finestra **File compositi** visualizzata, selezionare la casella **Non decomprimere file composti molto grandi** e specificare la dimensione di file nel campo sottostante.

TECNOLOGIA DI SCANSIONE

È possibile anche specificare la tecnologia che verrà utilizzata durante la scansione, scegliendo una delle due alternative disponibili:

- **Tecnologia iChecker**. Questa tecnologia è in grado di aumentare la velocità di scansione escludendo determinati oggetti dalla scansione. Un oggetto viene escluso dalla scansione utilizzando uno speciale algoritmo che prende in considerazione la data di rilascio del database del programma, la data dell'ultima scansione dell'oggetto e le modifiche alle impostazioni di scansione.

  Si supponga, ad esempio, di disporre di un file archivio a cui dopo la scansione da parte di Protezione del computer è stato assegnato lo stato *non infetto*. Alla scansione successiva, l'applicazione ignorerà questo archivio, a meno che non sia stato modificato o non siano state modificate le impostazioni di scansione. Se la struttura dell'archivio risulta modificata perché è stato aggiunto un nuovo oggetto oppure se le impostazioni di scansione sono state modificate o i database dell'applicazione aggiornati, il programma esaminerà nuovamente l'archivio.

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

- **Tecnologia iSwift**. Questa tecnologia è stata sviluppata a partire dalla tecnologia iChecker per i computer che utilizzano un file system di tipo NTFS. Anche iSwift presenta delle limitazioni: è associata a un percorso di file specifico nel file system e può essere applicata solo ad oggetti in NTFS.

Per cambiare tecnologia di scansione degli oggetti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella parte sinistra della finestra, selezionare l'attività richiesta nella sezione **Scansione** (**Scansione Completa**, **Scansione Rapida**, **Scansione Personalizzata**).
4. Nella sezione **Livello di protezione**, fare clic sul pulsante **Impostazioni** per l'attività selezionata.
5. Nella finestra visualizzata, nella scheda **Avanzate**, sezione **Tecnologie di scansione**, selezionare il valore dell'impostazione richiesta.

MODIFICA DEL METODO DI SCANSIONE

È possibile modificare le impostazioni di scansione che ne determinano l'accuratezza. Per impostazione predefinita, la modalità di utilizzo dei record del database dell'applicazione per cercare le minacce è sempre abilitata. Inoltre, è possibile applicare diversi metodi e tecnologie di scansione (vedere pagina 137).

La modalità di scansione nella quale Protezione del computer confronta l'oggetto rilevato con le voci nel relativo database è nota come *analisi delle firme* e viene sempre utilizzata per impostazione predefinita. Inoltre, è sempre possibile utilizzare l'*analisi euristica*. Questo metodo presuppone l'analisi delle azioni eseguite da un oggetto all'interno del sistema. Se tali azioni sono tipiche di oggetti nocivi, è probabile che l'oggetto venga classificato come nocivo o sospetto.

Inoltre, è possibile impostare il livello di dettaglio delle scansioni, **superficiale**, **media** o **approfondita**, spostando il cursore nella posizione selezionata.

Oltre a tali metodi di scansione è possibile utilizzare la scansione rootkit. I rootkit sono insiemi di strumenti in grado di nascondere i programmi dannosi nel sistema operativo. Queste utilità vengono inserite nel sistema, nascondendo la loro presenza e quella dei processi, delle cartelle e delle chiavi di registro di altri programmi dannosi installati con il rootkit. Se la scansione è abilitata, è possibile specificare il livello dettagliato (analisi avanzata) per la rilevazione dei rootkit che eseguono una scansione accurata di tali programmi attraverso l'analisi di un gran numero di oggetti di vario tipo.

Per specificare il metodo di scansione da utilizzare:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella parte sinistra della finestra, selezionare l'attività richiesta nella sezione **Scansione** (**Scansione Completa**, **Scansione Rapida**, **Scansione Personalizzata**).
4. Nella sezione **Modalità di esecuzione**, fare clic sul pulsante **Impostazioni** per l'attività selezionata.
5. Nella finestra visualizzata, nella scheda **Avanzate**, sezione **Metodi di scansione**, selezionare i valori necessari per le impostazioni.

MODALITÀ DI ESECUZIONE: CREAZIONE DI UNA PIANIFICAZIONE

È possibile creare una pianificazione per avviare automaticamente le attività di scansione anti-virus.

L'impostazione principale riguarda l'intervallo di tempo tra gli avvii dell'attività. Per modificarla, specificare le impostazioni della pianificazione per l'opzione selezionata.

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

Per modificare una pianificazione per le attività di scansione:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella parte sinistra della finestra, selezionare l'attività richiesta nella sezione **Scansione** (**Scansione Completa**, **Scansione Rapida**, **Scansione Personalizzata**).
4. Nella sezione **Modalità di esecuzione**, fare clic sul pulsante **Impostazioni** per l'attività selezionata.
5. Nella finestra visualizzata, nella scheda **Modalità di esecuzione**, sezione **Pianificazione**, selezionare l'opzione **Manualmente** per avviare un'attività di scansione quando lo si ritiene più opportuno. Per eseguire l'attività periodicamente, selezionare **In base alla pianificazione** e creare una pianificazione di avvio dell'attività.

Per configurare l'avvio automatico delle attività ignorate:

1. Aprire la finestra principaledell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella parte sinistra della finestra, selezionare l'attività richiesta nella sezione **Scansione** (**Scansione Completa**, **Scansione Rapida**, **Scansione Personalizzata**).
4. Nella sezione **Modalità di esecuzione**, fare clic sul pulsante **Impostazioni** per l'attività selezionata.
5. Nella finestra visualizzata, nella scheda **Modalità di esecuzione**, sezione **Pianificazione**, selezionare la casella **Esegui attività ignorate**.

MODALITA DI ESECUZIONE: SPECIFICA DI UN ACCOUNT

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

Per specificare un account:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella parte sinistra della finestra, selezionare l'attività richiesta nella sezione **Scansione** (**Scansione Completa**, **Scansione Rapida**, **Scansione Personalizzata**).
4. Nella sezione **Modalità di esecuzione**, fare clic sul pulsante **Impostazioni** per l'attività selezionata.
5. Nella finestra visualizzata, nella scheda **Modalità di esecuzione**, sezione **Account utente**, selezionare la casella **Esegui l'attività come**. Specificare il nome utente e la password.

FUNZIONALITA DELL'AVVIO PIANIFICATO DELLE ATTIVITA

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

Le attività pianificate includono funzionalità aggiuntive, ad esempio la possibilità di *sospendere la scansione pianificata quando lo screensaver è inattivo o il computer è sbloccato*. Questa funzionalità consente di rimandare l'avvio dell'attività finché l'utente non avrà terminato di lavorare al computer. Pertanto, l'attività di scansione non richiederà l'utilizzo delle risorse del sistema durante le ore lavorative.

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

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.

2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.

3. Nella parte sinistra della finestra, selezionare l'attività richiesta nella sezione **Scansione** (**Scansione Completa**, **Scansione Rapida**, **Scansione Personalizzata**).

4. Nella sezione **Modalità di esecuzione**, fare clic sul pulsante **Impostazioni** per l'attività selezionata.

5. Nella finestra visualizzata, nella scheda **Modalità di esecuzione**, sezione **Pianificazione**, selezionare la casella **Sospendi la scansione se lo screensaver non è attivo e il computer non è bloccato**.

RIPRISTINO DELLE IMPOSTAZIONI DI SCANSIONE PREDEFINITE

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

Per ripristinare le impostazioni di scansione dei file predefinite:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.

2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.

3. Nella parte sinistra della finestra, selezionare l'attività richiesta nella sezione **Scansione** (**Scansione Completa**, **Scansione Rapida**, **Scansione Personalizzata**).

4. Nella sezione **Livello di protezione**, fare clic sul pulsante **Livello predefinito** per l'attività selezionata.

SCANSIONE VULNERABILITÀ

L'attività di ricerca delle vulnerabilità consiste nella diagnostica della protezione del sistema e nella ricerca di vulnerabilità potenziali utilizzate da utenti malintenzionati per arrecare danni ai computer.

Durante la ricerca delle vulnerabilità, l'applicazione analizza il sistema e cerca eventuali anomalie e danni presenti nelle impostazioni del browser e del sistema operativo. La diagnostica della protezione presenta diversi aspetti quali la ricerca di installazioni Rootkit (ovvero programmi per il monitoraggio segreto di un sistema violato da un hacker), la ricerca di servizi e impostazioni vulnerabili e la raccolta di informazioni su processi e driver.

La diagnostica del sistema alla ricerca di eventuali vulnerabilità può richiedere diversi minuti. Quando è completa, le informazioni raccolte vengono analizzate per valutare i problemi di protezione nell'ottica di una possibile minaccia al sistema.

Tutti i problemi rilevati durante la fase di analisi del sistema vengono raggruppati in base al livello di pericolo che presentano. 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. Si tratta di 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 tutte le azioni appartenenti a questo gruppo.

- Le *azioni consigliate* eliminano i problemi che costituiscono un problema potenziale. È consigliabile eseguire anche tutte le azioni appartenenti a questo gruppo.

- Le *azioni aggiuntive* riparano i danni che non costituiscono una minaccia al momento ma che potrebbero minacciare la sicurezza del computer in futuro.

Il risultato della ricerca delle vulnerabilità potenziali nel sistema operativo e nelle applicazioni installate nel computer viene rappresentato da collegamenti diretti alle critical fix (aggiornamenti alle applicazioni).

Dopo l'avvio dell'attività di ricerca delle vulnerabilità (vedere pagina 141), ne viene visualizzato lo stato di avanzamento nella finestra principale dell'applicazione e nella finestra **Scansione Vulnerabilità**, nel campo **Fine**. Le vulnerabilità

rilevate durante la scansione del sistema e delle applicazioni vengono visualizzate nella stessa finestra, nelle schede **Vulnerabilità di sistema** e **Applicazioni vulnerabili**.

Durante la ricerca di minacce, le informazioni sui risultati vengono registrate in un rapporto di Protezione del computer.

Nella sezione **Scansione Vulnerabilità** della finestra delle impostazioni dell'applicazione, è possibile impostare una pianificazione iniziale (vedere pagina 142) e creare un elenco di oggetti da sottoporre a scansione per un'attività di ricerca delle vulnerabilità (vedere pagina 142), analogamente alle attività di scansione anti-virus. Per impostazione predefinita, le applicazioni già installate nel computer vengono selezionate come oggetti da esaminare.

VEDERE ANCHE:

Avvio dell'attività di ricerca delle vulnerabilità 141

Creazione di un collegamento per l'esecuzione di attività 141

Creazione di un elenco di oggetti da esaminare 142

Modalità di esecuzione: creazione di una pianificazione 142

Modalità di esecuzione: specifica di un account 143

AVVIO DELL'ATTIVITA DI RICERCA DELLE VULNERABILITA

L'attività di ricerca delle vulnerabilità può essere avviata nei modi seguenti:

- dalla finestra principale di Protezione del computer (vedere la sezione "Protezione del computer" a pagina 45);
- utilizzando un collegamento esistente (vedere pagina 141).

Le informazioni sull'esecuzione dell'attività vengono visualizzate nella finestra principale di Protezione del computer e nella finestra **Scansione Vulnerabilità**.

Per avviare l'attività utilizzando un collegamento:

1. Aprire la cartella in cui è stato creato il collegamento.
2. Avviare l'attività facendo doppio clic su un collegamento. Lo stato di avanzamento dell'attività verrà visualizzato nella finestra principale dell'applicazione.

Per avviare l'attività di ricerca delle vulnerabilità dalla finestra principale dell'applicazione:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione**.
3. Fare clic sul pulsante **Apri la finestra della Scansione Vulnerabilità**.
4. Nella finestra visualizzata, fare clic sul pulsante **Avvia Scansione Vulnerabilità**. Lo stato di avanzamento dell'esecuzione dell'attività verrà visualizzato nel campo **Fine**. Fare clic di nuovo sul pulsante per interrompere l'esecuzione dell'attività.

CREAZIONE DI UN COLLEGAMENTO PER L'ESECUZIONE DI ATTIVITÀ

L'applicazione offre l'opportunità di creare un collegamento per un avvio rapido dell'attività di ricerca delle vulnerabilità. Ciò consente di avviare l'attività senza aprire la finestra principale dell'applicazione.

Per creare un collegamento per l'avvio dell'attività di ricerca delle vulnerabilità:

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

CREAZIONE DI UN ELENCO DI OGGETTI DA ESAMINARE

L'attività di ricerca delle vulnerabilità include un elenco predefinito personalizzato di oggetti da esaminare. Questi oggetti contengono il sistema operativo e i programmi installati nel computer. È possibile anche specificare oggetti ulteriori da esaminare: oggetti del file system del computer (ad esempio, unità logiche, **database della posta**) o altri tipi di oggetti, ad esempio unità di rete.

Gli oggetti vengono visualizzati nell'elenco subito dopo essere stati aggiunti. Se si seleziona la casella **Includi sottocartelle** mentre si aggiunge un oggetto, la scansione verrà eseguita in modo ricorsivo. Gli oggetti aggiunti manualmente vengono anche sottoposti a una scansione anti-virus.

Per eliminare un oggetto dall'elenco, selezionarlo e fare clic sul collegamento **Elimina**.

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

Oltre a eliminare gli oggetti dall'elenco, è possibile anche ignorarli temporaneamente durante l'esecuzione di una scansione. A tal fine, selezionare l'oggetto dall'elenco e deselezionare la casella a sinistra del nome dell'oggetto.

Se l'ambito di scansione è vuoto o non contiene oggetti selezionati, l'attività di scansione manuale non può essere avviata.

Per creare l'elenco di oggetti per un'attività di ricerca delle vulnerabilità:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella parte sinistra della finestra, selezionare l'attività **Scansione Vulnerabilità** nella sezione **Scansione**.
4. Nella sezione **Ambito della scansione**, fare clic sul pulsante **Impostazioni** per l'attività selezionata.
5. Nella finestra **Scansione Vulnerabilità: elenco degli oggetti**, creare l'elenco utilizzando i collegamenti **Aggiungi**, **Modifica**, **Elimina**. Per escludere temporaneamente un oggetto dall'elenco di oggetti da esaminare, deselezionare la relativa casella.

MODALITA DI ESECUZIONE: CREAZIONE DI UNA PIANIFICAZIONE

È possibile pianificare l'esecuzione automatica dell'attività di ricerca delle vulnerabilità.

L'impostazione principale riguarda l'intervallo di tempo tra gli avvii dell'attività.

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

Per modificare una pianificazione per le attività di scansione:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella parte sinistra della finestra, selezionare l'attività **Scansione Vulnerabilità** nella sezione **Scansione**.
4. Nella sezione **Modalità di esecuzione**, fare clic sul pulsante **Impostazioni** per l'attività selezionata.
5. Nella finestra visualizzata, nella scheda **Modalità di esecuzione**, sezione **Pianificazione**, selezionare l'opzione **Manualmente** per avviare un'attività di scansione quando lo si ritiene più opportuno. Per eseguire l'attività periodicamente, selezionare **In base alla pianificazione** e creare una pianificazione di avvio dell'attività.

Per configurare l'avvio automatico delle attività ignorate:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella parte sinistra della finestra, selezionare l'attività **Scansione Vulnerabilità** nella sezione **Scansione**.
4. Nella sezione **Modalità di esecuzione**, fare clic sul pulsante **Impostazioni** per l'attività selezionata.
5. Nella finestra visualizzata, nella scheda **Modalità di esecuzione**, sezione **Pianificazione**, selezionare la casella **Esegui attività ignorate**.

MODALITA DI ESECUZIONE: SPECIFICA DI UN ACCOUNT

È possibile specificare un account utilizzato dall'applicazione durante l'esecuzione di un'attività di ricerca delle vulnerabilità.

Per specificare un account:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella parte sinistra della finestra, selezionare l'attività **Scansione Vulnerabilità** nella sezione **Scansione**.
4. Nella sezione **Modalità di esecuzione**, fare clic sul pulsante **Impostazioni** per l'attività selezionata.
5. Nella finestra visualizzata, nella scheda **Modalità di esecuzione**, sezione **Account utente**, selezionare la casella **Esegui l'attività come**. Specificare il nome utente e la password.

AGGIORNAMENTI

Mantenere l'applicazione aggiornata è un requisito fondamentale per garantire l'affidabilità della protezione del computer. Poiché ogni giorno nascono nuovi virus, Trojan e software dannosi, è importante aggiornare regolarmente l'applicazione per proteggere costantemente i dati personali. Le informazioni sulle minacce e i metodi che consentono di neutralizzarle sono memorizzate nei database di Protezione del computer. L'aggiornamento tempestivo di tali database è quindi un'operazione fondamentale per garantire una protezione affidabile.

L'aggiornamento dell'applicazione viene scaricato e comporta l'installazione degli aggiornamenti seguenti nel computer:

- Database di Protezione del computer.

  La protezione delle informazioni è basata su database contenenti le firme delle minacce e gli attacchi di rete, nonché i metodi per contrastarli. I componenti della protezione li utilizzano per rilevare e disinfettare gli oggetti pericolosi sul computer. I database vengono aggiornati ogni ora con nuove voci relative alle nuove minacce. È pertanto consigliabile aggiornarli regolarmente.

  Oltre ai database di Protezione del computer, 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 Protezione del computer, è possibile aggiornare i moduli del programma. I pacchetti di aggiornamento eliminano le vulnerabilità di Protezione del computer e aggiungono funzionalità nuove o migliorate.

I server degli aggiornamenti di Kaspersky Lab sono la principale origine degli aggiornamenti per Protezione del computer.

Per scaricare dai server gli aggiornamenti disponibili è necessario disporre di una connessione Internet. Per impostazione predefinita, le impostazioni di connessione a Internet vengono determinate automaticamente. Se le impostazioni del server proxy non vengono configurate automaticamente, è possibile configurare le impostazioni di connessione (vedere pagina 147) manualmente.

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

Se i database sono obsoleti, le dimensioni del pacchetto di aggiornamento possono essere piuttosto grandi e aumentare ulteriormente il traffico in Internet (fino a diverse decine di MB).

Prima di procedere all'aggiornamento dei database, Protezione del computer crea copie di backup di tali database qualora si decida di ripristinarne la versione precedente.

Potrebbe essere necessario utilizzare l'opzione di rollback dell'aggiornamento (vedere pagina 146) se, ad esempio, i database vengono danneggiati durante il processo di aggiornamento. È possibile eseguire facilmente il rollback alla versione precedente e cercare di aggiornare nuovamente i database.

È possibile copiare gli aggiornamenti recuperati (vedere pagina 148) in una sorgente locale durante l'aggiornamento di Protezione del computer. Questo servizio consente di aggiornare i database e i moduli del programma su computer di rete per non intasare il traffico in Internet.

È inoltre possibile configurare l'avvio dell'aggiornamento automatico.

Nella sezione **Aggiornamenti** della finestra principale dell'applicazione sono contenute informazioni sullo stato corrente dei database di Protezione del computer:

- data e ora di rilascio;
- numero di record del database e relativa composizione;
- stato dei database (aggiornati, obsoleti o danneggiati).

È possibile visualizzare il rapporto di aggiornamento contenente tutte le informazioni relative agli eventi verificatisi durante l'esecuzione dell'attività di aggiornamento facendo clic sul collegamento **Rapporto** nella parte superiore della finestra. Una panoramica sull'attività dei virus è disponibile nel sito Web www.kaspersky.com facendo clic sul collegamento **Osservatorio sui virus**.

IN QUESTA SEZIONE:

Avvio dell'aggiornamento 145

Rollback dell'ultimo aggiornamento 146

Sorgente degli aggiornamenti 146

Utilizzo di un server proxy 147

Impostazioni internazionali 147

Azioni da eseguire dopo l'aggiornamento 147

Aggiornamento da una cartella locale 148

Modifica della modalità di esecuzione dell'attività di aggiornamento 149

Esecuzione degli aggiornamenti utilizzando un altro account utente 149

AVVIO DELL'AGGIORNAMENTO

È possibile avviare l'aggiornamento di Protezione del computer in qualsiasi momento. Gli aggiornamenti vengono scaricati dalla sorgente degli aggiornamenti selezionata.

È possibile aggiornare Protezione del computer in uno dei seguenti modi:

- dal menu di scelta rapida (vedere la sezione "Menu di scelta rapida" a pagina 42);
- dalla finestra principale dell'applicazione (vedere la sezione "Protezione del computer" a pagina 45).

Le informazioni sull'aggiornamento verranno visualizzate nella sezione **Aggiornamenti** della finestra principale dell'applicazione.

Per avviare l'aggiornamento di Protezione del computer dal menu di scelta rapida:

1. Fare clic con il pulsante destro del mouse sull'icona nell'area di notifica della barra delle applicazioni.
2. Selezionare la voce **Aggiornamenti** dal menu a discesa.

Per avviare l'aggiornamento di Protezione del computer dalla finestra principale dell'applicazione:

1. Aprire la finestra principale dell'applicazione.
2. Nella finestra visualizzata, selezionare la sezione **Protezione del computer**.
3. Nella finestra visualizzata, selezionare la scheda **Aggiornamenti** e fare clic sul pulsante **Avvia aggiornamento**.

ROLLBACK DELL'ULTIMO AGGIORNAMENTO

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

L'opzione di rollback è utile, ad esempio, se una parte dei database è stata danneggiata. I database locali possono essere danneggiati dall'utente o da un programma dannoso. Ciò è possibile solo se la funzionalità Auto-Difesa di Kaspersky PURE (vedere pagina 247) è disabilitata. È possibile riportare i database allo stato precedente e ritentarne l'aggiornamento in un secondo momento.

Per eseguire il rollback alla versione precedente del database:

1. Aprire la finestra principale dell'applicazione.
2. Nella finestra visualizzata, selezionare la sezione **Protezione del computer**.
3. Nella finestra visualizzata, selezionare la scheda **Aggiornamenti** e fare clic sul pulsante **Rollback**.

SORGENTE DEGLI AGGIORNAMENTI

Per *sorgente degli aggiornamenti* si intende una risorsa contenente gli aggiornamenti per i database e i moduli di applicazione di Protezione del computer. Le sorgenti degli aggiornamenti possono essere server HTTP o FTP, cartelle locali o cartelle di rete.

La sorgente degli aggiornamenti principale è costituita dai server degli aggiornamenti di Kaspersky Lab. Si tratta di speciali siti Internet contenenti gli aggiornamenti disponibili per i database e i moduli di applicazione per tutti i prodotti Kaspersky Lab.

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

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

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

Per impostazione predefinita, l'elenco contiene solo i server degli aggiornamenti di Kaspersky Lab.

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

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

Per scegliere una sorgente degli aggiornamenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Selezionare la sezione **Aggiornamenti** nella parte sinistra della finestra.
4. Fare clic sul pulsante **Impostazioni** nella sezione **Sorgente dell'aggiornamento**.

5. Nella finestra visualizzata, nella scheda **Sorgente**, fare clic sul collegamento **Aggiungi**.

6. Selezionare un sito FTP o HTTP oppure immetterne l'indirizzo IP, il nome simbolico o l'URL nella finestra **Sorgente degli aggiornamenti** visualizzata.

UTILIZZO DI UN SERVER PROXY

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

Per configurare il server proxy, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.

2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.

3. Selezionare la sezione **Aggiornamenti** nella parte sinistra della finestra.

4. Fare clic sul pulsante **Impostazioni** nella sezione **Sorgente dell'aggiornamento**.

5. Nella finestra visualizzata, nella scheda **Sorgente**, fare clic sul pulsante **Server proxy**.

6. Modificare le impostazioni del server proxy nella finestra **Impostazioni del server proxy** visualizzata.

IMPOSTAZIONI INTERNAZIONALI

Se si utilizzano i server degli aggiornamenti 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. La scelta del server più vicino consente di risparmiare tempo e accelerare il download degli aggiornamenti.

Per scegliere il server più vicino:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.

2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.

3. Selezionare la sezione **Aggiornamenti** nella parte sinistra della finestra.

4. Fare clic sul pulsante **Impostazioni** nella sezione **Sorgente dell'aggiornamento**.

5. Nella finestra visualizzata, nella scheda **Sorgente**, sezione **Impostazioni internazionali**, selezionare la casella **Seleziona dall'elenco** e scegliere il paese più vicino alla propria posizione corrente nell'elenco a discesa.

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

AZIONI DA ESEGUIRE DOPO L'AGGIORNAMENTO

Protezione del computer consente inoltre di specificare le azioni che verranno eseguite automaticamente al termine dell'aggiornamento. È possibile eseguire le azioni seguenti:

- **Ripetere la scansione degli oggetti in Quarantena**. L'area di quarantena contiene oggetti che sono stati contrassegnati dall'applicazione come sospetti o possibilmente infetti. È possibile che al termine dell'aggiornamento del database il prodotto riesca a riconoscere la minaccia in modo inequivocabile e neutralizzarla. Di conseguenza, l'applicazione esegue la scansione degli oggetti in quarantena dopo ogni

aggiornamento. Per questo motivo, l'applicazione esegue la scansione degli oggetti in quarantena dopo ogni aggiornamento. La scansione potrebbe infatti modificarne lo stato e consentire quindi il ripristino di alcuni oggetti nelle posizioni precedenti in modo che l'utente possa continuare a utilizzarli.

- **Crea una copia degli aggiornamenti nella cartella**. Se i computer sono collegati in una rete LAN domestica, non è necessario scaricare e installare gli aggiornamenti individualmente su ciascuno di essi. È possibile utilizzare il servizio di distribuzione degli aggiornamenti per risparmiare larghezza di banda di rete, poiché il servizio garantisce che gli aggiornamenti vengono scaricati solo una volta.

Per esaminare i file in quarantena dopo la scansione:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Selezionare la sezione **Aggiornamenti** nella parte sinistra della finestra.
4. Selezionare la casella **Ripeti la scansione degli oggetti in Quarantena dopo l'aggiornamento** nella sezione **Avanzate**.

AGGIORNAMENTO DA UNA CARTELLA LOCALE

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

1. Uno dei computer della rete recupera un pacchetto di aggiornamento di Protezione del computer dai server degli aggiornamenti di Kaspersky Lab o da un server mirror che ospita la versione corrente degli aggiornamenti. Gli aggiornamenti recuperati vengono salvati in una cartella condivisa.
2. Gli altri computer della rete accedono alla cartella condivisa per recuperare gli aggiornamenti di Protezione del computer.

Per abilitare la modalità di distribuzione degli aggiornamenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Selezionare la sezione **Aggiornamenti** nella parte sinistra della finestra.
4. Selezionare la casella **Crea una copia degli aggiornamenti nella cartella** nella sezione **Avanzate** e specificare il percorso di una cartella condivisa in cui verranno copiati tutti gli aggiornamenti scaricati. È inoltre possibile selezionare il percorso nella finestra di dialogo visualizzata dopo aver fatto clic sul pulsante **Sfoglia**.

Se si desidera che gli aggiornamenti vengano eseguiti dalla cartella ad accesso pubblico selezionata, eseguire queste azioni su tutti i computer della rete:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Selezionare la sezione **Aggiornamenti** nella parte sinistra della finestra.
4. Fare clic sul pulsante **Impostazioni** nella sezione **Sorgente dell'aggiornamento**.
5. Nella finestra visualizzata, nella scheda **Sorgente**, fare clic sul collegamento **Aggiungi**.
6. Nella finestra **Sorgente degli aggiornamenti** visualizzata, selezionare una cartella o immetterne il percorso completo nel campo **Sorgente**.
7. Deselezionare la casella **Server degli aggiornamenti di Kaspersky Lab** nella scheda **Sorgente**.

MODIFICA DELLA MODALITA DI ESECUZIONE DELL'ATTIVITA DI AGGIORNAMENTO

È necessario selezionare la modalità di avvio per l'attività di aggiornamento di Protezione del computer quando la procedura guidata per la configurazione di Protezione del computer è attiva (vedere la sezione "Passaggio 4. Configurazione dell'aggiornamento dell'applicazione" a pagina 33). Se si desidera modificare la modalità di avvio dell'aggiornamento selezionata, è possibile riconfigurarla.

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

- **Automaticamente**. Protezione del computer verifica a intervalli specificati la disponibilità di aggiornamenti nella relativa sorgente. La frequenza della scansione può essere aumentata durante le epidemie e ridotta nei periodi più tranquilli. I nuovi aggiornamenti rilevati vengono scaricati e installati nel computer.
- **In base alla pianificazione** (l'intervallo di tempo cambia in base alle impostazioni). Gli aggiornamenti vengono eseguiti automaticamente in base alla pianificazione.
- **Manualmente**. Se si seleziona questa opzione, gli aggiornamenti verranno eseguiti manualmente.

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

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Selezionare la sezione **Aggiornamenti** nella parte sinistra della finestra.
4. Fare clic sul pulsante **Impostazioni** nella sezione **Modalità di esecuzione**.
5. Nella finestra visualizzata, nella scheda **Modalità di esecuzione**, selezionare la modalità di avvio dell'attività di aggiornamento nella sezione **Pianificazione**. Se l'opzione **In base alla pianificazione** è selezionata, creare la pianificazione.

   Se per qualsiasi motivo un aggiornamento viene saltato, ad esempio perché all'ora prevista il computer era spento, è possibile configurare l'attività in modo che inizi automaticamente non appena possibile. A tale scopo, è sufficiente selezionare la casella **Esegui attività ignorate** nella parte inferiore della finestra. Questa casella è disponibile per tutte le opzioni di pianificazione, ad eccezione di **Ore**, **Minuti** e **Dopo l'avvio dell'applicazione**.

ESECUZIONE DEGLI AGGIORNAMENTI UTILIZZANDO UN ALTRO ACCOUNT UTENTE

Per impostazione predefinita, la procedura di aggiornamento viene eseguita utilizzando il proprio account utente. Tuttavia, Protezione del computer può eseguire l'aggiornamento da un'origine per la quale non si dispone di privilegi di accesso, ad esempio una cartella di rete contenente aggiornamenti, o di credenziali utente per il server proxy. È possibile eseguire l'aggiornamento di Protezione del computer tramite l'account di un utente che dispone dei diritti necessari.

Per avviare l'aggiornamento utilizzando un altro account utente:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Selezionare la sezione **Aggiornamenti** nella parte sinistra della finestra.
4. Fare clic sul pulsante **Impostazioni** nella sezione **Modalità di esecuzione**.
5. Nella finestra visualizzata, nella scheda **Modalità di esecuzione**, sezione **Account utente**, selezionare la casella **Esegui l'attività come**. Specificare il nome utente e la password.

CONFIGURAZIONE DELLE IMPOSTAZIONI DI PROTEZIONE DEL COMPUTER

La finestra delle impostazioni dell'applicazione consente di accedere rapidamente alle principali impostazioni di Protezione del computer.

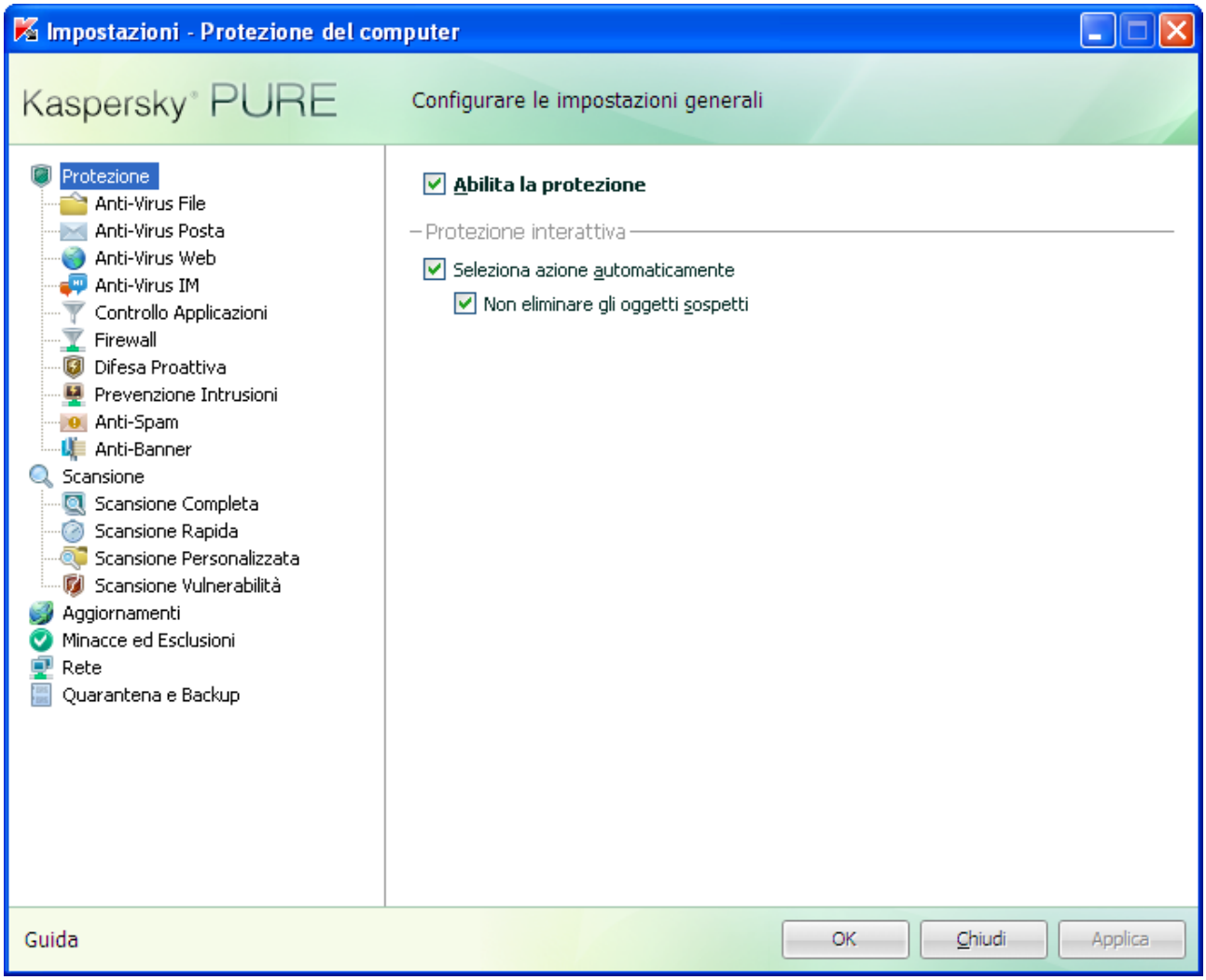


Figura 14. Finestra delle impostazioni dell'applicazione

La finestra delle impostazioni si compone di due parti:

- La parte sinistra della finestra consente di accedere a impostazioni di Protezione del computer, attività di scansione anti-virus, attività di aggiornamento e così via;
- la parte destra della finestra contiene un elenco di impostazioni relative al componente o all'attività selezionati nella parte sinistra della finestra.

È possibile aprire questa finestra:

- dalla finestra principale dell'applicazione (vedere la sezione "Protezione del computer" a pagina 45). Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.

- dal menu di scelta rapida (vedere la sezione "Menu di scelta rapida" a pagina 42); A tale scopo, selezionare la voce **Impostazioni** dal menu di scelta rapida.

Figura 15. Menu di scelta rapida

IN QUESTA SEZIONE:

Protezione 151
Anti-Virus File 153
Anti-Virus Posta 153
Anti-Virus Web 154
Anti-Virus IM 155
Controllo Applicazioni 155
Firewall 156
Difesa Proattiva 157
Prevenzione Intrusioni 158
Anti-Spam 158
Anti-Banner 159
Scansione 160
Aggiornamenti 161
Impostazioni 161

PROTEZIONE

Nella finestra **Protezione** è possibile utilizzare le funzioni avanzate di Protezione del computer elencate di seguito:

- Abilitazione / disabilitazione della protezione fornita da Protezione del computer (vedere pagina 152).
- Utilizzo della modalità di protezione interattiva (vedere pagina 152).

ABILITAZIONE/DISABILITAZIONE DELLA PROTEZIONE DEL COMPUTER

Per impostazione predefinita, Protezione del computer 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 Protezione del computer può essere abilitata 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.

Quando la protezione è disabilitata, tutti i componenti diventano inattivi. Vengono utilizzati i simboli seguenti:

- icona inattiva (in grigio) di Protezione del computer (vedere sezione "Icona dell'area di notifica" a pagina 42) nell'area di notifica della barra delle applicazioni;
- colore rosso dell'indicatore di protezione.

In questo caso, la protezione è descritta nel contesto dei componenti di protezione. La disabilitazione o la sospensione dei componenti di protezione non influisce sull'esecuzione delle attività di scansione anti-virus e degli aggiornamenti di Protezione del computer.

Per disabilitare completamente la protezione:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, selezionare la sezione **Protezione**.
4. Deselezionare la casella **Abilita la protezione**.

UTILIZZO DELLA MODALITA DI PROTEZIONE INTERATTIVA

Protezione del computer interagisce con l'utente in due modi:

- *Modalità di protezione interattiva*. Protezione del computer notifica all'utente tutti gli eventi pericolosi o sospetti che si verificano nel sistema. lasciandogli la libertà di scegliere se consentire o bloccare le azioni.
- *Modalità di protezione automatica*. Protezione del computer applica automaticamente le azioni raccomandate dagli specialisti di Kaspersky Lab in risposta al verificarsi di eventi pericolosi.

Per utilizzare la modalità di protezione automatica:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, selezionare la sezione **Protezione**.
4. Nella sezione **Protezione interattiva** selezionare la casella **Scegli l'azione automaticamente**. Se non si desidera che Protezione del computer elimini gli oggetti sospetti quando viene eseguito in modalità automatica, selezionare la casella **Non eliminare gli oggetti sospetti**.

ANTI-VIRUS FILE

In questa finestra sono raggruppate le impostazioni del componente Anti-Virus File (vedere la sezione "Protezione del file system del computer" a pagina 52). Modificando le impostazioni, è possibile eseguire le azioni seguenti:

- disabilitare Anti-Virus File;
- modificare il livello di protezione (vedere pagina 54);
- modificare l'azione da eseguire sugli oggetti rilevati (vedere pagina 54);
- creare un ambito di protezione (vedere pagina 55);
- ottimizzare la scansione (vedere pagina 56);
- configurare la scansione dei file compositi (vedere pagina 57);
- modificare la modalità di scansione (vedere pagina 58);
- utilizzare l'analisi euristica (vedere pagina 56).
- sospendere il componente (vedere pagina 59);
- selezionare una tecnologia di scansione (vedere pagina 58);
- ripristinare le impostazioni di protezione predefinite (vedere pagina 61) se sono state modificate.

Per disabilitare Anti-Virus File, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Virus File**.
4. Deselezionare la casella **Abilita Anti-Virus File** nella parte destra della finestra.

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

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Virus File**.
4. Nella parte destra della finestra, selezionare le impostazioni del componente relative al livello di protezione e alla reazione alle minacce. Fare clic sul pulsante **Impostazioni** per visualizzare le altre impostazioni di Anti-Virus File.

ANTI-VIRUS POSTA

In questa finestra sono raggruppate le impostazioni del componente Anti-Virus Posta (vedere la sezione "Protezione della posta" a pagina 62). Modificando le impostazioni, è possibile eseguire le azioni seguenti:

- disabilitare Anti-Virus Posta;
- modificare il livello di protezione (vedere pagina 63);
- modificare l'azione da eseguire sugli oggetti rilevati (vedere pagina 64);

- creare un ambito di protezione (vedere pagina 65);
- utilizzare l'analisi euristica (vedere pagina 67).
- configurare la scansione dei file compositi (vedere pagina 67);
- configurare il filtraggio degli oggetti allegati al messaggio di posta elettronica (vedere pagina 67);
- ripristinare le impostazioni di protezione della posta elettronica (vedere pagina 68).

Per disabilitare Anti-Virus Posta, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, selezionare il componente **Anti-Virus Posta** nella sezione **Protezione**.
4. Deselezionare la casella **Abilita Anti-Virus Posta** nella parte destra della finestra.

Per passare alle impostazioni di Anti-Virus Posta, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul. pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, selezionare il componente **Anti-Virus Posta** nella sezione **Protezione**.
4. Nella parte destra della finestra, selezionare le impostazioni del componente relative al livello di protezione e alla reazione alle minacce. Fare clic sul pulsante **Impostazioni** per visualizzare le altre impostazioni di Anti-Virus Posta.

ANTI-VIRUS WEB

In questa finestra sono raggruppate le impostazioni del componente Anti-Virus Web (vedere la sezione "Protezione del traffico Web" a pagina 69). Modificando le impostazioni, è possibile eseguire le azioni seguenti:

- disabilitare Anti-Virus Web;
- modificare il livello di protezione (vedere pagina 71);
- modificare l'azione da eseguire sugli oggetti rilevati (vedere pagina 71);
- creare un ambito di protezione (vedere pagina 71);
- modificare i metodi di scansione (vedere pagina 72);
- utilizzare il Barra degli strumenti di Kaspersky (vedere pagina 73);
- ottimizzare la scansione (vedere pagina 74);
- utilizzare l'analisi euristica (vedere pagina 74).
- ripristinare le impostazioni predefinite di Anti-Virus Web (vedere pagina 75).

Per disabilitare Anti-Virus Web, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.

3. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Anti-Virus Web**.

4. Deselezionare la casella **Abilita Anti-Virus Web** nella parte destra della finestra.

Per passare alle impostazioni di Anti-Virus Web, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.

2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.

3. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Anti-Virus Web**.

4. Nella parte destra della finestra, selezionare le impostazioni del componente relative al livello di protezione e alla reazione alle minacce. Fare clic sul pulsante **Impostazioni** per visualizzare le altre impostazioni di Anti-Virus Web.

ANTI-VIRUS IM

In questa finestra sono raggruppate le impostazioni del componente Anti-Virus IM (vedere la sezione "Protezione del traffico dei programmi di messaggistica istantanea" a pagina 76). Modificando le impostazioni, è possibile eseguire le azioni seguenti:

- disabilitare Anti-Virus IM;
- creare un ambito di protezione (vedere pagina 77);
- modificare il metodo di scansione (vedere pagina 77);
- utilizzare l'analisi euristica (vedere pagina 78).

Per disabilitare Anti-Virus IM, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.

2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.

3. Nella finestra visualizzata, selezionare il componente **Anti-Virus IM** nella sezione **Protezione**.

4. Deselezionare la casella **Abilita Anti-Virus IM** nella parte destra della finestra.

Per passare alle impostazioni di Anti-Virus IM, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.

2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.

3. Nella finestra visualizzata, selezionare il componente **Anti-Virus IM** nella sezione **Protezione**.

4. Nella parte destra della finestra, modificare le impostazioni del componente nel modo desiderato.

CONTROLLO APPLICAZIONI

In questa finestra sono raggruppate le impostazioni di Controllo Applicazioni (vedere pagina 80). Modificando le impostazioni, è possibile eseguire le azioni seguenti:

- disabilitare Controllo Applicazioni;

- creare un ambito di protezione (vedere pagina 83);
- gestire l'inserimento delle applicazioni in gruppi (vedere pagina 85);
- modificare il tempo utilizzato per determinare lo stato dell'applicazione (vedere pagina 86);
- modificare la regola per l'applicazione (vedere pagina 87);
- modificare la regola per un gruppo di applicazioni (vedere pagina 87);
- creare una regola di rete per l'applicazione (vedere pagina 87);
- specificare le esclusioni (vedere pagina 88);
- gestire l'eliminazione delle regole per le applicazioni (vedere pagina 88).

Per disabilitare Controllo Applicazioni, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Controllo Applicazioni**.
4. Nella parte destra della finestra, deselezionare la casella **Abilita Controllo Applicazioni**.

Per modificare le impostazioni di Controllo Applicazioni, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, nella sezione **Protezione**, selezionare il componente **Controllo Applicazioni**.
4. Nella parte destra della finestra, modificare le impostazioni del componente nel modo desiderato.

FIREWALL

In questa finestra sono raggruppate le impostazioni di Firewall (vedere pagina 94). Modificando le impostazioni, è possibile eseguire le azioni seguenti:

- disabilitare Firewall;
- modificare lo stato della rete (vedere pagina 94);
- estendere l'intervallo degli indirizzi di rete (vedere pagina 95);
- selezionare la modalità di notifica delle modifiche alla rete (vedere pagina 95);
- specificare le impostazioni avanzate del componente (vedere pagina 96);
- specificare le regole di Firewall (vedere pagina 96):
  - creare una regola per i pacchetti (vedere pagina 97);
  - creare una regola per l'applicazione (vedere pagina 98);
  - utilizzare la Creazione guidata regole (vedere pagina 98);
  - selezionare l'azione eseguita dalla regola (vedere pagina 99);

- modificare le impostazioni del servizio di rete (vedere pagina 99);
- estendere l'intervallo di indirizzi (vedere pagina 100);
- modificare la priorità della regola.

Per disabilitare Firewall, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Firewall**.
4. Deselezionare la casella **Abilita Firewall** nella parte destra della finestra.

Per procedere alla modifica delle impostazioni di Firewall, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Firewall**.
4. Nella parte destra della finestra, fare clic sul pulsante **Impostazioni** e modificare le impostazioni del componente nel modo desiderato nella finestra visualizzata.

DIFESA PROATTIVA

In questa finestra sono raggruppate le impostazioni del componente Difesa Proattiva (vedere pagina 101). Modificando le impostazioni, è possibile eseguire le azioni seguenti:

- disabilitare Difesa Proattiva;
- gestire l'elenco di attività pericolose (vedere pagina 101);
- modificare la reazione dell'applicazione alle attività pericolose nel sistema (vedere pagina 102);
- creare un gruppo di applicazioni attendibili (vedere pagina 103);
- monitorare gli account utente del sistema (vedere pagina 103).

Per disabilitare Difesa Proattiva, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Difesa Proattiva**.
4. Deselezionare la casella **Abilita Difesa Proattiva** a destra della finestra.

Per procedere alla modifica delle impostazioni di Difesa Proattiva, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Difesa Proattiva**.

4. Nella parte destra della finestra, modificare le impostazioni del componente nel modo desiderato.

PREVENZIONE INTRUSIONI

In questa finestra sono raggruppate le impostazioni del componente Prevenzione Intrusioni (vedere pagina 105). Modificando le impostazioni, è possibile eseguire le azioni seguenti:

- disabilitare Prevenzione Intrusioni;
- aggiungere un computer di origine dell'attacco a un elenco di computer bloccati (vedere pagina 105).

Per disabilitare Prevenzione Intrusioni, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Prevenzione Intrusioni**.
4. Nella parte destra della finestra, deselezionare la casella **Abilita Prevenzione Intrusioni**.

Per procedere alla modifica delle impostazioni di Prevenzione Intrusioni, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fareclic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Prevenzione Intrusioni**.
4. Nella parte destra della finestra, modificare le impostazioni del componente nel modo desiderato.

ANTI-SPAM

In questa finestra sono raggruppate le impostazioni del componente Anti-Spam (vedere pagina 107). Modificando le impostazioni, è possibile eseguire le azioni seguenti:

- disabilitare Anti-Spam
- addestrare Anti-Spam (vedere pagina 109):
  - utilizzando l'Addestramento guidato (vedere pagina 110);
  - con i messaggi in uscita (vedere pagina 111);
  - tramite il client di posta (vedere pagina 111);
  - tramite i rapporti (vedere pagina 113);
- modificare il livello di protezione (vedere pagina 113);
- modificare il metodo di scansione (vedere pagina 114);
- creare un elenco di:
  - URL attendibili (vedere pagina 115);
  - mittenti bloccati (vedere pagina 115);
  - frasi bloccate (vedere pagina)116;

- frasi oscene (vedere pagina 117);
- mittenti consentiti (vedere pagina 117);
- frasi consentite (vedere pagina 118);

- importare l'elenco di mittenti consentiti (vedere pagina 119);
- determinare i fattori di spam e probabile spam (vedere pagina 119);
- selezionare l'algoritmo di riconoscimento dello spam (vedere pagina 120);
- utilizzare funzioni aggiuntive di filtraggio dello spam (vedere pagina 121);
- aggiungere un'etichetta all'oggetto del messaggio (vedere pagina 121);
- utilizzare Gestore della posta (vedere pagina 122);
- escludere dalla scansione i messaggi di Microsoft Exchange Server (vedere pagina 122);
- configurare l'elaborazione della posta spam:
  - in Microsoft Office Outlook (vedere pagina 123);
  - in Microsoft Outlook Express (Windows Mail) (vedere pagina 125);
  - in The Bat! (vedere pagina 125);
  - in Thunderbird (vedere pagina 126);
- ripristinare le impostazioni predefinite di Anti-Spam (vedere pagina 126).

Per disabilitare Anti-Spam, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Spam**.
4. Deselezionare la casella **Abilita Anti-Spam** nella parte destra della finestra.

Per procedere alla modifica delle impostazioni di Anti-Spam, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Spam**.
4. Nella parte destra della finestra, fare clic sul pulsante **Impostazioni** e modificare le impostazioni del componente nel modo desiderato nella finestra visualizzata.

ANTI-BANNER

In questa finestra sono raggruppate le impostazioni del componente Anti-Banner (vedere pagina 127). Modificando le impostazioni, è possibile eseguire le azioni seguenti:

- disabilitare Anti-Banner;

- utilizzare l'analisi euristica (vedere pagina 127).
- specificare le impostazioni avanzate del componente (vedere pagina 128);
- creare l'elenco di indirizzi consentiti (vedere pagina 128);
- creare l'elenco di indirizzi bloccati (vedere pagina 129);
- esportare/importare gli elenchi di banner (vedere pagina 129).

Per disabilitare Anti-Banner, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul. pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Banner**.
4. Deselezionare la casella **Abilita Anti-Banner** nella parte destra della finestra.

Per procedere alla modifica delle impostazioni di Anti-Banner, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, sezione **Protezione**, selezionare il componente **Anti-Banner**.
4. Nella parte destra della finestra, modificare le impostazioni del componente nel modo desiderato.

SCANSIONE

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

Kaspersky Lab distingue tra attività di scansione anti-virus e attività di ricerca delle vulnerabilità. Le attività di scansione anti-virus includono quanto segue:

- **Scansione Personalizzata**. Scansione degli oggetti selezionati dall'utente. È possibile esaminare qualsiasi oggetto nel file system del computer.
- **Scansione Completa**. Una scansione approfondita dell'intero sistema. Gli oggetti seguenti vengono esaminati per impostazione predefinita: memoria di sistema, programmi caricati all'avvio, backup di sistema, database di posta, dischi rigidi, unità rimovibili e unità di rete.
- **Scansione Rapida**. Scansione anti-virus degli oggetti di avvio del sistema operativo.

È possibile eseguire le azioni seguenti nella finestra delle impostazioni di ogni attività anti-virus:

- selezionare il livello di protezione con le impostazioni correlate definendo il comportamento dell'attività in fase di runtime;
- selezionare l'azione che verrà eseguita dall'applicazione al rilevamento di un oggetto infetto/potenzialmente infetto;
- creare una pianificazione per eseguire le attività automaticamente;
- creare un elenco di oggetti da esaminare (per attività di scansione rapida e di scansione completa);
- specificare i tipi di file su cui eseguire una scansione anti-virus;

- specificare le impostazioni per la scansione dei file compositi;
- selezionare i metodi di scansione e le tecnologie di scansione.

Nella sezione **Scansione** è possibile specificare le impostazioni per la scansione automatica delle unità rimovibili quando sono connesse al computer, nonché creare collegamenti per l'avvio rapido delle attività di scansione anti-virus e ricerca delle vulnerabilità.

Nella finestra delle impostazioni, è possibile eseguire le azioni seguenti per un'attività di ricerca delle vulnerabilità:

- creare una pianificazione per eseguire le attività automaticamente;
- creare un elenco di oggetti da sottoporre a scansione.

Per modificare le impostazioni delle attività:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, selezionare l'attività richiesta nella sezione **Scansione** (**Scansione Completa**, **Scansione Rapida**, **Scansione Personalizzata**, **Scansione Vulnerabilità**).
4. Nella parte destra della finestra, configurare le impostazioni.

AGGIORNAMENTI

L'aggiornamento di Protezione del computer viene eseguito in base all'insieme dei parametri.

Nella finestra di configurazione dell'attività di aggiornamento è possibile eseguire le azioni seguenti:

- modificare l'indirizzo della risorsa dalla quale verranno distribuiti e installati gli aggiornamenti delle applicazioni;
- specificare il tipo di modalità, in base al quale verrà avviato il processo di aggiornamento dell'applicazione;
- impostare la pianificazione per l'esecuzione di un'attività;
- specificare l'account con cui avviare l'aggiornamento;
- selezionare le azioni da eseguire al termine dell'aggiornamento dell'applicazione.

Per procedere alla configurazione dell'aggiornamento:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Selezionare la sezione **Aggiornamenti** nella parte sinistra della finestra.
4. Selezionare la modalità di esecuzione richiesta nella parte destra della finestra e selezionare un'origine di aggiornamento. Configurare altre impostazioni dell'attività nella sezione **Avanzate**.

IMPOSTAZIONI

Nella finestra **Impostazioni** è possibile utilizzare le funzioni avanzate di Protezione del computer elencate di seguito:

- Selezionare le categorie di minacce rilevabili (vedere pagina 162).
- Creare l'area attendibile per l'applicazione (vedere 163pagina).
- Creare regole di esclusione (vedere pagina 164).
- Creare un elenco di porte monitorate (vedere pagina 166);
- Abilitare/disabilitare la modalità di scansione delle connessioni crittografate utilizzando il protocollo SSL (vedere pagina 167);
- Configurare Quarantena e Backup (vedere pagina 169).

MINACCE ED ESCLUSIONI

Nella sezione **Minacce ed Esclusioni** della finestra delle impostazioni di Protezione del computer è possibile eseguire le azioni seguenti:

- selezionare le categorie di minacce rilevabili (vedere la sezione "Selezione delle categorie di minacce rilevabili" a pagina 162);
- creare l'area attendibile per l'applicazione.

L'*area attendibile* è un elenco di oggetti creato dall'utente che non dovrebbe essere controllato dall'applicazione. In altre parole, si tratta di una serie di programmi esclusi dall'ambito di Protezione del computer.

L'area attendibile viene creata in base all'elenco di applicazioni attendibili (vedere la sezione "Selezione delle applicazioni attendibili" a pagina 163) e alle regole di esclusione (vedere la sezione "Regole di esclusione" a pagina 164).

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

VEDERE ANCHE:

Selezione delle categorie di minacce rilevabili 162

Selezione delle applicazioni attendibili 163

Regole di esclusione 164

Maschere di esclusione file consentite 164

Maschere dei tipi di minaccia consentiti 165

SELEZIONE DELLE CATEGORIE DI MINACCE RILEVABILI

Protezione del computer offre la protezione da diversi tipi di programmi dannosi. A prescindere dalle impostazioni selezionate, l'applicazione esegue sempre la scansione e la disinfezione per eliminare virus, Trojan e utilità degli hacker. Questi programmi infatti possono danneggiare gravemente il computer. Per offrire una maggiore protezione, è possibile ampliare l'elenco di minacce da rilevare, abilitando il controllo di vari programmi potenzialmente pericolosi.

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

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, selezionare la sezione **Minacce ed Esclusioni**. Fare clic sul pulsante **Impostazioni** nella sezione **Minacce**.
4. Nella finestra **Minacce** visualizzata, selezionare le categorie di minacce da cui si desidera proteggere il computer.

SELEZIONE DELLE APPLICAZIONI ATTENDIBILI

È possibile creare un elenco delle applicazioni attendibili che impedirà il controllo delle relative attività di rete e dei file, incluse quelle sospette, nonché dei relativi tentativi di accedere al Registro di sistema.

È possibile ad esempio che si ritenga che gli oggetti utilizzati da Blocco note di Microsoft Windows siano sicuri e non necessitino di scansione. In altre parole, quest'applicazione viene considerata attendibile. Per escludere dalla scansione gli oggetti utilizzati da questo processo, aggiungere l'applicazione Blocco note all'elenco delle applicazioni attendibili. Il file eseguibile e il processo dell'applicazione attendibile saranno contemporaneamente sottoposti a scansione anti-virus come in precedenza. Per escludere completamente un'applicazione dalla scansione, è consigliabile utilizzare le regole di esclusione.

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

L'esclusione delle applicazioni attendibili dalla scansione consente di risolvere 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 Protezione del computer e di un'altra applicazione anti-virus, nonché di aumentare la velocità delle prestazioni del computer, aspetto di fondamentale importanza quando si utilizzano applicazioni server.

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

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

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, selezionare la sezione **Minacce ed Esclusioni**.
4. Nella sezione **Esclusioni**, fare clic sul pulsante **Impostazioni**.
5. Nella finestra visualizzata, nella scheda **Applicazioni attendibili**, fare clic sul collegamento **Aggiungi**.
6. Nel menu visualizzato, selezionare un'applicazione. Quando si seleziona la voce **Sfoglia**, viene aperta una finestra nella quale è necessario specificare il percorso di un file eseguibile. Quando si seleziona la voce **Applicazioni**, viene aperto l'elenco di applicazioni attualmente in esecuzione.
7. Nella finestra **Esclusioni per l'applicazioni** visualizzata, specificare le impostazioni delle regole per l'applicazione.

Si noti che, se è selezionata la casella **Non esaminare il traffico di rete**, il traffico dell'applicazione specificata non verrà sottoposto a scansione anti-virus ma solo a quella dello spam. Questo tuttavia non influenza la scansione del traffico eseguita dal componente Firewall le cui impostazioni regolano l'analisi delle attività di rete dell'applicazione.

L'applicazione affidabile può essere cambiata o eliminata dall'elenco tramite i corrispondenti collegamenti nella parte inferiore della scheda. Per rimuovere un'applicazione dall'elenco senza eliminarla, deselezionare la casella in corrispondenza del nome.

REGOLE DI ESCLUSIONE

Il software potenzialmente pericoloso non svolge una funzione dannosa vera e propria ma può essere utilizzato dagli hacker come componente ausiliario di un codice nocivo in quanto contiene errori e vulnerabilità. Questa categoria include, ad esempio, programmi di amministrazione remota, client IRC, server FTP, utilità multiuso per arrestare o nascondere processi, keylogger, password cracker, autodialer e così via. Tali programmi non sono classificati come virus (not-a-virus). Possono essere suddivisi in diversi tipi, quali Adware, Joke, Riskware e così via. Per ulteriori informazioni sui programmi potenzialmente pericolosi rilevati dall'applicazione, vedere l'Enciclopedia dei Virus all'indirizzo www.viruslist.com. Dopo la scansione, questi programmi possono essere bloccati. Poiché molti di essi sono ampiamente utilizzati dagli utenti, è possibile escluderli dalla scansione.

È ad esempio possibile che si utilizzi frequentemente un programma di amministrazione remota, ovvero un programma di accesso remoto che consente di lavorare da un altro computer. Protezione del computer visualizza l'attività di questo programma come potenzialmente pericolosa e potrebbe bloccarla. Se non si desidera bloccare l'applicazione, è necessario creare una regola di esclusione per l'applicazione in modo che venga rilevata come *not-a-virus:RemoteAdmin.Win32.RAdmin.22* secondo l'Enciclopedia dei Virus.

Le *regole di esclusione* sono insiemi di condizioni utilizzate da Protezione del computer per verificare se è possibile evitare la scansione di un oggetto.

È possibile escludere dalla scansione determinati formati di file, utilizzare una maschera file o escludere una determinata area, ad esempio una cartella o un programma, processi di programma o oggetti in base alla classificazione del tipo di minaccia nell'Enciclopedia dei Virus.

Il *tipo di minaccia* è lo stato assegnato da Protezione del computer a un oggetto durante la scansione. Lo stato viene assegnato in base alla classificazione dei programmi dannosi o potenzialmente pericolosi elencati nell'Enciclopedia dei Virus di Kaspersky Lab.

Quando si aggiunge un'esclusione, viene creata una regola che può essere utilizzata con diversi componenti dell'applicazione, ad esempio Anti-Virus File (vedere la sezione "Protezione del file system del computer" a pagina 52), Anti-Virus Posta (vedere la sezione "Protezione della posta" a pagina 62), Anti-Virus Web (vedere la sezione "Protezione del traffico Web" a pagina 69) e per l'attività di scansione anti-virus.

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

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, selezionare la sezione **Minacce ed Esclusioni**.
4. Nella sezione **Esclusioni**, fare clic sul pulsante **Impostazioni**.
5. Nella finestra visualizzata, nella scheda **Regole di esclusione**, fare clic sul collegamento **Aggiungi**.
6. Nella finestra **Regola di esclusione** visualizzata, modificare le impostazioni delle regole di esclusione.

VEDERE ANCHE:

Maschere di esclusione file consentite 164

Maschere dei tipi di minaccia consentiti 165

MASCHERE DI ESCLUSIONE FILE CONSENTITE

Durante la creazione di elenchi di esclusione file, è possibile utilizzare alcune maschere. Le più comuni sono le seguenti:

1. Maschere senza percorsi file:
   - ***.exe**: tutti i file con estensione *exe*;
   - ***.ex?:** - tutti i file con l'estensione *ex?* in cui **?** può rappresentare qualsiasi carattere;

- **test**: tutti i file con il nome *test.*

2. Maschere con percorsi file assoluti:

   - **C:\dir*.*** o **C:\dir*** o **C:\dir** – tutti i file contenuti nella cartella *C:\dir*;
   - **C:\dir*.exe**: tutti i file con estensione exe contenuti nella cartella *C:\dir*;
   - **C:\dir*.ex?** - tutti i file con l'estensione *ex?* contenuti nella cartella *C:\dir*, dove **?** può rappresentare qualsiasi carattere;
   - **C:\dir\test**: solo il file *C:\dir\test*.

     Se si desidera escludere la scansione dei file in tutte le sottocartelle nidificate della cartella specificata, selezionare la casella **Includi sottocartelle** durante la creazione di una maschera.

3. Maschere con percorsi file:

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

     Se si desidera escludere la scansione dei file in tutte le sottocartelle nidificate della cartella specificata, selezionare la casella **Includi sottocartelle** durante la creazione di una maschera.

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

MASCHERE DEI TIPI DI MINACCIA CONSENTITI

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

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

RETE

Nella sezione **Rete** della finestra delle impostazioni dell'applicazione è possibile selezionare le porte monitorate da Protezione del computer e configurare la scansione delle connessioni crittografate:

- creare un elenco di porte monitorate (vedere pagina 166);
- Abilitare/disabilitare la modalità di scansione delle connessioni crittografate utilizzando il protocollo SSL (vedere pagina 167);

VEDERE ANCHE:

Scansione delle connessioni crittografate 167

Scansione delle connessioni crittografate in Mozilla Firefox..... 167

Scansione delle connessioni crittografate in Opera..... 168

Creazione di un elenco delle porte monitorate 166

CREAZIONE DI UN ELENCO DELLE PORTE MONITORATE

I componenti della protezione, ad esempio Anti-Virus Posta (vedere la sezione "Protezione della posta" a pagina 62), Anti-Virus Web (vedere la sezione "Protezione del traffico Web" a pagina 69), e Anti-Spam (vedere pagina 107), monitorano i flussi di dati trasmessi tramite determinati protocolli che attraversano specifiche porte aperte del computer. Anti-Virus Posta, ad esempio, analizza le informazioni trasferite tramite il protocollo SMTP mentre Anti-Virus Web analizza i pacchetti HTTP.

È possibile selezionare una delle due modalità di monitoraggio delle porte:

- **Tutte le porte di rete**;
- **Soltanto le porte selezionate**. L'applicazione comprende un elenco delle porte utilizzate per trasmettere la posta elettronica e il traffico HTTP.

Per aggiungere una porta all'elenco delle porte monitorate:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, selezionare la sezione **Rete**.
4. Nella sezione **Porte da monitorare** fare clic sul pulsante **Seleziona**.
5. Nella finestra **Porte di rete** visualizzata, fare clic sul collegamento **Aggiungi**.
6. Nella finestra **Porta di rete** visualizzata, specificare i dati richiesti.

Per escludere una porta dall'elenco di porte monitorate:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, selezionare la sezione **Rete**.
4. Nella sezione **Porte da monitorare** fare clic sul pulsante **Seleziona**.

5. Nella finestra **Porte di rete** visualizzata, deselezionare la casella accanto alla descrizione della porta.

Per creare l'elenco delle applicazioni per le quali si desidera monitorare tutte le porte, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, selezionare la sezione **Rete**.
4. Nella sezione **Porte da monitorare** fare clic sul pulsante **Seleziona**.
5. Nella finestra **Porte di rete** visualizzata, selezionare la casella **Controlla tutte le porte per le applicazioni specificate** e fare clic sul collegamento **Aggiungi** nella sezione sottostante.
6. Nel menu visualizzato, selezionare un'applicazione. Quando si seleziona la voce **Sfoglia**, viene aperta una finestra nella quale è necessario specificare il percorso di un file eseguibile. Quando si seleziona la voce **Applicazioni**, viene aperto l'elenco di applicazioni attualmente in esecuzione.
7. Nella finestra **Applicazione** visualizzata, specificare la descrizione per l'applicazione selezionata.

SCANSIONE DELLE CONNESSIONI CRITTOGRAFATE

La connessione mediante il protocollo SSL (Secure Sockets Layer) consente di proteggere il canale di scambio dei dati in Internet. Il protocollo SSL è in grado di identificare le parti che scambiano dati tramite certificati elettronici, codificare i dati trasferiti e garantirne l'integrità durante il trasferimento.

Queste funzioni del protocollo vengono utilizzate dai pirati informatici per diffondere programmi dannosi, poiché quasi tutti i programmi anti-virus non esaminano il traffico SSL.

Protezione del computer verifica le connessioni protette utilizzando il certificato di Kaspersky Lab. Tale certificato verrà sempre utilizzato per controllare se la connessione è sicura.

Scansioni successive del traffico tramite il protocollo SSL verranno eseguite utilizzando il certificato di Kaspersky Lab installato. 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 suggerisce di accettare o rifiutare il certificato o visualizzarne le informazioni. Se l'applicazione funziona in modalità automatica, la connessione che utilizza un certificato non valido verrà interrotta senza alcuna notifica.

Per abilitare la scansione delle connessioni crittografate, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, selezionare la sezione **Rete**.
4. Nella finestra visualizzata, selezionare la casella **Esamina le connessioni crittografate** e fare clic sul pulsante **Installa certificato**.
5. Nella finestra visualizzata, fare clic sul pulsante **Installa certificato**. In questo modo viene avviata una procedura guidata che contiene le istruzioni da seguire per installare correttamente il certificato.

L'installazione automatica del certificato è disponibile solo in Microsoft Internet Explorer. Per eseguire la scansione delle connessioni crittografate in Mozilla Firefox e Opera, è necessario installare il certificato di Kaspersky Lab manualmente.

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.

Per installare il certificato di Kaspersky Lab, eseguire le operazioni seguenti:

1. Nel menu del browser, selezionare la voce **Strumenti** → **Impostazioni**.
2. Nella finestra visualizzata, selezionare la sezione **Avanzate**.
3. Nella sezione **Certificati**, selezionare la scheda **Protezione** e fare clic sul pulsante **Visualizzazione certificati**.
4. Nella finestra visualizzata, selezionare la scheda **Centri certificati** e fare clic sul pulsante **Ripristina**.
5. Nella finestra visualizzata, selezionare il file di certificato di Kaspersky Lab. Il percorso del file di certificato di Kaspersky Lab è il seguente:
%AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\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 clic sul pulsante **Visualizza**.

Per installare il certificato di Kaspersky Lab per Mozilla Firefox versione 3.x, eseguire le operazioni seguenti:

1. Nel menu del browser, selezionare la voce **Strumenti** → **Impostazioni**.
2. Nella finestra visualizzata, selezionare la sezione **Avanzate**.
3. Nella scheda **Crittografia dei dati**, fare clic sul pulsante **Visualizzazione certificati**.
4. Nella finestra visualizzata, selezionare la scheda **Centri certificati** e fare clic sul pulsante **Importa**.
5. Nella finestra visualizzata, selezionare il file di certificato di Kaspersky Lab. Il percorso del file di certificato di Kaspersky Lab è il seguente:
%AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\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 clic sul pulsante **Visualizza**.

Se il computer utilizza Microsoft Windows Vista, il percorso del file di certificato di Kaspersky Lab è il seguente: *%AllUsersProfile%\Kaspersky Lab\AVP9\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, eseguire le operazioni seguenti:

1. Nel menu del browser, selezionare la voce **Strumenti** → **Impostazioni**.
2. Nella finestra visualizzata, selezionare la sezione **Avanzate**.
3. Nella parte sinistra della finestra, selezionare la scheda **Protezione** e fare clic sul pulsante **Gestisci certificati**.
4. Nella finestra visualizzata, selezionare la scheda **Fornitori** e fare clic sul pulsante **Importa**.
5. Nella finestra visualizzata, selezionare il file di certificato di Kaspersky Lab. Il percorso del file di certificato di Kaspersky Lab è il seguente:
%AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer.
6. Nella finestra visualizzata, fare clic sul pulsante **Installa**. Il certificato di Kaspersky Lab verrà installato. Per visualizzare le informazioni sul certificato e selezionare le azioni per le quali il certificato verrà utilizzato, selezionare il certificato nell'elenco e fare clic sul pulsante **Visualizza**.

Per installare il certificato di Kaspersky Lab per Opera versione 9.x, eseguire le operazioni seguenti:

1. Nel menu del browser, selezionare la voce **Strumenti** → **Impostazioni**.
2. Nella finestra visualizzata, selezionare la sezione **Avanzate**.
3. Nella parte sinistra della finestra, selezionare la scheda **Protezione** e fare clic sul pulsante **Gestisci certificati**.
4. Nella finestra visualizzata, selezionare la scheda **Centri certificati** e fare clic sul pulsante **Importa**.
5. Nella finestra visualizzata, selezionare il file di certificato di Kaspersky Lab. Il percorso del file di certificato di Kaspersky Lab è il seguente: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.
6. Nella finestra visualizzata, fare clic sul pulsante **Installa**. Il certificato di Kaspersky Lab verrà installato.

Se il computer utilizza Microsoft Windows Vista, il percorso del file di certificato di Kaspersky Lab è il seguente: *%AllUsersProfile%\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

QUARANTENA E BACKUP

Questa sezione contiene le impostazioni che controllano l'utilizzo dei file di dati di Protezione del computer.

I *file di dati dell'applicazione* sono oggetti spostati in Quarantena e Backup da Protezione del computer. In questa sezione, è possibile configurare Quarantena e Backup (vedere pagina 170).

VEDERE ANCHE:

Archiviazione degli oggetti della quarantena e del backup 170

Rapporti 172

Azioni con gli oggetti in quarantena 170

Quarantena per oggetti potenzialmente infetti 169

Copie di backup degli oggetti pericolosi 170

QUARANTENA PER OGGETTI POTENZIALMENTE INFETTI

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

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

Un oggetto potenzialmente infetto può essere individuato e messo in quarantena da Anti-Virus File, Anti-Virus Posta, Difesa Proattiva o nel corso di una scansione anti-virus.

Gli oggetti vengono messi in quarantena in seguito al funzionamento di Anti-Virus File e Anti-Virus Posta, nonché nel corso di una scansione anti-virus, se:

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

  I database di Protezione del computer contengono informazioni aggiornate sulle minacce individuate dagli specialisti di Kaspersky Lab. Se un programma dannoso viene modificato e le modifiche non sono state ancora inserite nei database, Protezione del computer classifica l'oggetto infettato dal programma dannoso modificato come oggetto potenzialmente infetto e indica con esattezza la minaccia alla quale questa infezione somiglia.

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

  È probabile che si tratti di un nuovo tipo di minaccia, pertanto Protezione del computer classifica l'oggetto come oggetto potenzialmente infetto.

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

Come per Difesa Proattiva, il componente mette un oggetto in quarantena se, come risultato dell'analisi del comportamento, la sequenza di azioni dell'oggetto desta sospetti.

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

È possibile che al termine dell'aggiornamento del database Protezione del computer riesca a riconoscere la minaccia in modo inequivocabile e neutralizzarla. Di conseguenza, l'applicazione esegue la scansione degli oggetti in quarantena dopo ogni aggiornamento.

COPIE DI BACKUP DEGLI OGGETTI PERICOLOSI

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

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

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

AZIONI CON GLI OGGETTI IN QUARANTENA

È possibile eseguire le azioni seguenti sugli oggetti in quarantena:

- mettere in quarantena i file sospettati di essere infetti;
- esaminare e disinfettare tutti gli oggetti potenzialmente infetti in quarantena utilizzando i database correnti di Protezione del computer;
- ripristinare i file nelle cartelle da cui sono stati spostati per essere messi in quarantena oppure nelle cartelle selezionate dall'utente;
- eliminare tutti gli oggetti in quarantena oppure un gruppo di oggetti selezionati;
- inviare gli oggetti in quarantena a Kaspersky Lab per l'analisi.

Per eseguire azioni sugli oggetti in quarantena:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Quarantena**.
2. Eseguire le azioni richieste nella scheda **Minacce rilevate** della finestra visualizzata.

ARCHIVIAZIONE DEGLI OGGETTI DELLA QUARANTENA E DEL BACKUP

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

- Determinare la durata massima di archiviazione degli oggetti in quarantena o delle copie di questi nel backup (casella **Mantieni gli oggetti per non più di**). Per impostazione predefinita, la durata di archiviazione degli oggetti è di 30 giorni. Una volta trascorso questo periodo, gli oggetti vengono eliminati. È possibile modificare il termine archiviazione massima o rimuovere del tutto questa restrizione.

- Specificare la dimensione massima dell'area di archiviazione dei dati (casella **Dimensione massima**). Per impostazione predefinita, la dimensione massima è di 100 MB. È possibile annullare il limite delle dimensioni del rapporto o impostare un altro valore.

Per configurare le impostazioni della quarantena e del backup:

1. Aprire la finestra principale dell'applicazione e fare clic sul **Protezione del computer**.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella finestra visualizzata, selezionare la sezione **Rapporti e Backup**.
4. Nella sezione **Quarantena e Backup**, selezionare le caselle desiderate e immettere la dimensione massima dell'area di archiviazione dei dati in base alle esigenze.

RAPPORTI

Il funzionamento di ogni componente di Protezione del computer e le prestazioni di ogni scansione e aggiornamento anti-virus vengono registrati in un rapporto.

I rapporti consentono di eseguire le operazioni seguenti:

- selezionare il componente o l'attività (vedere pagina 172) per la quale si desidera visualizzare il rapporto sull'evento;
- gestire il raggruppamento dei dati (vedere pagina 173) e la visualizzazione dei dati sullo schermo (vedere pagina 175);
- creare una pianificazione (vedere pagina 173) in base alla quale Protezione del computer notificherà all'utente quando il rapporto è pronto;
- selezionare i tipi di evento (vedere pagina 174) per i quali si desidera creare un rapporto;
- selezionare la modalità di visualizzazione (vedere pagina 176) delle statistiche sullo schermo;
- salvare un rapporto come file (vedere pagina 176);
- specificare condizioni di filtraggio complesso (vedere pagina 177);
- configurare la ricerca degli eventi (vedere pagina 177) verificatisi nel sistema ed elaborati dall'applicazione.

IN QUESTA SEZIONE:

Selezione di un componente o di un'attività per creare un rapporto 172

Gestione del raggruppamento delle informazioni nel rapporto 173

Notifica sul completamento del rapporto 173

Selezione dei tipi di evento 174

Visualizzazione dei dati sullo schermo 175

Modalità di visualizzazione estesa per le statistiche 176

Salvataggio di un rapporto in un file 176

Utilizzo del filtraggio complesso 177

Ricerca eventi 177

SELEZIONE DI UN COMPONENTE O DI UN'ATTIVITA PER CREARE UN RAPPORTO

È possibile ottenere informazioni sugli eventi verificatisi durante il funzionamento di ciascun componente di Protezione del computer o durante l'esecuzione di attività, ad esempio Anti-Virus File, aggiornamenti e così via.

Per creare un rapporto relativo a un componente o un'attività specifica:

1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Rapporto** nella parte superiore.

2. Nella finestra visualizzata, nella scheda **Rapporto**, fare clic sul pulsante **Rapporto dettagliato**.

3. Nella finestra visualizzata, selezionare un componente o un'attività per cui creare un rapporto nell'elenco a discesa a sinistra. Dopo aver selezionato la voce **Protezione**, verrà creato il rapporto per tutti i componenti di protezione.

GESTIONE DEL RAGGRUPPAMENTO DELLE INFORMAZIONI NEL RAPPORTO

È possibile gestire le modalità di raggruppamento delle informazioni nel rapporto utilizzando uno dei diversi attributi disponibili. L'insieme di attributi varia in base al componente e all'attività dell'applicazione. Sono disponibili le opzioni seguenti:

- **Non raggruppare**. verranno visualizzati tutti gli eventi.
- **Raggruppa per attività**. i dati verranno raggruppati in base alle attività eseguite dai componenti di Protezione del computer.
- **Raggruppa per applicazione**. i dati verranno raggruppati in base alle applicazioni attive nel sistema ed elaborati dal modulo di Protezione del computer.
- **Raggruppa per risultato**. i dati verranno raggruppati in base ai risultati della scansione o dell'elaborazione dell'oggetto.

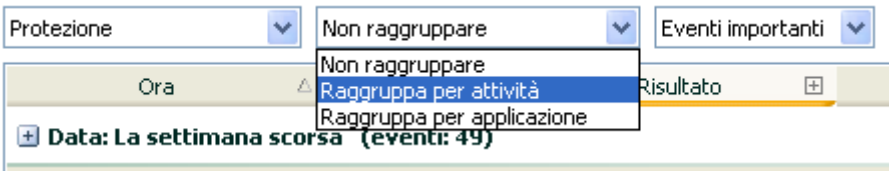


Figura 16. Attributi di raggruppamento delle informazioni nel rapporto

Per ottenere rapidamente le informazioni desiderate e ridurre le dimensioni di raggruppamento, viene fornito un criterio di ricerca (vedere la sezione "Ricerca eventi" a pagina 177). È inoltre possibile specificare un criterio di ricerca.

Per utilizzare il raggruppamento in base a un determinato attributo:

1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Rapporto** nella parte superiore della finestra.

2. Nella finestra visualizzata, nella scheda **Rapporto**, fare clic sul pulsante **Rapporto dettagliato**.

3. Selezionare l'attributo di raggruppamento dal menu a discesa nella finestra visualizzata.

NOTIFICA SUL COMPLETAMENTO DEL RAPPORTO

È possibile creare una pianificazione in base alla quale Protezione del computer notificherà all'utente quando il rapporto è pronto.

Per creare una pianificazione di notifica:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante Crittografia dei dati. collegamento **Rapporto** nella parte superiore della finestra.

2. Nella finestra visualizzata, nella scheda **Rapporto**, selezionare la casella **Notifica completamento rapporto**. Fare clic sul collegamento con il valore temporale preimpostato.

3. Creare la pianificazione nella finestra **Pianificazione rapporti** visualizzata.

SELEZIONE DEI TIPI DI EVENTO

In un rapporto viene registrato un elenco completo di tutti gli eventi importanti che si verificano durante l'attività del componente della protezione, l'esecuzione delle scansioni o l'aggiornamento del database dell'applicazione. È possibile selezionare il tipo di evento da registrare.

Gli eventi possono appartenere a uno dei tipi seguenti:

- *Eventi critici*. Eventi di importanza fondamentale che indicano problemi riscontrati nel funzionamento di Protezione del computer o vulnerabilità della protezione. Includono, ad esempio, il rilevamento di un virus o un errore di funzionamento.

- *Eventi importanti*. Eventi da esaminare sempre con attenzione in quanto riflettono situazioni importanti nel funzionamento dell'applicazione, ad esempio l'evento **terminato**.

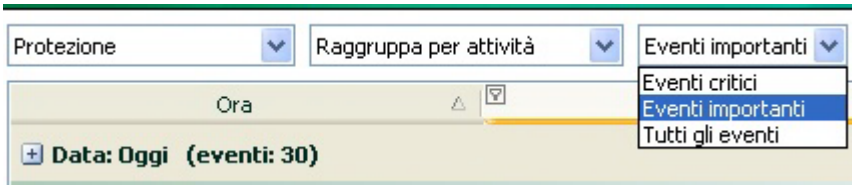


Figura 17. Selezione del tipo di evento

Se la voce **Tutti gli eventi** è selezionata, nel rapporto verranno visualizzati tutti gli eventi a condizione che nella sezione **Rapporti** all'interno della sezione di impostazioni **Rapporti e backup** le caselle corrispondenti siano selezionate. Si tratta di caselle che consentono la registrazione nel rapporto di record di eventi non critici nonché di eventi del file system e del Registro di sistema. Se tali caselle non sono selezionate, vengono visualizzati un'icona di avviso e il collegamento **Disabilitato** accanto all'elenco a discesa di selezione del tipo di evento. Utilizzare il collegamento per passare alla finestra delle impostazioni dei rapporti e per selezionare le relative caselle.

Per creare un rapporto su un determinato tipo di evento:

1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Rapporto** nella parte superiore della finestra.

2. Nella finestra visualizzata, nella scheda **Rapporto**, fare clic sul pulsante **Rapporto dettagliato**.

3. Selezionare il tipo di evento dal menu a discesa nella finestra visualizzata. Se è necessario creare un rapporto per tutti gli eventi, selezionare il valore **Tutti gli eventi**.

VISUALIZZAZIONE DEI DATI SULLO SCHERMO

Gli eventi inclusi nel rapporto vengono visualizzati in una tabella. È possibile creare un insieme di dati per filtrare le informazioni specificando una condizione di restrizione. A tale scopo, fare clic sull'area a sinistra dell'intestazione della colonna della tabella per la quale si desidera imporre una restrizione. L'elenco a discesa visualizza i valori possibili delle condizioni di restrizione, ad esempio **Ieri** per la colonna **Ora**, **Messaggio e-mail** per la colonna **Oggetto** e così via. Selezionare il valore richiesto per ogni colonna. La query verrà eseguita in base alla condizione di restrizione specificata. Se si desidera visualizzare tutti i dati, selezionare la voce **Tutto** nell'elenco di restrizioni.

Figura 18. Specifica di una condizione di restrizione

È inoltre possibile specificare le impostazioni di una ricerca complessa sotto forma di un intervallo all'interno del quale selezionare dati su eventi passati. A tale scopo, selezionare la voce **Personalizzato** dall'elenco a discesa delle restrizioni. Nella finestra visualizzata, specificare l'intervallo temporale desiderato (vedere la sezione "Utilizzo del filtraggio complesso" a pagina 177).

Per semplificare la creazione del rapporto, utilizzare il menu di scelta rapida per accedere agli attributi che consentono il raggruppamento e l'esecuzione di query sugli eventi.

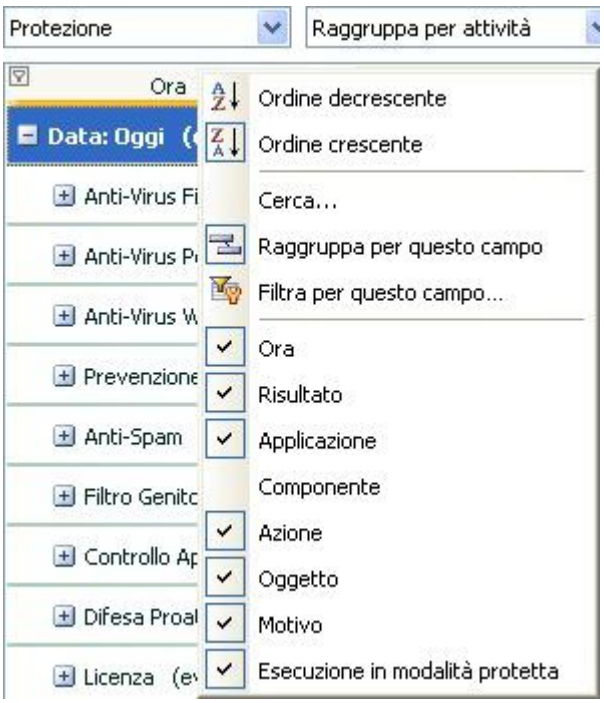


Figura 19. Menu di scelta rapida

Per specificare una limitazione:

1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Rapporto** nella parte superiore.
2. Nella finestra visualizzata, nella scheda **Rapporto**, fare clic sul pulsante **Rapporto dettagliato**.
3. Nella finestra visualizzata, fare clic sull'area a sinistra dell'intestazione della colonna della tabella per la quale si desidera imporre una restrizione. Selezionare una restrizione richiesta nell'elenco a discesa. Se la voce **Personalizzato** è selezionata, sarà possibile specificare condizioni di filtraggio complesso (vedere la sezione "Utilizzo del filtraggio complesso" a pagina 177).

Per nascondere o mostrare le colonne della tabella:

1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Rapporto** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella scheda **Rapporto**, fare clic sul pulsante **Rapporto dettagliato**.
3. Nella finestra visualizzata, fare clic con il tasto destro del mouse sull'area a destra dell'intestazione di qualsiasi colonna di tabella. Per nascondere le colonne della tabella, deselezionare le caselle accanto ai nomi corrispondenti nel menu di scelta rapida.

MODALITA DI VISUALIZZAZIONE ESTESA PER LE STATISTICHE

Nella parte inferiore della finestra del rapporto vengono riportate le statistiche relative al funzionamento dell'attività o del componente selezionato di Protezione del computer. È possibile visualizzare statistiche complete in formato grafico o tabulare, a seconda del componente o dell'attività. Per passare alla visualizzazione delle statistiche complete, utilizzare il pulsante nella parte superiore della finestra. Le statistiche vengono visualizzate per il giorno corrente e per l'intero periodo durante il quale l'applicazione è rimasta installata nel computer.

Per visualizzare statistiche dettagliate, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Rapporto** nella parte superiore.
2. Nella finestra visualizzata, nella scheda **Rapporto**, fare clic sul pulsante **Rapporto dettagliato**.
3. Nella finestra visualizzata, selezionare il componente dell'applicazione di cui si desidera visualizzare le statistiche e fare clic sul pulsante nella parte superiore della finestra.

SALVATAGGIO DI UN RAPPORTO IN UN FILE

Il rapporto ottenuto può essere salvato in un file.

Per farlo, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Rapporto** nella parte superiore.
2. Nella finestra visualizzata, nella scheda **Rapporto**, fare clic sul pulsante **Rapporto dettagliato**.
3. Nella finestra visualizzata creare il rapporto richiesto e fare clic sul pulsante **Salva**.
4. Nella finestra visualizzata, selezionare una cartella in cui salvare il file dei rapporti e immettere il nome del file.

UTILIZZO DEL FILTRAGGIO COMPLESSO

La finestra **Filtro personalizzato** (vedere la figura sotto) consente di specificare condizioni di filtraggio complesso dei dati nonché indicare criteri di ricerca dei dati per qualsiasi colonna della tabella. A titolo di esempio, verrà esaminata la procedura di utilizzo della finestra con la colonna **Ora**.

L'esecuzione di query sui dati con un filtro complesso si basa sulle funzioni di congiunzione logica (AND logico) e di disgiunzione logica (OR logico) che possono essere utilizzate per controllare la query.

I limiti della query, in questo caso Ora, si trovano nei campi a destra della finestra. Per specificarli, è possibile utilizzare i tasti freccia sulla tastiera. L'elenco a discesa **Mostra righe il cui valore è** consente di scegliere la condizione per la query di eventi, ad esempio **Maggiore di se si** desidera ottenere solo i risultati che superano il valore specificato nel campo a destra.

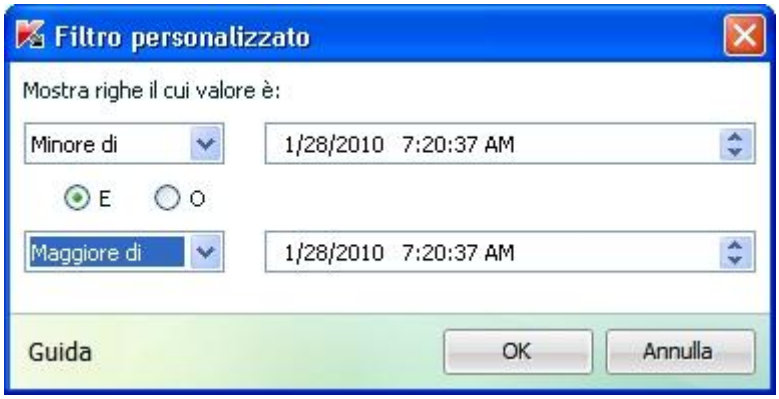


Figura 20. Specifica delle condizioni di filtraggio complesso

Se si desidera che la query dati soddisfi entrambe le condizioni specificate, selezionare **E**. Se è richiesta solo una delle due condizioni, selezionare **O**.

Per diversi tipi di dati, il limite dell'intervallo di ricerca non è un valore numerico o temporale ma una parola, ad esempio la query può restituire il valore **OK** per la colonna **Risultato**. In questo caso la parola specificata quale limite verrà confrontata con altre condizioni di parole in ordine alfabetico.

Per specificare condizioni di filtraggio complesse:

1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Rapporto** nella parte superiore.
2. Nella finestra visualizzata, nella scheda **Rapporto**, fare clic sul pulsante **Rapporto dettagliato**.
3. Nella finestra visualizzata fare clic sull'area a sinistra della colonna di tabella per la quale si desidera specificare condizioni di filtraggio complesso. Selezionare la voce **Personalizzato** dal menu a discesa. È inoltre possibile selezionare la voce **Filtra per questo campo** nel menu di scelta rapida (vedere la sezione "Visualizzazione dei dati sullo schermo" a pagina 175) che viene visualizzato dopo aver fatto clic con il pulsante destro del mouse sulla colonna desiderata nella tabella.
4. Nella finestra **Filtro personalizzato** visualizzata, specificare le condizioni di filtraggio desiderate.

RICERCA EVENTI

Questa finestra (vedere la figura seguente) è stata progettata per consentire la ricerca degli eventi verificatisi nel sistema ed elaborati da Protezione del computer.

Di seguito vengono descritti i concetti utilizzati per lavorare con questa finestra.

- Il campo **Stringa** viene utilizzato per immettere la parola chiave (ad esempio, explorer). Per avviare la ricerca, fare clic sul pulsante **Trova successivo**. La ricerca dei dati desiderati può richiedere tempo. Una volta

completata la ricerca, gli eventi relativi alla parola chiave inserita verranno visualizzati. Facendo clic sul pulsante **Evidenzia tutto** vengono selezionate tutte le voci trovate corrispondenti alla parola chiave di ricerca.

- Il campo **Colonna** consente di selezionare la colonna della tabella in base alla quale verrà eseguita la ricerca della parola chiave. Questa selezione consente di risparmiare il tempo richiesto per eseguire una ricerca (a meno che, naturalmente, non sia stato selezionato il valore **Tutto**).

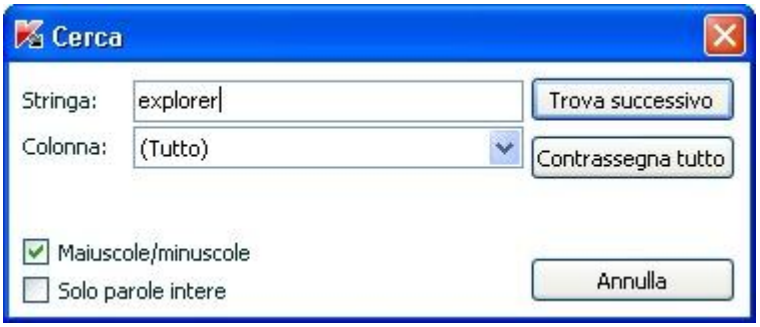


Figura 21. Ricerca eventi

Per effettuare una ricerca sensibile alle maiuscole/minuscole, selezionare la casella **Maiuscole/minuscole**. La casella **Solo parole intere** consente di restringere la ricerca alle sole parole intere.

Per utilizzare la ricerca eventi:

1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Rapporto** nella parte superiore della finestra.
2. Nella finestra visualizzata, nella scheda **Rapporto**, fare clic sul pulsante **Rapporto dettagliato**.
3. Nella finestra visualizzata, fare clic con il tasto destro del mouse sull'area a destra dell'intestazione di qualsiasi colonna di tabella. Scegliere la voce **Cerca** dal menu di scelta rapida.
4. Specificare i criteri di ricerca nella finestra **Cerca** che viene visualizzata.

BACKUP

Durante il processo di backup, copie di backup dei file selezionati vengono create in una speciale area di archiviazione.

Un archivio di backup è un'area dedicata di un disco o di un supporto rimovibile. Gli archivi vengono utilizzati dalle attività di backup per memorizzare copie di backup dei dati.

Durante la creazione di un'area di archiviazione (vedere la sezione "Creazione di un'area per l'archivio di backup" a pagina 179), l'utente seleziona il supporto dati e specifica il nome della nuova area di archiviazione e le impostazioni per l'archiviazione delle copie di backup. È anche possibile proteggere i dati archiviati dagli accessi non autorizzati tramite password. Sul supporto dati vengono inoltre memorizzate informazioni di servizio sull'area di archiviazione.

Per l'esecuzione dei backup di dati, vengono create attività di backup (vedere la sezione "Creazione di un'attività di backup" a pagina 181). *Un'attività di backup* è una raccolta di parametri definita dall'utente che individua i dati da sottoporre a backup, l'area di archiviazione delle copie di backup e le condizioni del backup. Le attività possono essere utilizzate più volte, manualmente o tramite pianificazione.

Le copie di backup di file create nell'ambito di una singola attività vengono memorizzate in *archivi*. Gli archivi di copie di backup vengono denominati in base al nome dell'attività e sono memorizzati in un archivio.

In caso sia necessario ripristinare dati da copie di backup, viene avviata la procedura di ripristino (vedere la sezione "Ripristino dei dati" a pagina 184) o è possibile utilizzare l'utility di ripristino Kaspersky. I file possono essere ripristinati nelle rispettive posizioni originarie o in una qualsiasi cartella disponibile.

Tutti gli eventi relativi al backup vengono memorizzati nel rapporto (vedere la sezione "Visualizzazione del rapporto sugli eventi" a pagina 184).

IN QUESTA SEZIONE:

Creazione di un'area per l'archivio di backup 179

Connessione di un archivio 180

Cancellazione di un archivio 180

Rimozione di un archivio 181

Creazione di un'attività di backup 181

Esecuzione di un'attività di backup 182

Ricerca di copie di backup 182

Visualizzazione dei dati sulle copie di backup 183

Ripristino dei dati 184

Visualizzazione del rapporto sugli eventi 184

CREAZIONE DI UN'AREA PER L'ARCHIVIO DI BACKUP

Un'area per l'archivio di backup può essere creata tramite una procedura guidata. La Creazione guidata archivio di backup può essere avviata in due modi:

- dalla finestra principale del modulo;

- dalla Creazione guidata attività di backup (vedere la sezione "Creazione di un'attività di backup" a pagina 181).

La procedura guidata è costituita da una serie di schermate (passaggi) tra le quali è possibile spostarsi servendosi dei pulsanti **Avanti** e **Indietro**. Per chiudere la procedura guidata al completamento, utilizzare il pulsante **Fine**. Per interrompere la procedura in qualsiasi momento, utilizzare il pulsante **Annulla**.

È anche possibile spostarsi tra i passaggi della procedura guidata completati utilizzando i collegamenti di spostamento nella parte superiore della finestra.

Per creare un'area per l'archivio di backup, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul Pulsante **Backup**.
2. Nella finestra visualizzata, selezionare la sezione **Archivi** e fare clic sul pulsante **Crea**.
3. Verrà avviata la Creazione guidata archivio di backup. I passaggi della procedura guidata sono descritti di seguito:
   a. Nella parte sinistra della finestra **Unità**, selezionare il tipo di supporto di archiviazione dati che verrà utilizzato come archivio di backup.

      Per garantire la sicurezza dei dati, è consigliabile creare archivi di backup in unità disco rimovibili.

   b. Se necessario, nella finestra **Protezione** impostare una password per proteggere i dati dagli accessi non autorizzati.
   c. Se necessario, nella finestra **Impostazioni** specificare il numero massimo di versioni di file che possono coesistere nell'archivio e indicare la durata di archiviazione delle copie di backup.
   d. Nella finestra **Riepilogo**, immettere il nome dell'archivio e confermarne la creazione con le impostazioni specificate.

CONNESSIONE DI UN ARCHIVIO

Se è stato creato un archivio con il modulo Backup, ma non è disponibile nel computer in uso (ad esempio, dopo la reinstallazione del sistema operativo o se l'archivio viene copiato da un altro computer), sarà necessario stabilire la connessione a tale archivio per iniziare a utilizzare i dati.

Per stabilire la connessione a un archivio esistente, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul Pulsante **Backup**.
2. Nella finestra visualizzata, selezionare la sezione **Archivi** e fare clic sul pulsante **Connetti**.
3. Selezionare un tipo di archivio e specificare le impostazioni di connessione desiderate nella finestra **Connetti archivio**.

   Se le impostazioni sono specificate correttamente, l'archivio viene visualizzato nell'elenco.

CANCELLAZIONE DI UN ARCHIVIO

Se il volume di archiviazione non dispone di spazio sufficiente per l'operazione in corso, è possibile eliminare le versioni obsolete e le copie di backup dei file già eliminati dal computer.

Per cancellare un archivio, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Backup**.

2. Nella finestra visualizzata, selezionare la sezione **Archivi**.

3. Selezionare l'archivio da cancellare e fare clic sul pulsante **Cancella**.

4. Nella finestra **Cancella archivio** visualizzata, selezionare le versioni dei file che si desidera eliminare.

RIMOZIONE DI UN ARCHIVIO

Per rimuovere un archivio per il backup di dati, è necessario utilizzare Rimozione guidata archivio. Durante la rimozione, viene chiesto di determinare le operazioni da eseguire sui dati in archivio, prossimi all'eliminazione, e sulle attività che utilizzano l'archivio per le proprie copie di backup.

La procedura guidata è costituita da una serie di schermate (passaggi) tra le quali è possibile spostarsi servendosi dei pulsanti **Avanti** e **Indietro**. Per chiudere la procedura guidata al completamento, utilizzare il pulsante **Fine**. Per interrompere la procedura in qualsiasi momento, utilizzare il pulsante **Annulla**.

È anche possibile spostarsi tra i passaggi della procedura guidata completati utilizzando i pulsanti di spostamento nella parte superiore della finestra.

Per rimuovere un archivio di backup, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Backup**.

2. Nella finestra visualizzata, selezionare la sezione **Archivi**.

3. Selezionare l'archivio che si desidera eliminare e fare clic sul pulsante **Elimina**.

4. Verrà avviata la Rimozione guidata archivio. I passaggi della procedura guidata sono descritti di seguito:

   a. Selezionare un'azione da eseguire sulle copie di backup presenti nell'archivio da rimuovere nella finestra **Contenuto**.

   b. Selezionare un'azione da eseguire sulle attività che utilizzano l'archivio per le proprie copie di backup nella finestra **Attività**.

   c. Confermare la rimozione dell'archivio con le impostazioni selezionate nella finestra **Riepilogo**.

CREAZIONE DI UN'ATTIVITA DI BACKUP

Le attività di backup vengono utilizzate per creare copie di backup dei file.

Un'attività di backup può essere creata utilizzando la procedura guidata.

Quando si crea un'attività di backup, è necessario definire le impostazioni seguenti:

- il set di file di cui creare copie di backup;
- l'archivio in cui crearle;
- le condizioni che comportano l'avvio del processo di backup.

La Creazione guidata attività di backup può essere avviata in due modi:

- dalla finestra principale del modulo;
- dal menu di scelta rapida di Microsoft Windows.

La procedura guidata è costituita da una serie di schermate (passaggi) tra le quali è possibile spostarsi servendosi dei pulsanti **Avanti** e **Indietro**. Per chiudere la procedura guidata al completamento, utilizzare il pulsante **Fine**. Per interrompere la procedura in qualsiasi momento, utilizzare il pulsante **Annulla**.

È anche possibile spostarsi tra i passaggi della procedura guidata completati utilizzando i pulsanti di spostamento nella parte superiore della finestra.

- *Per creare un'attività di backup, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Backup**.
2. Nella finestra visualizzata, selezionare la scheda **Backup** e fare clic sul pulsante **Crea**.
3. Verrà avviata la Creazione guidata attività di backup. I passaggi della procedura guidata sono descritti di seguito:
   a. Nella finestra **Contenuto**, selezionare gli oggetti di cui creare copie di backup.
   b. Nella finestra **Archivio**, selezionare l'archivio in cui creare le copie di backup.
   c. Nella finestra **Pianificazione**, specificare le condizioni per l'esecuzione dell'attività.
   d. Nella finestra **Riepilogo**, immettere il nome dell'attività e confermarne la creazione con le impostazioni specificate.

ESECUZIONE DI UN'ATTIVITA DI BACKUP

Le attività di backup possono essere eseguite automaticamente (tramite pianificazione) o manualmente. La modalità effettiva di esecuzione di un'attività viene visualizzata nell'elenco delle attività (vedere la figura sotto).

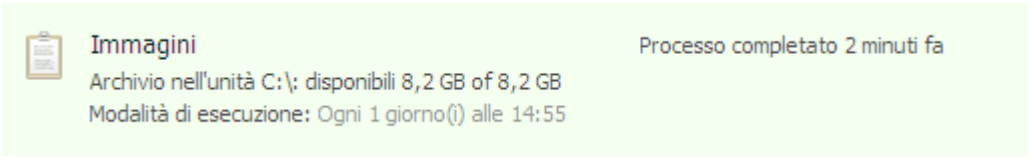


Figura 22. Attività di backup

La pianificazione per l'esecuzione automatica viene configurata al momento della creazione dell'attività, ma può essere modificata successivamente.

- *Per eseguire un'attività di backup manualmente, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e fare clic sul Pulsante **Backup**.
2. Nella finestra visualizzata, selezionare la sezione **Backup**.
3. Dall'elenco presente nella parte destra della finestra, selezionare l'attività da eseguire e fare clic sul collegamento **Esegui**.

   Nella riga dell'attività selezionata viene indicato il tempo trascorso dall'inizio dell'esecuzione. L'attività può essere annullata o sospesa utilizzando i relativi pulsanti presenti nella parte superiore della finestra.

   L'esecuzione dell'attività comporta l'inserimento in archivio di copie di backup aggiornate.

RICERCA DI COPIE DI BACKUP

Per cercare copie di backup in un archivio, è possibile utilizzare il filtro e il campo di ricerca.

Il filtro delle copie di backup consente di visualizzare solo le copie conformi ai criteri di ricerca specificati:

- Dall'elenco a discesa **Archivio**, selezionare il nome dell'attività che ha creato le copie di backup desiderate.
- Nel campo **Data**, specificare la data di creazione delle copie di backup desiderate.
- Dall'elenco a discesa **Categoria**, selezionare i tipi di file le cui copie di backup si desidera trovare.

È possibile trovare una copia di backup immettendone il nome nel campo di ricerca.

Per visualizzare le copie di backup dei file che non sono stati inclusi nell'elenco dei file sottoposti a backup durante l'ultima esecuzione dell'attività (ovvero, che sono stati eliminati dal computer), selezionare la casella **Mostra file eliminati**.

Per filtrare le copie di backup, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul Pulsante **Backup**.
2. Nella finestra visualizzata, selezionare la sezione **Ripristina**.
3. Nella parte sinistra della finestra, selezionare i criteri di ricerca dagli elenchi a discesa del filtro. In questo modo, nella parte destra della finestra verranno visualizzate solo le copie di backup che soddisfano le condizioni specificate.

Per trovare una copia di backup in base al nome, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Backup**.
2. Nella finestra visualizzata, selezionare la sezione **Ripristina**.
3. Nel campo **Cerca** presente nella parte sinistra della finestra, immettere il nome completo o una parte del nome di un file. In questo modo, nella parte destra della finestra verranno elencate solo le copie di backup dei file i cui nomi iniziano con i caratteri specificati.

VISUALIZZAZIONE DEI DATI SULLE COPIE DI BACKUP

Prima di ripristinare i dati, è possibile visualizzare il contenuto della versione della copia di backup selezionata. A tale scopo, è possibile aprire l'ultima versione o selezionare una versione in base alla data specificata.

Per aprire la versione più recente del file, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul Pulsante **Backup**.
2. Nella finestra visualizzata, selezionare la sezione **Ripristina**.
3. Selezionare l'archivio in cui sono contenute le copie di backup desiderate, quindi fare clic sul pulsante **Ripristina dati**.
4. Nella parte sinistra della finestra **Ripristino dei dati dall'archivio** selezionare un archivio.
5. Nella parte destra della finestra, selezionare il file desiderato dall'elenco e fare clic sul pulsante **Apri**.

Per aprire una versione del file in base alla data specificata, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul Pulsante **Backup**.
2. Nella finestra visualizzata, selezionare la sezione **Ripristina**.
3. Selezionare l'archivio in cui sono contenute le copie di backup desiderate, quindi fare clic sul pulsante **Ripristina dati**.

4. Nella parte sinistra della finestra **Ripristino dei dati dall'archivio** selezionare un archivio.
5. Nella parte destra della finestra, selezionare il file desiderato dall'elenco e fare clic sul pulsante **Versioni**.
6. Nella finestra **Versioni file** visualizzata, selezionare la data desiderata e fare clic sul collegamento **Apri**.

RIPRISTINO DEI DATI

Se necessario, è possibile ripristinare i dati dalle copie di backup dei file. La procedura di backup è disponibile solo per gli archivi connessi. Durante il ripristino, i dati prelevati dalle copie di backup vengono salvati nella cartella selezionata.

È possibile ripristinare i file in più modi:

- ripristinare la versione più recente;
- selezionare una versione in base alla data.

Per ripristinare la versione più recente del file, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul Pulsante **Backup**.
2. Nella finestra visualizzata, selezionare la sezione **Ripristina**.
3. Selezionare l'archivio in cui sono contenute le copie di backup desiderate, quindi fare clic sul pulsante **Ripristina dati**.
4. Nella parte sinistra della finestra **Ripristino dei dati dall'archivio** selezionare un archivio.
5. Nella parte destra della finestra, selezionare i file da ripristinare. A tale scopo, selezionare le caselle accanto ai file desiderati. Per selezionare tutti i file, fare clic sul pulsante **Seleziona tutto** nella parte inferiore dell'elenco. Fare clic sul pulsante **Ripristina** nella parte superiore della finestra.
6. Nella finestra **Ripristino** visualizzata selezionare il percorso in cui salvare i file ripristinati e la condizione per il salvataggio se i nomi dei file coincidono. Fare clic sul pulsante **Ripristina**.

Per selezionare la versione desiderata del file, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul Pulsante **Backup**.
2. Nella finestra visualizzata, selezionare la sezione **Ripristina**.
3. Selezionare l'archivio in cui sono contenute le copie di backup desiderate, quindi fare clic sul pulsante **Ripristina dati**.
4. Nella parte sinistra della finestra **Ripristino dei dati dall'archivio** selezionare un archivio.
5. Nella parte destra della finestra, selezionare il file di cui si desidera specificare una versione da ripristinare. A tale scopo, selezionare la casella accanto al file desiderato. Fare clic sul pulsante **Versioni** nella parte superiore della finestra.
6. Nella finestra **Versioni file** visualizzata, selezionare la data della versione da ripristinare e fare clic sul collegamento **Ripristina**.
7. Nella finestra **Ripristino** visualizzata selezionare il percorso in cui salvare i file ripristinati e la condizione per il salvataggio se i nomi dei file coincidono. Fare clic sul pulsante **Ripristina**.

VISUALIZZAZIONE DEL RAPPORTO SUGLI EVENTI

Nel rapporto sono visualizzati tutti gli eventi correlati al backup e al ripristino dei dati.

Per ottenere un report sul modulo di backup, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul Pulsante **Backup**.
2. Nella finestra visualizzata, fare clic sul pulsante **Rapporto** nella parte superiore della finestra.
3. Nella finestra **Rapporto** visualizzata specificare le impostazioni di visualizzazione degli eventi.

PARENTAL CONTROL

Parental Control è un modulo dell'applicazione che consente di controllare diverse azioni utente nel computer locale e in rete. Tale modulo consente di limitare l'accesso a risorse e applicazioni e visualizzare rapporti sulle azioni degli utenti.

Oggi sempre più bambini e adolescenti hanno accesso al computer e alle risorse disponibili in Internet. Questo solleva problemi di sicurezza perché la navigazione e la comunicazione in Internet presentano diversi rischi. Tra questi:

- accesso a siti Web che possono indurre a perdite di tempo (chat, giochi) o denaro (negozi online, aste);
- accesso a risorse Web rivolte a un pubblico adulto (contenenti materiale pornografico o materiale violento correlato all'utilizzo di armi o droga e così via);
- scaricamento di file infettati da programmi dannosi;
- utilizzo eccessivo del computer e di Internet, con potenziali rischi per la salute;
- comunicazione con sconosciuti che si fingono coetanei e tentano di entrare in possesso di dati personali, quali nome reale, indirizzo, orari in cui l'abitazione resta incustodita e così via.

Parental Control consente di ridurre i rischi correlati all'utilizzo del computer e di Internet. A tale scopo, il modulo sfrutta le seguenti funzionalità:

- limitazione del tempo di utilizzo del computer e di Internet;
- creazione di elenchi di siti Web consentiti e bloccati e selezione di categorie di contenuti di siti Web sconsigliati;
- abilitazione della modalità di ricerca sicura;
- limitazione del download di file da Internet;
- creazione di elenchi di contatti consentiti o bloccati;
- visualizzazione del testo dei messaggi;
- divieto di trasferimento di determinati dati personali;
- ricerca di parole chiave nel testo dei messaggi (il numero di parole chiave trovate viene visualizzato nella sezione **Rapporti**);
- creazione di elenchi di applicazioni consentite e bloccate e limitazioni temporali per l'esecuzione delle applicazioni consentite.

Poiché ogni limitazione è abilitabile separatamente, il Parental Control può soddisfare le esigenze di utenti diversi. Per ogni account utente è possibile visualizzare rapporti in cui vengono inclusi gli eventi previsti dalle categorie controllate per il periodo selezionato.

IN QUESTA SEZIONE:

Attivazione e configurazione di Parental Control 186

Limitazione del tempo di accesso a Internet 187

Accesso a siti Web 188

Download di file da Internet 188

Modalità di ricerca sicura 189

Messaggistica immediata 190

Invio di dati personali 191

Ricerca per parole chiave 192

Limitazione del tempo di utilizzo del computer 193

Esecuzione di applicazioni e giochi 193

Salvataggio e download delle impostazioni di Parental Control 194

ATTIVAZIONE E CONFIGURAZIONE DI PARENTAL CONTROL

Per iniziare a gestire il componente, è necessario eseguire la procedura di autenticazione. Dopo aver immesso il nome e la password di amministratore, sarà possibile abilitare, sospendere o disabilitare il Parental Control, nonché modificarne le impostazioni.

Quando il componente è attivo, sarà possibile abilitare e configurare diverse funzioni del Parental Control per i singoli account. Se il componente non è attivo, non verrà eseguito alcun controllo.

- *Per abilitare il Parental Control, eseguire le operazioni seguenti:*

  1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Parental Control**.
  2. Nella finestra visualizzata, selezionare la sezione **Utenti**. Fare clic sul collegamento **Abilita**.

- *Per sospendere Parental Control, eseguire le operazioni seguenti:*

  1. Aprire la finestra principale dell'applicazione e fare clic sul. pulsante **Parental Control**.
  2. Nella finestra visualizzata, selezionare la sezione **Utenti**. Fare clic sul collegamento **Pausa**.
  3. Nella finestra **Sospendi Parental Control**, specificare una modalità di riabilitazione.

  È anche possibile sospendere o riabilitare il Parental Control tramite la finestra principale di Kaspersky PURE.

- *Per configurare il Parental Control per un account, eseguire le operazioni seguenti:*

  1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Parental Control**.
  2. Nella finestra visualizzata selezionare la sezione **Utenti**, selezionare l'account per cui configurare il Parental Control, quindi fare clic sul pulsante **Configura**.

3. Nella finestra visualizzata, selezionare il componente da limitare e specificare le impostazioni di controllo.

Per configurare un alias e un'immagine per un account, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Parental Control**.

2. Nella finestra visualizzata selezionare la sezione **Utenti**, selezionare l'account per cui configurare il Parental Control, quindi fare clic sul pulsante **Configura**.

3. Nella finestra visualizzata, nella sezione **Avanzate**, selezionare il componente **Visualizzazione**. Immettere un alias per l'account e selezionare un'immagine da visualizzare.

VEDERE ANCHE:

Salvataggio e download delle impostazioni di Parental Control 194

LIMITAZIONE DEL TEMPO DI ACCESSO A INTERNET

È possibile limitare il tempo che l'utente trascorre su Internet. A tale scopo, è possibile specificare i giorni e le ore della settimana in cui l'accesso a Internet è consentito o bloccato e limitare il tempo complessivo trascorso in Internet.

Per ogni account utente del computer selezionato è possibile visualizzare statistiche di accesso a Internet e rapporti dettagliati sugli eventi.

Per limitare la durata dell'accesso a Internet, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Parental Control**.

2. Nella finestra visualizzata selezionare la sezione **Utenti**, selezionare l'account utente per cui creare una restrizione, quindi fare clic sul pulsante **Configura**.

3. Nella finestra visualizzata, nella sezione **Internet**, selezionare il componente **Utilizzo**.

4. Nella finestra **Controlla l'utilizzo di Internet** visualizzata, selezionare la casella **Abilita** e specificare le limitazioni temporali.

Per visualizzare statistiche di riepilogo, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Parental Control**.

2. Nella finestra visualizzata selezionare la sezione **Rapporti** e dal menu a discesa selezionare l'account utente per cui si desidera visualizzare il rapporto.

   Le statistiche di riepilogo sull'utilizzo di Internet da parte dell'account utente selezionato vengono visualizzate nella sezione **Internet**.

Per ottenere un rapporto dettagliato, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Parental Control**.

2. Nella finestra visualizzata selezionare la sezione **Rapporti** e dal menu a discesa selezionare l'account utente per cui si desidera visualizzare il rapporto. Fare clic sul collegamento **Rapporto dettagliato**.

3. Nella finestra visualizzata, nella sezione **Internet**, selezionare il componente **Utilizzo**.

   Nella finestra **Utilizzo** visualizzata verrà mostrato un rapporto dettagliato.

È anche possibile aprire il rapporto dettagliato nella sezione **Utenti** facendo clic sul pulsante **Rapporto dettagliato**.

ACCESSO A SITI WEB

È possibile impostare limitazioni dell'accesso a determinate risorse Web a seconda del contenuto. A tale scopo, è necessario creare elenchi di pagine Web consentite e bloccate, nonché scegliere le categorie di siti Web a cui bloccare l'accesso.

Per ogni account utente del computer selezionato è possibile visualizzare statistiche di accesso ai siti Web, nonché un rapporto dettagliato sugli eventi.

- *Per limitare la durata dell'accesso alle risorse Web, eseguire le operazioni seguenti:*

  1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Parental Control**.
  2. Nella finestra visualizzata selezionare la sezione **Utenti**, selezionare l'account utente per cui creare una restrizione, quindi fare clic sul pulsante **Configura**.
  3. Nella finestra visualizzata selezionare la sezione **Internet** e quindi il componente **Accesso a siti Web**.
  4. Nella finestra **Controlla l'accesso ai siti Web** visualizzata, selezionare la casella **Abilita** e specificare le limitazioni dell'accesso ai siti Web.

     Nelle schede **Indirizzi Web bloccati** e **Indirizzi Web consentiti** è possibile immettere gli indirizzi dei siti Web consentiti e bloccati. Nella scheda **Non consigliato** è possibile scegliere le categorie di siti Web a cui bloccare l'accesso.
  5. Nell'elenco a discesa **Azione**, selezionare un'azione predefinita per i siti Web non inclusi nell'elenco dei siti Web consentiti.

  Se si sceglie di bloccare l'accesso ai siti Web non inclusi nell'elenco dei siti Web consentiti come azione predefinita, aggiungere l'indirizzo del server proxy all'elenco degli **indirizzi Web consentiti** per consentire la connessione a Internet utilizzando un proxy.

- *Per visualizzare statistiche di riepilogo, eseguire le operazioni seguenti:*

  1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Parental Control**.
  2. Nella finestra visualizzata selezionare la sezione **Rapporti** e dal menu a discesa selezionare l'account utente per cui si desidera visualizzare il rapporto.

     Le statistiche di riepilogo sui siti Web visitati dall'account selezionato verranno visualizzate nella sezione **Internet**.

- *Per ottenere un rapporto dettagliato, eseguire le operazioni seguenti:*

  1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Parental Control**.
  2. Nella finestra visualizzata selezionare la sezione **Rapporti** e dal menu a discesa selezionare l'account utente per cui si desidera visualizzare il rapporto. Fare clic sul collegamento **Rapporto dettagliato**.
  3. Nella finestra visualizzata selezionare la sezione **Internet** e quindi il componente **Accesso a siti Web**.

     Nella finestra **Accesso a siti Web** visualizzata, verrà visualizzato un rapporto dettagliato.

  È anche possibile aprire il rapporto dettagliato nella sezione **Utenti** facendo clic sul pulsante **Rapporto dettagliato**.

DOWNLOAD DI FILE DA INTERNET

È possibile limitare i tipi di file scaricabili.

È possibile visualizzare statistiche per i file scaricati e bloccati per ogni account utente nel computer selezionato, nonché un rapporto dettagliato degli eventi.

Per limitare il download di file da Internet, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Parental Control**.
2. Nella finestra visualizzata selezionare la sezione **Utenti**, selezionare l'account utente per cui creare una restrizione, quindi fare clic sul pulsante **Configura**.
3. Nella finestra visualizzata, nella sezione **Internet**, selezionare il componente **Download di file**.
4. Nella finestra **Controlla il download di file da Internet** visualizzata, selezionare la casella **Abilita** e selezionare le categorie di file che possono essere scaricati.

Per visualizzare statistiche di riepilogo, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Parental Control**.
2. Nella finestra visualizzata selezionare la sezione **Rapporti** e dal menu a discesa selezionare l'account utente per cui si desidera visualizzare il rapporto.

   Le statistiche di riepilogo sul download di file da Internet per l'account selezionato verranno visualizzate nella sezione **Internet**.

Per ottenere un rapporto dettagliato, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Parental Control**.
2. Nella finestra visualizzata selezionare la sezione **Rapporti** e dal menu a discesa selezionare l'account utente per cui si desidera visualizzare il rapporto. Fare clic sul collegamento **Rapporto dettagliato**.
3. Nella finestra visualizzata, nella sezione **Internet**, selezionare il componente **Download di file**.

   Nella finestra visualizzata **Download di file** verrà presentato un rapporto dettagliato.

È anche possibile aprire il rapporto dettagliato nella sezione **Utenti** facendo clic sul pulsante **Rapporto dettagliato**.

MODALITA DI RICERCA SICURA

Alcuni motori di ricerca si sforzano di proteggere gli utenti dai contenuti di siti Web inappropriati. A tale scopo, durante l'indicizzazione dei siti Web utilizzano alcune frasi e parole chiave, categorie e indirizzi di siti Web. Per abilitare la modalità di ricerca sicura, vengono escluse dalla ricerca le seguenti categorie di siti Web: porno, droga, violenza e altri siti rivolti a un pubblico adulto.

Il Parental Control consente di passare alla modalità di ricerca sicura per i seguenti motori di ricerca simultaneamente:

- Google;
- Bing.com

Per passare alla modalità di ricerca sicura, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Parental Control**.
2. Nella finestra visualizzata selezionare la sezione **Utenti**, selezionare l'account utente per cui creare una restrizione, quindi fare clic sul pulsante **Configura**.
3. Nella finestra visualizzata, nella sezione **Internet**, selezionare il componente **Ricerca sicura**.
4. Nella finestra **Controlla i risultati della ricerca** visualizzata, selezionare la casella **Abilita**.

MESSAGGISTICA IMMEDIATA

Controllare la messaggistica immediata significa controllare i contenuti della corrispondenza e i contatti con cui è consentito scambiare messaggi. È possibile creare elenchi di contatti consentiti e bloccati, specificare parole chiave (vedere la sezione "Ricerca per parole chiave" a pagina. 192) in base alle quali verranno controllati tutti i messaggi in entrata e specificare i dati personali (vedere la sezione "Invio di dati personali" a pagina 191) che non è consentito inviare.

Se la messaggistica con un contatto è vietata, tutti i messaggi scambiati con tale contatto verranno bloccati. Nel rapporto vengono visualizzate informazioni sui messaggi bloccati e sulla presenza di parole chiave nei messaggi. Nel rapporto completo è possibile visualizzare la cronologia messaggi per ogni contatto.

Il controllo della messaggistica presenta le seguenti limitazioni:

- Se il client IM è stato avviato prima di Parental Control, il controllo della messaggistica non verrà attuato fino al riavvio del client IM.
- Quando si utilizzano proxy HTTP, il controllo della messaggistica non verrà attuato.

La versione corrente di Parental Control assicura il controllo delle comunicazioni svolte tramite i seguenti client IM:

- ICQ;
- QIP
- Windows Live Messenger (MSN);
- Yahoo Messenger;
- GoogleTalk;
- mIRC;
- Mail.Ru Agent;
- Psi;
- Miranda;

Alcuni client IM utilizzano la connessione crittografata. Per controllare la messaggistica di tali programmi, è necessario abilitare la scansione delle connessioni crittografate (vedere pagina 167).

Per limitare i contatti di messaggistica immediata, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Parental Control**.
2. Nella finestra visualizzata selezionare la sezione **Utenti**, selezionare l'account utente per cui creare una restrizione, quindi fare clic sul pulsante **Configura**.
3. Nella finestra visualizzata selezionare il componente **Messaggistica immediata** nella sezione **Messaggistica**.
4. Nella finestra **Controlla la messaggistica istantanea** visualizzata selezionare la casella **Abilita**.
5. Nelle schede **Consentiti** e **Bloccati** creare elenchi di contatti consentiti e bloccati.
6. Nell'elenco a discesa **Azione**, selezionare l'azione predefinita per i contatti non inclusi negli elenchi.

È inoltre possibile consentire o bloccare le comunicazioni con il contatto selezionato dal rapporto dettagliato sugli eventi per tale account.

Per visualizzare statistiche di riepilogo, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Parental Control**.
2. Nella finestra visualizzata selezionare la sezione **Rapporti** e dal menu a discesa selezionare l'account utente per cui si desidera visualizzare il rapporto.

   Nella sezione **Messaggistica** verranno visualizzate le statistiche di messaggistica IM di riepilogo per l'account utente selezionato.

Per ottenere un rapporto dettagliato, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Parental Control**.
2. Nella finestra visualizzata selezionare la sezione **Rapporti** e dal menu a discesa selezionare l'account utente per cui si desidera visualizzare il rapporto. Fare clic sul collegamento **Rapporto dettagliato**.
3. Nella finestra visualizzata selezionare il componente **Messaggistica immediata** nella sezione **Messaggistica**.

   Nella finestra **Messaggistica immediata** visualizzata verrà mostrato un rapporto dettagliato.

È anche possibile aprire il rapporto dettagliato nella sezione **Utenti** facendo clic sul pulsante **Rapporto dettagliato**.

INVIO DI DATI PERSONALI

È possibile vietare l'invio di dati contenenti informazioni personali. A tale scopo, creare un elenco di record contenenti dati riservati, quali l'indirizzo dell'abitazione, il numero di telefono e così via.

I tentativi di inviare dati contenuti nell'elenco verranno bloccati e le informazioni sui messaggi bloccati verranno visualizzate nel rapporto.

Per bloccare l'invio di dati specifici:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Parental Control**.
2. Nella finestra visualizzata selezionare la sezione **Utenti**, selezionare l'account utente per cui creare una restrizione, quindi fare clic sul pulsante **Configura**.
3. Nella finestra visualizzata, nella sezione **Messaggistica**, selezionare il componente **Dati personali**.
4. Nella finestra **Controlla l'invio di dati personali** visualizzata, selezionare la casella **Abilita**. Aggiungere il record all'elenco dei dati di cui si desidera impedire l'invio facendo clic sul collegamento **Aggiungi**.

Per visualizzare statistiche di riepilogo, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Parental Control**.
2. Nella finestra visualizzata selezionare la sezione **Rapporti** e dal menu a discesa selezionare l'account utente per cui si desidera visualizzare il rapporto.

   Nella sezione **Messaggistica** verranno visualizzate statistiche di riepilogo sul trasferimento di dati personali per l'account selezionato.

Per ottenere un rapporto dettagliato, eseguire le operazioni seguenti:

1. Aprire lafinestra principale dell'applicazione e fare clic sul pulsante **Parental Control**.

2. Nella finestra visualizzata selezionare la sezione **Rapporti** e dal menu a discesa selezionare l'account utente per cui si desidera visualizzare il rapporto. Fare clic sul collegamento **Rapporto dettagliato**.

3. Nella finestra visualizzata, nella sezione **Messaggistica**, selezionare il componente **Dati personali**.

   Nella finestra visualizzata **Dati personali** verrà presentato un rapporto dettagliato.

> È anche possibile aprire il rapporto dettagliato nella sezione **Utenti** facendo clic sul pulsante **Rapporto dettagliato**.

RICERCA PER PAROLE CHIAVE

È possibile controllare la presenza di parole chiave nella messaggistica istantanea.

Ogni volta che una parola chiave contenuta nell'elenco viene trovata nei messaggi, l'evento viene segnalato nel rapporto.

> Se Controllo della messaggistica immediata (vedere la sezione "Messaggistica immediata" a pagina 190) è disabilitato, la ricerca delle parole chiave non viene eseguita.

- *Per abilitare il controllo delle parole chiave nella messaggistica, eseguire le operazioni seguenti:*

  1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Parental Control**.

  2. Nella finestra visualizzata selezionare la sezione **Utenti**, selezionare l'account utente per cui creare una restrizione, quindi fare clic sul pulsante **Configura**.

  3. Nella finestra visualizzata, nella sezione **messaggistica**, selezionare il componente **Parole chiave**.

  4. Nella finestra **Controlla l'utilizzo di parole chiave** visualizzata, selezionare la casella ☑ **Abilita**. Aggiungere il record all'elenco delle parole chiave che vengono controllate nella messaggistica facendo clic sul collegamento **Aggiungi**.

- *Per visualizzare statistiche di riepilogo, eseguire le operazioni seguenti:*

  1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Parental Control**.

  2. Nella finestra visualizzata selezionare la sezione **Rapporti** e dal menu a discesa selezionare l'account utente per cui si desidera visualizzare il rapporto.

     Le statistiche di riepilogo sulle parole chiave trovate nei messaggi dell'account utente selezionato vengono visualizzate nella sezione **Messaggistica**.

- *Per ottenere un rapporto dettagliato, eseguire le operazioni seguenti:*

  1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Parental Control**.

  2. Nella finestra visualizzata selezionare la sezione **Rapporti** e dal menu a discesa selezionare l'account utente per cui si desidera visualizzare il rapporto. Fare clic sul collegamento **Rapporto dettagliato**.

  3. Nella finestra visualizzata, nella sezione **messaggistica**, selezionare il componente **Parole chiave**.

     Nella finestra **Parole chiave** visualizzata verrà presentato un rapporto dettagliato.

> È anche possibile aprire il rapporto dettagliato nella sezione **Utenti** facendo clic sul pulsante **Rapporto dettagliato**.

LIMITAZIONE DEL TEMPO DI UTILIZZO DEL COMPUTER

È possibile creare una pianificazione dell'accesso degli utenti al computer in base ai giorni della settimana e alle ore del giorno, nonché limitare il tempo totale di utilizzo giornaliero.

È possibile visualizzare statistiche di accesso al computer per ogni account utente del computer selezionato, nonché un rapporto dettagliato sugli eventi.

- *Per limitare l'utilizzo giornaliero del computer:*

  1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Parental Control**.
  2. Nella finestra visualizzata selezionare la sezione **Utenti**, selezionare l'account utente per cui creare una restrizione, quindi fare clic sul pulsante **Configura**.
  3. Nella finestra visualizzata, nella sezione **Computer**, selezionare il componente **Utilizzo**.
  4. Nella finestra **Controlla l'utilizzo del computer** visualizzata, selezionare le caselle **Abilita** e impostare restrizioni temporali.

- *Per visualizzare statistiche di riepilogo, eseguire le operazioni seguenti:*

  1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Parental Control**.
  2. Nella finestra visualizzata selezionare la sezione **Rapporti** e dal menu a discesa selezionare l'account utente per cui si desidera visualizzare il rapporto.

     Statistiche di riepilogo sull'utilizzo del computer da parte dell'account selezionato verranno visualizzate nella sezione **Computer**.

- *Per ottenere un rapporto dettagliato, eseguire le operazioni seguenti:*

  1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Parental Control**.
  2. Nella finestra visualizzata selezionare la sezione **Rapporti** e dal menu a discesa selezionare l'account utente per cui si desidera visualizzare il rapporto. Fare clic sul collegamento **Rapporto dettagliato**.
  3. Nella finestra visualizzata, nella sezione **Computer**, selezionare il componente **Utilizzo**.

     Nella finestra **Utilizzo** visualizzata verrà mostrato un rapporto dettagliato.

     È anche possibile aprire il rapporto dettagliato nella sezione **Utenti** facendo clic sul pulsante **Rapporto dettagliato**.

ESECUZIONE DI APPLICAZIONI E GIOCHI

È possibile consentire o bloccare l'avvio di determinate applicazioni e giochi, nonché limitare l'avvio delle applicazioni consentite in base all'ora.

È possibile visualizzare statistiche dell'avvio di applicazioni e giochi per ogni account utente del computer selezionato, nonché un rapporto dettagliato sugli eventi.

- *Per limitare l'avvio di applicazioni e giochi:*

  1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Parental Control**.
  2. Nella finestra visualizzata selezionare la sezione **Utenti**, selezionare l'account utente per cui creare una restrizione, quindi fare clic sul pulsante **Configura**.

3. Nella finestra visualizzata, nella sezione **Computer**, selezionare il componente **Applicazioni in esecuzione**.

4. Nella finestra **Controlla l'esecuzione delle applicazioni** visualizzata, selezionare la casella **Abilita**.

5. Creare elenchi di applicazioni consentite e bloccate nelle schede **Consentite** e **Bloccate** e impostare la pianificazione per l'esecuzione delle applicazioni consentite.

Per visualizzare statistiche di riepilogo, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Parental Control**.

2. Nella finestra visualizzata selezionare la sezione **Rapporti** e dal menu a discesa selezionare l'account utente per cui si desidera visualizzare il rapporto.

   Statistiche di riepilogo sull'avvio di applicazioni e giochi per l'account selezionato vengono visualizzate nella sezione **Computer**.

Per ottenere un rapporto dettagliato, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Parental Control**.

2. Nella finestra visualizzata selezionare la sezione **Rapporti** e dal menu a discesa selezionare l'account utente per cui si desidera visualizzare il rapporto. Fare clic sul collegamento **Rapporto dettagliato**.

3. Nella finestra visualizzata, nella sezione **Computer**, selezionare il componente **Applicazioni in esecuzione**.

   Nella finestra **Applicazioni in esecuzione** visualizzata verrà presentato un rapporto dettagliato.

> È anche possibile aprire il rapporto dettagliato nella sezione **Utenti** facendo clic sul pulsante **Rapporto dettagliato**.

SALVATAGGIO E DOWNLOAD DELLE IMPOSTAZIONI DI PARENTAL CONTROL

Se il Parental Control è stato configurato per un account, le impostazioni potranno essere salvate come file. In seguito, le impostazioni salvate in tale file potranno essere importate per una rapida configurazione. È inoltre possibile utilizzare le impostazioni di controllo di un account diverso o utilizzare un modello di configurazione, ovvero set di regole preconfigurati per diversi tipi di utenti in base all'età, all'esperienza e ad altri parametri.

Al termine dell'importazione, le impostazioni selezionate per un singolo account saranno comunque modificabili.

Per salvare le impostazioni di controllo in un file, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Parental Control**.

2. Nella finestra visualizzata selezionare la sezione **Utenti**, selezionare l'account per cui salvare le impostazioni di Parental Control, quindi fare clic sul pulsante **Configura**.

3. Fare clic sul collegamento **Salva impostazioni** nella parte superiore della finestra visualizzata e salvare il file di configurazione.

Per caricare le impostazioni di controllo da un file, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Parental Control**.

2. Nella finestra visualizzata selezionare la sezione **Utenti**, selezionare l'account per cui applicare le impostazioni di Parental Control, quindi fare clic sul pulsante **Configura**.

3. Nella parte superiore della finestra visualizzata fare clic sul collegamento **Carica impostazioni**.

4. Nella finestra **Carica impostazioni di controllo** visualizzata selezionare l'opzione **File di configurazione** e specificare il percorso del file.

- *Per utilizzare le impostazioni di un account diverso, eseguire la procedura seguente:*

  1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Parental Control**.
  2. Nella finestra visualizzata selezionare la sezione **Utenti**, selezionare l'account per cui applicare le impostazioni di Parental Control, quindi fare clic sul pulsante **Configura**.
  3. Nella parte superiore della finestra visualizzata fare clic sul collegamento **Carica impostazioni**.
  4. Nella finestra **Carica impostazioni di controllo** visualizzata, selezionare l'opzione **Altro utente** e specificare l'account da cui si desidera copiare le impostazioni.

- *Per utilizzare un modello di configurazione, eseguire le operazioni seguenti:*

  1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Parental Control**.
  2. Nella finestra visualizzata selezionare la sezione **Utenti**, selezionare l'account per cui utilizzare le impostazioni predefinite di Parental Control, quindi fare clic sul pulsante **Configura**.
  3. Nella parte superiore della finestra visualizzata fare clic sul collegamento **Carica impostazioni**.
  4. Nella finestra **Carica impostazioni di controllo** visualizzata, selezionare l'opzione **Modello** e specificare il modello contenente le impostazioni che si desidera utilizzare.

OTTIMIZZAZIONE DEL SISTEMA

Garantire la protezione del computer è un'attività complessa che richiede una conoscenza approfondita delle funzioni del sistema operativo e delle vulnerabilità dei software. D'altro canto, la grande quantità e varietà di informazioni sulla protezione dei sistemi ne complica l'analisi e l'elaborazione.

Per facilitare l'esecuzione di attività specifiche mirate a garantire la protezione del computer, nel prodotto Kaspersky PURE è stato incluso un insieme di procedure guidate e di strumenti:

- La Configurazione guidata del browser (vedere pagina 196) consente di eseguire l'analisi e la valutazione delle impostazioni di Microsoft Internet Explorer, innanzitutto rispetto alla protezione.
- Il Ripristino guidato del sistema (vedere pagina 197) elimina le tracce della presenza di oggetti malware nel sistema.
- La Creazione guidata del Disco di Ripristino (vedere pagina 198) consente di ripristinare l'operatività del sistema dopo l'attacco di un virus o se i file di sistema del sistema operativo sono danneggiati e non è possibile riavviarlo nello stato precedente.
- L'Eliminazione guidata dei dati (vedere pagina 200) permette di eliminare i dati riservati senza alcuna possibilità di ripristinarli in futuro.
- La Cancellazione guidata dei dati (vedere pagina 201) consente di eliminare i file temporanei e inutilizzati dal computer e di ottimizzare il funzionamento del sistema.
- La Pulizia guidata dei dati riservati (vedere pagina 202) cerca ed elimina le tracce delle attività dell'utente nel sistema.

IN QUESTA SEZIONE:

Configurazione del browser 196

Ripristino dopo un'infezione 197

Disco di Ripristino 198

Eliminazione definitiva dei dati 200

Eliminazione dei dati inutilizzati 201

Pulizia guidata dei dati riservati 202

CONFIGURAZIONE DEL BROWSER

La Configurazione guidata del browser analizza le impostazioni di Microsoft Internet Explorer valutandole innanzitutto dal punto di vista della protezione. È possibile, infatti, che alcune impostazioni selezionate dall'utente o predefinite possano determinare problemi di protezione.

La procedura guidata verifica se sono stati installati gli ultimi aggiornamenti software del browser e se le relative impostazioni contengono vulnerabilità potenziali utilizzabili dagli intrusi per causare danni al computer. Esempi di oggetti analizzati:

- **La cache di Microsoft Internet Explorer**. La cache contiene dati riservati da cui è possibile ottenere anche una cronologia dei siti Web visitati dall'utente. Alcuni oggetti malware esaminano la cache durante la scansione del disco e gli intrusi possono ottenere l'indirizzo di posta elettronica dell'utente. Si consiglia di cancellare il contenuto della cache ogni volta che si chiude il browser.

- **Visualizzazione delle estensioni dei file di formato conosciuto**. Un'opzione di Esplora risorse consente di nascondere le estensioni dei file. Alcuni oggetti malware utilizzano l'estensione doppia e in tal caso l'utente può vedere solo una parte del nome file senza l'estensione reale. Questo schema viene utilizzato spesso dagli intrusi. Si consiglia di abilitare la visualizzazione delle estensioni per i file di formato conosciuto.

- **L'elenco di siti attendibili**. Gli oggetti malware possono aggiungere a questo elenco collegamenti a diversi siti dell'intruso.

Chiudere tutte le finestre di Microsoft Internet Explorer prima di avviare la diagnostica.

Una volta completata la revisione, la procedura guidata analizza le informazioni per valutare se sono presenti problemi di protezione del sistema che richiedono attenzione immediata. Compila quindi un elenco di azioni da eseguire per eliminare i problemi. Tali azioni vengono raggruppate in categorie in base alla gravità dei problemi rilevati.

Inoltre, una volta completata la procedura guidata, viene generato un rapporto che può essere inviato a Kaspersky Lab per l'analisi.

Tenere presente che alcune impostazioni possono causare problemi con la visualizzazione di determinati siti (ad esempio se utilizzano controlli ActiveX). Questo problema può essere risolto aggiungendo tali siti all'area attendibile.

La procedura guidata è costituita da una serie di schermate (passaggi) tra le quali è possibile spostarsi servendosi dei pulsanti **Avanti** e **Indietro**. Per chiudere la procedura guidata al completamento, utilizzare il pulsante **Fine**. Per interrompere la procedura in qualsiasi momento, utilizzare il pulsante **Annulla**.

Per avviare la procedura guidata:

1. Aprire la finestra principaledell'applicazione.
2. Nella sezione **Protezione+** fare clic sul pulsante **Ottimizzazione del sistema**.
3. Nella finestra visualizzata fare clic sul pulsante **Ottimizzazione delle impostazioni del browser Internet**.

RIPRISTINO DOPO UN'INFEZIONE

Il Ripristino guidato del sistema elimina le tracce di azioni di oggetti malware nel 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. Se si sospetta che il computer sia infetto, è possibile anche utilizzare la procedura guidata.

La procedura guidata verifica se sono state apportate modifiche al sistema, ad esempio il blocco dell'accesso alla rete, la modifica delle estensioni file di formato conosciuto o il blocco della barra degli strumenti. Tali danni possono essere causati dalle azioni di programmi dannosi, da problemi del sistema e da un funzionamento errato delle applicazioni di ottimizzazione del sistema.

Una volta completata la revisione, la procedura guidata analizza le informazioni raccolte per verificare la presenza di danni del sistema che richiedono attenzione immediata. In base alla revisione, viene generato un elenco di azioni necessarie per eliminare i problemi. Tali azioni vengono raggruppate in categorie in base alla gravità dei problemi rilevati.

La procedura guidata è costituita da una serie di schermate (passaggi) tra le quali è possibile spostarsi servendosi dei pulsanti **Avanti** e **Indietro**. Per chiudere la procedura guidata al completamento, utilizzare il pulsante **Fine**. Per interrompere la procedura in qualsiasi momento, utilizzare il pulsante **Annulla**.

Per avviare la procedura guidata:

1. Aprire la finestra principale dell'applicazione.
2. Nella sezione **Protezione+** fare clic sul pulsante **Ottimizzazione del sistema**.
3. Nella finestra visualizzata, fare clic sul pulsante **Ripristino di sistema**.

DISCO DI RIPRISTINO

Kaspersky PURE comprende un servizio che consente di creare un Disco di Ripristino.

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

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

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

Un computer con il sistema operativo danneggiato viene avviato da un dispositivo CD/DVD-ROM. A tale scopo, è necessario che il computer sia dotato di un dispositivo appropriato.

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

1. Aprire la finestra principale dell'applicazione.
2. Nella sezione **Protezione+** fare clic sul pulsante **Ottimizzazione del sistema**.
3. Nella finestra visualizzata fare clic sul pulsante **Creazione di un Disco di Ripristino** per eseguire la creazione guidata del disco.
4. Seguire le istruzioni della procedura guidata.
5. Utilizzando il file fornito con la procedura guidata, creare un CD/DVD di avvio. A tale scopo, è possibile utilizzare un'applicazione di masterizzazione di CD/DVD, come Nero.

VEDERE ANCHE:

Creazione del Disco di Ripristino 198

Avvio del computer attraverso il Disco di Ripristino 199

CREAZIONE DEL DISCO DI RIPRISTINO

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

L'immagine del disco di origine da utilizzare come base per la creazione del nuovo file può essere scaricata dal server Kaspersky Lab o copiata da un'origine locale.

Il file di immagine creato mediante la procedura guidata verrà salvato nella cartella "*Documents and Settings\All Users\Dati applicazioni\Kaspersky Lab\AVP9\Data\Rdisk*" o "*ProgramData\Kaspersky Lab\AVP9\Data\Rdisk*" per Microsoft Vista e verrà denominato *rescuecd.iso*. Se la procedura guidata rileva un file ISO creato in precedenza nella cartella specificata, è possibile utilizzarlo come immagine del disco originale selezionando la casella **Usa file ISO**

esistente e andare al passaggio 3 in cui viene eseguito l'aggiornamento dell'immagine. Se la procedura guidata non rileva alcun file di immagine, questa casella non sarà disponibile.

Il disco di ripristino viene creato mediante una procedura guidata costituita da una serie di caselle (passaggi) visualizzabili mediante i pulsanti **Indietro** e **Avanti**. Per terminare la procedura, fare clic sul pulsante **Fine**. Per interrompere la procedura in qualsiasi momento, utilizzare il pulsante **Annulla**.

VEDERE ANCHE:

Avvio del computer attraverso il Disco di Ripristino 199

AVVIO DEL COMPUTER ATTRAVERSO IL DISCO DI RIPRISTINO

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

Per caricare il sistema operativo, sarà necessario il file di immagine del disco di avvio (con estensione iso). È possibile scaricare un file ISO dal server Kaspersky Lab o aggiornare quello esistente.

Di seguito viene illustrato in modo dettagliato il funzionamento del Disco di Ripristino. Durante il caricamento del disco, vengono eseguite le operazioni seguenti:

1. Rilevamento automatico dell'hardware del computer.
2. Ricerca dei file system nei dischi rigidi. Ai file system rilevati verranno assegnati nomi che iniziano con *C*.

   È possibile che ai dischi rigidi e ai dispositivi rimovibili vengano assegnati nomi che non corrispondono a quelli assegnati dal sistema operativo.

   Se il sistema operativo del computer caricato è in modalità di sospensione o se il relativo file system presenta lo stato *infetto* a causa di una chiusura non corretta, l'utente potrà scegliere se installare il file system o riavviare il computer.

   L'installazione del file system potrebbe comportarne il danneggiamento.
3. Ricerca del file swap di Microsoft Windows *pagefile.sys*. Se tale file è assente, il volume della memoria virtuale sarà limitato dalla dimensione della RAM.
4. Selezione della lingua di localizzazione. Se la selezione non viene effettuata dopo un determinato intervallo di tempo, per impostazione predefinita verrà impostata la lingua inglese.
5. Ricerca (creazione) nelle cartelle di database anti-virus, rapporti, memoria di quarantena e file aggiuntivi. Per impostazione predefinita, verranno utilizzate le cartelle delle applicazioni di Kaspersky Lab, installate nel computer infetto (*ProgramData/Kaspersky Lab/AVP8* - per Microsoft Windows Vista, *Documents and Settings/All Users/Dati applicazioni/Kaspersky Lab/AVP8* - per le versioni precedenti di Microsoft Windows). Se non è possibile individuare tali cartelle, verrà effettuato il tentativo di crearle. Se non è possibile trovare le cartelle né crearle, la cartella *kl.files* verrà creata in un disco di sistema.
6. Tentativo di configurazione delle connessioni di rete in base ai dati rilevati nei system file del computer di cui è in corso il caricamento.
7. Caricamento del sottosistema grafico e avvio del Disco di Ripristino Kaspersky.

Nella modalità di ripristino del sistema sono disponibili solo le attività di scansione anti-virus e di aggiornamento dei database da un'origine locale, nonché il rollback degli aggiornamenti e la visualizzazione delle statistiche.

Per caricare il sistema operativo di un computer infetto, eseguire le operazioni seguenti:

1. Nelle impostazioni del BIOS abilitare l'avvio dal CD/DVD-ROM. Per informazioni dettagliate, fare riferimento alla documentazione relativa alla scheda madre installata nel computer.

2. Inserire il CD/DVD con l'immagine del Disco di Ripristino nell'unità CD/DVD di un computer infetto.

3. Riavviare il computer.

Le operazioni di avvio successive verranno eseguite in base all'algoritmo descritto prima. Per ulteriori dettagli sulle funzionalità del Disco di Ripristino, fare riferimento alla Guida del Disco di Ripristino Kaspersky.

VEDERE ANCHE:

Creazione del Disco di Ripristino.....198

ELIMINAZIONE DEFINITIVA DEI DATI

La sicurezza dei dati non è garantita solo dalla protezione contro virus, Trojan e altri tipi di malware, ma anche dalla protezione contro il ripristino non autorizzato di informazioni eliminate.

L'eliminazione dei dati con gli strumenti standard di Microsoft Windows non è in grado di garantire una completa protezione e impedire un possibile ripristino. I dati non scompaiono dal disco rigido quando vengono eliminati. Sono memorizzati nei settori del disco contrassegnati come liberi. Il record del file nella tabella file è l'unico elemento eliminato. Nemmeno la formattazione dei supporti di archiviazione (quali dischi rigidi, schede flash o schede USB) può garantire la totale eliminazione dei dati. Si ritiene che i dati possano essere eliminati solo dopo numerosi cicli di registrazione. Tuttavia, anche in questo caso, le informazioni possono essere ripristinate utilizzando strumenti software ad alte prestazioni.

Kaspersky PURE include una procedura guidata per l'eliminazione definitiva dei dati. Questa procedura guidata consente di eliminare i dati riservati senza offrire agli hacker alcuna opportunità di ripristinarli e utilizzarli. L'eliminazione definitiva dei dati impedisce il ripristino delle informazioni utilizzando strumenti software comuni. La procedura guidata è utilizzabile sia per gli oggetti di piccole dimensioni che per quelli di grandi dimensioni (fino a diversi gigabyte).

A seconda delle condizioni correnti, la procedura guidata supporta l'eliminazione di dati dai seguenti supporti di archiviazione:

- unità disco locali – l'eliminazione è possibile se l'utente dispone dei diritti necessari per la registrazione e l'eliminazione di informazioni;

- qualsiasi disco rimovibile o altro dispositivo che possa essere rilevato come un'unità rimovibile, come ad esempio dischi floppy, schede flash, schede USB o telefoni cellulari). I dati possono essere eliminati da una scheda flash se la protezione meccanica dalla riscrittura (modalità di blocco) è disattivata.

Prima di avviare l'eliminazione definitiva, l'applicazione rileva se è possibile eliminare i dati dal supporto di archiviazione selezionato. La procedura di eliminazione può essere eseguita solo se il supporto di archiviazione selezionato supporta l'eliminazione dei dati. In caso contrario, non è possibile eliminare definitivamente i dati.

È possibile eliminare oggetti come file o cartelle. Per evitare l'eliminazione accidentale di dati utili, è possibile selezionare un solo oggetto per l'eliminazione, anche se la cartella selezionata contiene numerosi file o cartelle nidificate.

La cartella selezionata per l'eliminazione può contenere file di sistema la cui rimozione potrebbe causare errori del sistema operativo. Se tra i dati selezionati vengono rilevati file e cartelle di sistema, la procedura guidata richiede un'ulteriore conferma prima di procedere all'eliminazione.

I metodi per l'eliminazione definitiva dei dati personali sono standardizzati. Sono basati su più cicli di riscrittura delle informazioni eliminate con uno, zero o simboli casuali. La velocità e la qualità dell'eliminazione possono variare a seconda del numero di cicli.

È possibile scegliere uno dei seguenti standard di eliminazione dei dati:

- **Eliminazione rapida**. Il processo di eliminazione è formato da due cicli di riscrittura dei dati: scrittura di zero e numeri pseudocasuali. Il principale vantaggio di questo algoritmo è la velocità. Due cicli sono sufficienti per complicare le operazioni degli strumenti di ripristino dei dati. Anche se un file viene ripristinato, i dati risulteranno inutilizzabili.

- **Standard GOST P 50739-95, Federazione russa**. L'algoritmo esegue un solo ciclo di riscrittura utilizzando numeri pseudocasuali e protegge i dati dal ripristino tramite strumenti comuni. Questo metodo rappresenta il secondo di sei livelli di protezione in base alla classificazione della State Technical Commission.

- **Standard VSITR, Germania**. L'algoritmo esegue sette cicli di riscrittura. Questo metodo è considerato affidabile, ma richiede più tempo per l'esecuzione.

- **Algoritmo Bruce Schneier**. Il processo è formato da sette cicli di riscrittura. Il metodo differisce dallo standard VSITR per la sequenza di riscrittura. Questo metodo avanzato di eliminazione dei dati viene considerato il più affidabile.

- **Standard NAVSO P-5239-26 (MFM), USA** e **standard NAVSO P-5239-26 (RLL), USA**. L'algoritmo esegue tre cicli di riscrittura. Gli standard differiscono tra loro per la sequenza di eliminazione dei dati.

- **Standard DoD 5250.22-M, USA**. L'algoritmo esegue tre cicli di riscrittura. È considerato un metodo affidabile per la protezione da persone prive di speciali strumenti, tuttavia i dati possono essere ripristinati nella maggior parte dei casi.

È possibile eliminare solo i dati a cui è possibile accedere tramite il proprio account personale. Prima di eliminare i dati, assicurarsi che il file o la cartella non sia aperto o in uso da altre applicazioni.

Per avviare la procedura guidata:

1. Aprire la finestra principale dell'applicazione.
2. Nella sezione **Protezione+** fare clic sul pulsante **Ottimizzazione del sistema**.
3. Nella finestra visualizzata, fare clic sul pulsante **Elimina definitivamente i dati**.
4. Nella finestra **Elimina definitivamente i dati** visualizzata selezionare un oggetto utilizzando il pulsante **Sfoglia**, quindi selezionare un oggetto da eliminare nella finestra **Seleziona cartella** visualizzata.

   Nell'elenco a discesa **Metodo di eliminazione dati** selezionare l'algoritmo di eliminazione dei dati desiderato.
5. Nella finestra visualizzata confermare il ripristino dei dati facendo clic sul pulsante **OK**. Se alcuni file non vengono eliminati, tentare di eliminarli nuovamente facendo clic sul pulsante **Riprova** nella finestra visualizzata. Per selezionare un altro oggetto da eliminare, fare clic sul pulsante **Fine**.

ELIMINAZIONE DEI DATI INUTILIZZATI

Il sistema spesso accumula un numero eccessivo di file temporanei o inutilizzati che ne riducono le prestazioni.

Tutte le applicazioni o i sistemi operativi creano file temporanei all'avvio. Tuttavia, alcuni di essi non vengono eliminati alla chiusura dell'applicazione o del sistema operativo. I file temporanei o inutilizzati spesso richiedono una grande quantità di memoria. Inoltre, possono essere sfruttati da programmi dannosi. Le informazioni inutilizzate includono i seguenti file:

- registri eventi di sistema, in cui vengono registrati i nomi di tutte le applicazioni attive;
- registri eventi di varie applicazioni (come Microsoft Office, Microsoft Visio o Macromedia Flash Player) o utilità di aggiornamento (come Windows Update o Adobe Updater);
- registri di connessione di sistema;

- file temporanei dei browser Internet (cookie);
- file temporanei rimanenti dopo l'installazione o la rimozione di applicazioni;
- contenuto del Cestino;
- file nella cartella TEMP, le cui dimensioni possono arrivare a diversi gigabyte.

Kaspersky PURE include la Cancellazione guidata dei dati. Lo scopo di questa procedura guidata è aiutare l'utente a ottimizzare il funzionamento del sistema. Oltre a eliminare i file inutilizzati dal sistema, la procedura guidata rimuove i file che possono contenere dati riservati (password, nomi utente, dati da moduli di registrazione). Tuttavia, per l'eliminazione completa di tali dati è consigliabile utilizzare la Pulizia guidata dei dati riservati (vedere pagina 202).

Durante la pulizia del sistema, alcuni file (come file registro di Microsoft Windows, registri eventi di Microsoft Office) possono essere in uso da parte del sistema. Per eliminare tali file, la procedura guidata suggerisce di riavviare il sistema.

La procedura guidata è costituita da una serie di schermate (passaggi) tra le quali è possibile spostarsi servendosi dei pulsanti **Avanti** e **Indietro**. Per chiudere la procedura guidata al completamento, utilizzare il pulsante **Fine**. Per interrompere la procedura in qualsiasi momento, utilizzare il pulsante **Annulla**.

Per avviare la procedura guidata:

1. Aprire la finestra principale dell'applicazione.
2. Nella sezione **Protezione+** fare clic sul pulsante **Ottimizzazione del sistema**.
3. Nella finestra visualizzata, fare clic sul pulsante **Elimina dati inutilizzati**.

PULIZIA GUIDATA DEI DATI RISERVATI

Gran parte delle azioni dell'utente del computer viene registrata nel sistema. In questo caso vengono salvati i dati seguenti:

- Cronologie contenenti informazioni:
  - sui siti Web visitati;
  - sull'avvio delle applicazioni;
  - sulle richieste di ricerca;
  - sull'apertura o il salvataggio di file in applicazioni diverse.
- Record del log di sistema di Microsoft Windows.
- File temporanei e così via.

Tutte queste fonti di informazione sulle attività dell'utente possono contenere dati riservati, incluse le password, e possono diventare disponibili per gli intrusi che le analizzeranno. L'utente spesso non dispone di sufficienti conoscenze per evitare il furto di informazioni con questo metodo.

Kaspersky PURE include la **Pulizia guidata dei dati riservati**. 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.

La memorizzazione di informazioni sull'attività dell'utente nel sistema viene eseguita 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 **Pulizia guidata dei dati riservati** può rilevare tracce di attività non pulite durante la precedente esecuzione della procedura guidata. Alcuni file, ad esempio il file log di Microsoft Windows, possono essere utilizzati nel sistema mentre la procedura guidata cerca di eliminarli. Per eliminare tali file, la procedura guidata suggerisce di riavviare il sistema. Tuttavia, durante il riavvio tali file potrebbero essere ricreati e rilevati nuovamente come tracce di attività.

La procedura guidata è costituita da una serie di schermate (passaggi) tra le quali è possibile spostarsi servendosi dei pulsanti **Avanti** e **Indietro**. Per chiudere la procedura guidata al completamento, utilizzare il pulsante **Fine**. Per interrompere la procedura in qualsiasi momento, utilizzare il pulsante **Annulla**.

Per avviare la procedura guidata:

1. Aprire la finestra principale dell'applicazione.
2. Nella sezione **Protezione+** fare clic sul pulsante **Ottimizzazione del sistema**.
3. Nella finestra visualizzata fare clic sul pulsante **Eliminazione della cronologia delle attività**.

TASTIERA VIRTUALE

L'utilizzo del computer implica spesso situazioni in cui è necessario immettere i propri dati personali o il nome utente e la password, ad esempio quando si effettua una registrazione ai siti Web, quando si utilizzano negozi online e così via.

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.

La Tastiera virtuale previene l'intercettazione dei dati immessi tramite tastiera.

La Tastiera virtuale non può proteggere i dati riservati se il sito che richiede l'immissione di tali dati è stato hackerato; in tal caso, infatti, le informazioni verranno ottenute direttamente dagli intrusi.

Molte delle applicazioni classificate come spyware svolgono la funzione di creare screenshot che vengono quindi trasferiti a un intruso che li analizzerà per trafugare i dati personali dell'utente. La Tastiera virtuale previene l'intercettazione dei dati immessi tramite tastiera

ma solo quando si lavora con i browser Microsoft Internet Explorer e Mozilla Firefox.

- *Per utilizzare la Tastiera virtuale:*

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Tastiera virtuale**.

2. Immettere i dati richiesti premendo i tasti della tastiera virtuale. Verificare che i dati siano immessi nel campo corretto. Premendo i tasti funzione (**Maiusc**, **Alt**, **Ctrl**) della tastiera virtuale, verrà selezionata una determinata modalità (ad esempio, premendo **Maiusc** tutti i simboli verranno immessi in maiuscolo). Per uscire dalla modalità selezionata, premere nuovamente lo stesso tasto funzione.

È possibile cambiare la lingua per la tastiera virtuale utilizzando la combinazione di tasti **Ctrl** + clic destro su **Maiusc** oppure **Ctrl** + clic destro su **Alt di sinistra**, a seconda delle impostazioni selezionate.

CRITTOGRAFIA DEI DATI

Il modulo di crittografia dei dati è progettato per proteggere le informazioni personali dagli accessi non autorizzati. A tale scopo, le informazioni crittografate sono memorizzate in uno speciale contenitore.

Un *contenitore* è un oggetto crittografato creato dall'utente con il modulo di crittografia dei dati. File e cartelle vengono spostati nel contenitore. Per accedere ai dati memorizzati nel contenitore, è necessario immettere una password. È inoltre necessario che l'applicazione Kaspersky PURE sia installata nel computer.

Il contenitore deve essere connesso per poter utilizzare i dati. A tale scopo, il sistema richiede una password per l'accesso. Una volta connesso, il contenitore è visualizzato nel sistema come un'unità virtuale rimovibile in cui è possibile copiare o spostare file e cartelle di dati.

IN QUESTA SEZIONE:

Creazione di un contenitore 205

Connessione e disconnessione del contenitore 206

Aggiunta di file nel contenitore 207

Configurazione del contenitore 207

Creazione di un collegamento per l'accesso al contenitore 208

CREAZIONE DI UN CONTENITORE

Per memorizzare dati crittografati, è necessario creare un contenitore. È possibile creare un contenitore in un'unità locale o rimovibile.

Per la creazione del contenitore è disponibile una procedura guidata. Durante la creazione di un contenitore, è necessario specificare il nome, le dimensioni, la password di accesso e il percorso del file del contenitore.

La procedura guidata è costituita da una serie di schermate (passaggi) tra le quali è possibile spostarsi servendosi dei pulsanti **Avanti** e **Indietro**. Per chiudere la procedura guidata al completamento, utilizzare il pulsante **Fine**. Per interrompere la procedura in qualsiasi momento, utilizzare il pulsante **Annulla**.

È anche possibile spostarsi tra i passaggi della procedura guidata completati utilizzando i pulsanti di spostamento nella parte superiore della finestra.

È inoltre possibile specificare un contenitore esistente se non è disponibile nel computer in uso (ad esempio, dopo la reinstallazione del sistema operativo o se il contenitore viene copiato da un altro computer). In questo caso, il contenitore viene visualizzato nell'elenco ma rimane disattivato. Il contenitore deve essere connesso per poter utilizzare i dati (vedere la sezione "Connessione e disconnessione del contenitore" a pagina 206).

Per creare un contenitore, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul Pulsante **Crittografia dei dati**.
2. Nella finestra visualizzata, fare clic sul pulsante **Crea contenitore**.
3. Verrà avviata la Creazione guidata contenitore crittografato. I passaggi della procedura guidata sono descritti di seguito:
    a. Immettere il nome, le dimensioni e la password di accesso del contenitore nella finestra **Impostazioni principali**.

b. Specificare il percorso del file del contenitore nella finestra **Percorso**.

c. Selezionare la lettera di un'unità virtuale per connettere il contenitore, specificare le impostazioni avanzate, se necessario, e confermare la creazione del contenitore con le impostazioni specificate nella finestra **Riepilogo**.

Per specificare un contenitore esistente, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Crittografia dei dati**.
2. Nella finestra visualizzata, fare clic sul pulsante **Seleziona contenitore**.
3. Nella finestra visualizzata specificare il percorso del file del contenitore.

CONNESSIONE E DISCONNESSIONE DEL CONTENITORE

Una volta creato, un contenitore viene connesso automaticamente. Se si specifica un contenitore esistente, questo è disconnesso per importazione predefinita. È necessario connettere il contenitore per l'archiviazione dei dati. È possibile eseguire tale operazione tramite l'interfaccia di Kaspersky PURE o il menu di scelta rapida di Microsoft Windows.

Se il contenitore è memorizzato in un supporto rimovibile, è possibile configurare la connessione automatica del contenitore al momento della connessione del supporto.

Un contenitore connesso è disponibile per tutti gli account del computer come un'unità rimovibile nell'elenco dei dispositivi, pertanto è consigliabile disconnettere il contenitore quando non è necessario eseguire operazioni sui dati. È possibile eseguire tale operazione tramite l'interfaccia di Kaspersky PURE o il menu di scelta rapida di Microsoft Windows.

Per connettere un contenitore tramite l'interfaccia dell'applicazione, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Crittografia dei dati**.
2. Nella finestra visualizzata, fare clic sul pulsante **Connetti**.
3. Nella finestra visualizzata immettere le impostazioni di connessione del contenitore e confermare la connessione.

Per connettere un contenitore tramite il menu di scelta rapida, eseguire le operazioni seguenti:

1. Fare clic con il pulsante destro del mouse sull'icona del file del contenitore o il collegamento sul desktop per aprire il menu di scelta rapida (vedere la sezione "Creazione di un collegamento per l'accesso al contenitore" a pagina 208).
2. Scegliere **Connetti contenitore** dal menu visualizzato.

Per connettere automaticamente il contenitore al momento della connessione del supporto, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul Pulsante **Crittografia dei dati**.
2. Nella finestra visualizzata selezionare un contenitore connesso e fare clic sul pulsante **Configura**.
3. Nella finestra visualizzata selezionare la casella **Connetti automaticamente il contenitore**.

Per disconnettere un contenitore tramite l'interfaccia dell'applicazione, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Crittografia dei dati**.
2. Nella finestra visualizzata, fare clic sul pulsante **Disconnetti**.

- *Per disconnettere un contenitore tramite il menu di scelta rapida, eseguire le operazioni seguenti:*

1. Fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida di un file, di un collegamento sul desktop per l'accesso al contenitore (vedere la sezione "Creazione di un collegamento per l'accesso al contenitore208" a pagina), o di un'unità rimovibile.

2. Scegliere **Disconnetti contenitore** dal menu visualizzato.

AGGIUNTA DI FILE NEL CONTENITORE

Una volta connesso (vedere la sezione "Connessione e disconnessione del contenitore" a pagina 206),il contenitore viene visualizzato nel sistema come un'unità virtuale rimovibile ed è disponibile per tutti gli utenti del sistema operativo. È possibile aprire un contenitore e inserirvi file e cartelle se è necessario memorizzarli in formato crittografato.

Per assicurare la protezione dei dati, è consigliabile disattivare il contenitore al termine delle operazioni. Una volta disattivato il contenitore, è necessario immettere una password per ottenere l'accesso ai dati crittografati.

- *Per aprire un contenitore tramite l'interfaccia dell'applicazione:*

1. Aprire la finestra principaledell'applicazione e fare clic sul pulsante **Crittografia dei dati**.

2. Nella finestra visualizzata selezionare un contenitore connesso e aprirlo facendo doppio clic.

3. Inserire i dati che si desidera crittografare.

- *Per aprire un contenitore tramite il menu di scelta rapida, eseguire le operazioni seguenti:*

1. Fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida di un contenitore connesso o di un collegamento sul desktop per l'accesso al contenitore (vedere la sezione "Creazione di un collegamento per l'accesso al contenitore" a pagina 208).

2. Scegliere **Apri contenitore** dal menu visualizzato.

CONFIGURAZIONE DEL CONTENITORE

È possibile modificare il nome e la password di accesso del contenitore.

Le impostazioni possono essere modificate solo per un contenitore disconnesso.

- *Per rinominare un contenitore, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Crittografia dei dati**.

2. Nella finestra visualizzata selezionare un contenitore e fare clic sul pulsante **Configura**.

3. Nella finestra visualizzata immettere la password per ottenere l'accesso al contenitore.

4. Nella finestra **Impostazioni contenitore** visualizzata specificare il nuovo nome del contenitore.

- *Per cambiare la password per il contenitore, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione e fare clic sul Pulsante **Crittografia dei dati**.

2. Nella finestra visualizzata selezionare un contenitore e fare clic sul pulsante **Configura**.

3. Nella finestra visualizzata immettere la password per ottenere l'accesso al contenitore.

4. Nella finestra **Impostazioni contenitore** visualizzata fare clic sul collegamento **Cambia password**.

5. Nella finestra **Cambia password** visualizzata compilare tutti i campi.

CREAZIONE DI UN COLLEGAMENTO PER L'ACCESSO AL CONTENITORE

Per semplificare la gestione dei dati, è possibile creare un collegamento sul desktop per l'accesso al contenitore. Il collegamento può essere utilizzato per aprire, connettere e disconnettere velocemente il contenitore, indipendentemente dalla posizione effettiva del file del contenitore (se si dispone dell'accesso al file dal computer in uso).

È possibile creare un collegamento durante la creazione del contenitore o in qualsiasi momento dopo la creazione.

Per creare un collegamento per l'accesso al contenitore, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Crittografia dei dati**.
2. Nella finestra visualizzata selezionare un contenitore disconnesso e fare clic sul pulsante **Configura**.
3. Nella finestra visualizzata fare clic sul collegamento **Crea collegamento sul desktop**.

GESTIONE DELLE PASSWORD

Gestione delle password archivia e protegge tutti i dati personali, quali password, nomi utente, account di sistemi di messaggistica immediata, contatti, numeri di telefono e così via. Gestione delle password associa password e account alle applicazioni di Microsoft Windows e alle pagine Web in cui vengono utilizzati. Tutte le informazioni vengono archiviate in forma crittografata nel database delle password, il cui accesso è protetto da una password master. I dati personali sono facilmente accessibili quando il database delle password è sbloccato. All'apertura di una pagina Web o all'avvio di un'applicazione, Gestione delle password immette automaticamente la password, il nome utente e altri dati personali. In tal modo non è necessario ricordare tutte le password, ma è sufficiente ricordarne una sola.

Per impostazioni predefinita, Gestione delle password viene avviato insieme al computer. Poiché questo componente è incorporato nell'applicazione, i dati personali possono essere gestiti direttamente nella finestra dell'applicazione.

Gestione delle password controlla le azioni delle applicazioni con password e previene l'intercettazione e il furto di dati personali. Questo componente controlla le applicazioni che utilizzano password o le richiedono ad altre applicazioni prima di chiedere all'utente di consentire o negare un'azione sospetta.

Gestione delle password può inoltre:

- salvare e utilizzare le password (vedere pagina 221);
- trovare account, password, nomi utente e altre informazioni personali nel database delle password (vedere pagina 222);
- generare password sicure (vedere pagina 238) durante la registrazione di nuovi account;
- salvare tutte le password in dispositivi rimovibili;
- ripristinare il database delle password da una copia di backup (vedere pagina 224);
- proteggere le password dall'accesso non autorizzato (vedere pagina 213).

Per avviare Gestione delle password, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella sezione **Protezione+** fare clic su **Gestione delle password**.

IN QUESTA SEZIONE:

Interfaccia di Gestione delle password 210

Configurazione guidata 212

Gestione del database delle password 213

Configurazione delle impostazioni dell'applicazione 225

Funzioni avanzate 238

INTERFACCIA DI GESTIONE DELLE PASSWORD

L'interfaccia di Gestione delle password è semplice e pratica. In questa sezione verranno descritti più in dettaglio i concetti relativi all'utilizzo dell'applicazione.

Gestione delle password dispone di plug-in incorporati nelle applicazioni che richiedono l'autorizzazione. È possibile installare i plug-in in modo indipendente per i browser desiderati. I plug-in installati consentono di accedere alle funzioni di Gestione delle password dall'interfaccia dell'applicazione o del browser.

È possibile utilizzare il puntatore di Gestione delle password per selezionare velocemente un'applicazione o una pagina Web per l'immissione automatica dei dati personali.

IN QUESTA SEZIONE:

Icona dell'area di notifica 210

Menu di scelta rapida di Gestione delle password 210

Finestra di Gestione delle password 211

Finestra delle impostazioni dell'applicazione 211

Pulsante Titolo 212

ICONA DELL'AREA DI NOTIFICA

Subito dopo aver installato Gestione delle password, la relativa icona viene visualizzata nell'area di notifica della barra delle applicazioni di Microsoft Windows.

A seconda della situazione, l'icona di Gestione delle password può assumere il seguente aspetto:

- attiva (verde) – Gestione delle password sbloccato, accesso ai dati personali consentito;
- inattiva (rosso) – Gestione delle password bloccato, accesso ai dati personali non consentito.

Inoltre, facendo clic sull'icona sono accessibili i seguenti elementi di interfaccia:

- menu di scelta rapida (vedere pagina 210);
- finestra principale dell'applicazione (vedere pagina 211);
- puntatore di Gestione delle password (vedere pagina 239).

È possibile aprire il menu di scelta rapida facendo clic con il pulsante destro del mouse sull'icona di Gestione delle password.

Facendo doppio clic sull'icona di Gestione delle password, è possibile bloccare o sbloccare l'applicazione.

Per utilizzare il puntatore di Gestione delle password, posizionare il puntatore del mouse sull'icona dell'applicazione e attendere alcuni secondi. Il puntatore di Gestione delle password verrà visualizzato sopra l'icona dell'applicazione.

MENU DI SCELTA RAPIDA DI GESTIONE DELLE PASSWORD

Le attività principali dell'applicazione sono accessibili dal menu di scelta rapida di Gestione delle password. Il menu di Gestione delle password contiene i seguenti elementi:

- **Blocca / Sblocca** – consentire o impedire l'accesso ai dati personali.
- Elenco degli account utilizzati di frequente – avviare velocemente uno degli account utilizzati di frequente. L'elenco viene generato automaticamente in base alla frequenza di utilizzo degli account. L'elenco è disponibile se è configurato per la visualizzazione nel menu di scelta rapida (vedere pagina 226). Al primo avvio dell'applicazione, l'elenco non è disponibile perché non è ancora stato utilizzato alcun account.
- **Account** – visualizzare un elenco di tutti gli account e avviarne rapidamente uno. Il numero di account nel database delle password è specificato tra parentesi quadre.
- **Aggiungi account** – aggiungere un nuovo account a Gestione delle password.
- **Gestione delle password** – passare alla finestra principale dell'applicazione (vedere pagina 211).
- **Impostazioni** – configurare le impostazioni dell'applicazione.
- **Generatore di password** – creare password.
- **Guida** – aprire la documentazione sull'applicazione.
- **Esci** – chiudere l'applicazione. Quando è selezionata questa opzione, l'applicazione viene scaricata dalla RAM del computer.

Se l'applicazione è bloccata, l'accesso ai dati personali non è consentito. In questo caso, il menu di scelta rapida conterrà solo i seguenti elementi: **Sblocca**, **Generatore di password**, **Guida** ed **Esci**.

FINESTRA DI GESTIONE DELLE PASSWORD

È possibile aprire la finestra principale dell'applicazione dal menu di scelta rapida di Gestione delle password (vedere pagina 210). A tale scopo, selezionare **Gestione delle password** dal menu di scelta rapida.

È inoltre possibile avviare la finestra principale di Gestione delle password facendo doppio clic sull'icona di Gestione delle password nell'area di notifica della barra delle applicazioni.

La finestra di **Gestione delle password** può essere suddivisa in due parti:

- nella parte superiore della finestra è possibile selezionare le funzioni di Gestione delle password ed eseguire le attività principali;
- la parte inferiore della finestra contiene un elenco di tutti gli account e altre informazioni personali e consente di gestire le informazioni personali.

È possibile utilizzare il campo di ricerca per eseguire ricerche di dati personali nel database delle password. Il campo di ricerca è disponibile nella parte inferiore della finestra principale dell'applicazione.

FINESTRA DELLE IMPOSTAZIONI DELL'APPLICAZIONE

La finestra delle impostazioni di Gestione delle password può essere aperta in uno dei seguenti modi:

- dal menu di scelta rapida di Gestione delle password (vedere pagina 210) – a tale scopo, selezionare la voce **Impostazioni** dal menu di scelta rapida di Gestione delle password;
- dalla finestra di Kaspersky PURE **–** nella sezione **Protezione+** fare clic su **Gestione delle password**.

La finestra delle impostazioni si compone di due parti:

- la parte sinistra della finestra contiene l'elenco delle funzioni dell'applicazione;
- la parte destra della finestra contiene l'elenco delle impostazioni per la funzione o l'attività selezionata.

PULSANTE TITOLO

Il pulsante Titolo consente di utilizzare i dati personali dalla finestra dell'applicazione o del browser. Questo pulsante visualizzato è nell'angolo superiore destro dell'applicazione.

Il pulsante Titolo è attivo se Gestione delle password non è bloccato. Facendo clic su di esso, è possibile eseguire le operazioni seguenti:

- **Aggiungi account** – aggiungere un nuovo account.
- **Gestisci account** – aggiungere un nome utente o modificare l'account attivato. Il comando è disponibile se l'account è attivato.
- **Account Web** – visualizzare l'elenco di tutti gli account Web e aprirne uno. Il numero di account nel database delle password è specificato tra parentesi quadre.
- Elenco degli account utilizzati di frequente – avviare un account dall'elenco. L'elenco viene generato automaticamente in base alla frequenza di utilizzo degli account. L'elenco è disponibile nel menu se è configurato per la visualizzazione (vedere pagina 226).
- **Identità** – visualizzare l'elenco delle identità create e selezionare un'identità per il modulo di registrazione.
- **Guida** – passare alla sezione della documentazione sull'applicazione.

Il pulsante Titolo non è attivo se Gestione delle password è bloccato. In tal caso, facendo clic sul pulsante non sarà possibile eseguire alcuna operazione. Il pulsante inattivo viene visualizzato nella finestra dell'applicazione se sono state configurate le impostazioni aggiuntive del pulsante Titolo (vedere pagina 237).

CONFIGURAZIONE GUIDATA

La Configurazione guidata dell'applicazione viene eseguita quando si avvia Gestione delle password per la prima volta. Il suo obiettivo è aiutare l'utente a eseguire la configurazione iniziale di Gestione delle password in base alle proprie preferenze e attività.

La procedura guidata è visualizzata come una sequenza di finestre (passaggi). È possibile spostarsi tra i vari passaggi facendo clic su **Avanti** e **Indietro** in base alle esigenze. Per chiudere la procedura guidata durante qualsiasi passaggio, fare clic su **Esci**. Per completare la procedura guidata, fare clic su **Fine**. Verranno ora illustrati più in dettaglio i passaggi della procedura guidata.

GESTIONE DEL DATABASE DELLE PASSWORD

Nel database delle password sono memorizzati tutti gli account per le applicazioni e le pagine Web con uno o più nomi utente, oltre che identità (schede contenenti, ad esempio, dettagli sui contatti, numeri di telefono, numeri di sistemi di messaggistica immediata e così via).

È possibile utilizzare il database delle password se è sbloccato (vedere pagina 213). Prima di immettere modifiche nel database delle password, è consigliabile configurare il Backup del database delle password (vedere pagina 230). Se tali dati vengono accidentalmente modificati o eliminati, utilizzare il Ripristino del database delle password (vedere pagina 224).

È possibile eseguire le operazioni seguenti:

- aggiunta (vedere pagina 214), modifica (vedere pagina 220), eliminazione (vedere pagina 222) di dati personali;
- importazione / esportazione (vedere pagina 222), ripristino (vedere pagina 224) del database delle password.

IN QUESTA SEZIONE:

Accesso al database delle password 213

Aggiunta di dati personali 214

Modifica di dati personali 220

Utilizzo di dati personali 221

Ricerca di password 222

Eliminazione di dati personali 222

Importazione ed esportazione di password 222

Backup e ripristino del database delle password 224

ACCESSO AL DATABASE DELLE PASSWORD

Tutti i dati personali vengono archiviati in forma crittografata nel database delle password. Per utilizzare tali dati, il database delle password deve essere sbloccato. Per accedere al database delle password, selezionare uno dei metodi di autorizzazione:

- **Protezione della password master**. La password master viene utilizzata per accedere al database delle password.
- **Dispositivo USB**. Per accedere al database delle password, connettere un dispositivo USB al computer. Quando il dispositivo USB è disabilitato, il database delle password viene bloccato automaticamente.
- **Dispositivo Bluetooth**. Per accedere al database delle password, connettere un dispositivo Bluetooth al computer. Quando il dispositivo Bluetooth è disabilitato, il database delle password viene bloccato automaticamente.
- **Nessuna autorizzazione**. L'accesso al database delle password non è protetto.

Per impostazione predefinita, la protezione viene attivata dalla password master, pertanto è sufficiente ricordare una sola password.

La password master è lo strumento di base per la protezione dei dati personali. Se è stato selezionato il metodo di autorizzazione con un dispositivo e quest'ultimo è divenuto inutilizzabile o è andato perso, sarà possibile accedere ai dati personali utilizzando la password master.

Per impostazione predefinita, Gestione delle password blocca il database delle password quando l'applicazione viene avviata e dopo un tempo specificato (vedere pagina 232) di inutilizzo del computer. L'applicazione può essere utilizzata solo se il database delle password è sbloccato.

È inoltre possibile sbloccare/bloccare il database delle password in uno dei modi seguenti:

- utilizzando un dispositivo USB o Bluetooth - solo per autorizzazioni tramite dispositivo USB o Bluetooth;
- facendo doppio clic sull'icona dell'applicazione (vedere pagina 235) - l'azione doppio clic in questo caso richiede una configurazione aggiuntiva;
- dal menu di scelta rapida di Gestione delle password;
- utilizzando la combinazione di tasti CTRL+ALT+L (vedere pagina 228).

Per immettere la password master, utilizzare una tastiera virtuale che consente l'immissione delle password senza premere i tasti della tastiera.

Per bloccare un'applicazione dal menu di scelta rapida dell'applicazione, eseguire le operazioni seguenti:

1. Fare clic con il pulsante destro del mouse sull'icona di Gestione delle password nell'area di notifica della barra delle applicazioni.
2. Nel menu visualizzato, selezionare la voce **Blocca**.

Per sbloccare il database delle password dal menu di scelta rapida, eseguire le operazioni seguenti:

1. Fare clic con il pulsante destro del mouse sull'icona di Gestione delle password nell'area di notifica della barra delle applicazioni.
2. Nel menu visualizzato, selezionare **Sblocca**.
3. Immettere la password master nella finestra visualizzata.

AGGIUNTA DI DATI PERSONALI

È possibile aggiungere dati personali se il database delle password non è bloccato (vedere pagina 213). Quando si avvia un'applicazione o una pagina Web, un nuovo account viene riconosciuto automaticamente se non è stato individuato nel database delle password. In seguito all'autorizzazione nell'applicazione o nella pagina Web, Gestione delle password può aggiungere i dati personali al database delle password.

È possibile aggiungere i seguenti dati personali al database delle password:

- **Account** (vedere pagina 215).
- **Nome utente** (vedere pagina 219). Per impostazione predefinita, gestione delle password offre la possibilità di creare un account con un solo nome utente. Un ulteriore nome utente viene utilizzato quando le applicazioni o le pagine Web consentono la creazione di diversi nomi utente per l'accesso alle risorse.
- **Identità** (vedere pagina 219). Utilizzata per memorizzare dati come sesso, data di nascita, informazioni di contatto, numeri di telefono, luogo di lavoro, numeri di sistemi di messaggistica immediata, indirizzi di homepage e così via. Per separare le informazioni personali e lavorative, è possibile creare diverse schede di identità.
- **Gruppi di account** (vedere pagina 220). Utilizzati per organizzare gli account nel database delle password.

ACCOUNT.

Gestione delle password riconosce automaticamente un nuovo account se questo non viene individuato nel database delle password. Dopo l'autorizzazione nell'applicazione o nella pagina Web, Gestione delle password offre la possibilità di salvare i dati nel database delle password. È anche possibile aggiungere manualmente un nuovo account al database delle password.

Un account contiene i seguenti dati:

- uno o più nomi utente;
- password;
- percorso dell'applicazione / indirizzo Internet della pagina Web;
- impostazioni che definiscono le relazioni tra l'account e l'oggetto;
- impostazioni che definiscono come viene attivato l'account;
- commenti;
- impostazioni per la compilazione di ulteriori campi della pagina Web.

Gestione delle password consente di utilizzare uno o più account per le applicazioni o i siti Web. In base al percorso dell'applicazione o all'indirizzo Internet della pagina Web, Gestione delle password consente di specificare un ambito per ciascun account.

È possibile aggiungere un account in diversi modi:

- facendo clic sul pulsante Titolo – a tale scopo, è necessario selezionare **Aggiungi account** nel menu del pulsante Titolo;
- dal menu di scelta rapida di Gestione delle password – a tale scopo, è necessario selezionare **Aggiungi account** nel menu di scelta rapida di Gestione delle password;
- dalla finestra principale di Gestione delle password.

Per aggiungere un nuovo account:

1. Nel menu di scelta rapida dell'applicazione selezionare **Gestione delle password**.
2. Nella finestra **Gestione delle password** visualizzata fare clic su **Aggiungi account**.
3. Nella finestra visualizzata, nel campo **Nome**, immettere il nome del nuovo account, ad esempio il nome dell'applicazione o della pagina Web.
4. Nella scheda **Informazioni di accesso** immettere il nome utente e la password.

   Il nome utente può essere formato da una o più parole. Per specificare parole chiave (vedere pagina 216) per il nome utente, fare clic su .

   Per copiare un nome utente o una password negli Appunti, fare clic su .

   Per creare automaticamente una password, fare clic sul collegamento **Genera password**.
5. Nella scheda **Collegamenti** specificare il percorso del programma o della pagina Web, quindi specificare le impostazioni dell'account.
6. Nella scheda **Modifica manuale modulo** modificare le impostazioni per la compilazione di altri campi della pagina Web, se necessario.

7. Se necessario, nella scheda **Commenti** immettere un testo descrittivo per l'account. Per visualizzare i commenti in una notifica dopo l'attivazione dell'account, selezionare la casella **Mostra commenti nella notifica**.

RICERCA PER PAROLE CHIAVE

Per cercare velocemente i dati personali nel database delle password, è possibile utilizzare parole chiave. Le parole chiave vengono generate per ogni nome utente. È consigliabile assegnare parole chiave quando si aggiunge un account (vedere pagina 215) o un nome utente (vedere pagina 219).

Per specificare parole chiave per un nome utente, eseguire le operazioni seguenti:

1. Nel menu di scelta rapida dell'applicazione selezionare **Gestione delle password**.
2. Nella scheda **Modifica** della finestra **Gestione delle password** selezionare il nome utente dall'**elenco Password**, quindi aprirlo facendo clic su **Modifica**.
3. Nella finestra visualizzata fare clic su accanto al campo **Nome di accesso** e compilare il campo **Descrizione**.

   Se è stato selezionato un account con un unico nome utente, nella scheda **Informazioni di accesso** della finestra **Account con singolo nome di accesso**, fare clic su .

AGGIUNTA DEL PERCORSO DI UN PROGRAMMA O DI UNA PAGINA WEB

I dati personali dell'account verranno immessi automaticamente nei campi di autorizzazione della pagina Web o del programma. Per definire un'applicazione o una pagina Web viene utilizzato un collegamento. Per una pagina Web è l'indirizzo, mentre per un programma è il percorso del file eseguibile dell'applicazione nel computer. Senza questa informazione non sarà possibile associare l'account all'applicazione o alla pagina Web.

È possibile associare l'account a un programma o una pagina Web nei seguenti modi:

- facendo clic sul collegamento nell'elenco dei siti Web visitati del browser o nell'elenco delle applicazioni nel computer;
- specificando manualmente il percorso dell'applicazione o della pagina Web;
- utilizzando il puntatore di Gestione delle password.

Per controllare il percorso immesso, avviare l'applicazione o la pagina Web facendo clic su .

Per selezionare un collegamento per l'account, eseguire le operazioni seguenti:

1. Nel menu di scelta rapida dell'applicazione selezionare **Gestione delle password**.
2. Nella finestra **Gestione delle password** visualizzata fare clic su **Aggiungi account**.
3. Nella finestra visualizzata, nel campo **Collegamento** della scheda **Collegamenti**, fare clic su .
4. Nella finestra visualizzata, nel campo **Collegamento,** immettere il percorso dell'applicazione o della pagina Web.

   Per specificare una pagina Web dall'elenco di pagine Web memorizzate (Preferiti), nell'elenco **Schede**, selezionare una pagina Web, quindi fare clic sul collegamento **Copia collegamento da Preferiti**. Per copiare il percorso della pagina Web dalla finestra del browser, fare clic sul collegamento **Usa il percorso dell'applicazione collegata**.

   Per selezionare un collegamento per l'applicazione, nel campo **Collegamento**, specificare il percorso sul computer facendo clic su .

- *Per specificare manualmente il percorso del programma o della pagina Web, eseguire le operazioni seguenti:*

  1. Nel menu di scelta rapida dell'applicazione selezionare **Gestione delle password**.
  2. Nella finestra **Gestione delle password** visualizzata fare clic su **Aggiungi account**.
  3. Nella finestra visualizzata, nel campo **Collegamento** della scheda **Collegamenti**, immettere il percorso del programma o l'indirizzo della pagina Web. L'indirizzo della pagina Web deve iniziare con http://www.

- *Per immettere il percorso del programma o della pagina Web utilizzando il puntatore di Gestione delle password, eseguire le operazioni seguenti:*

  1. Nel menu di scelta rapida dell'applicazione selezionare **Gestione delle password**.
  2. Nella finestra **Gestione delle password** visualizzata fare clic su **Aggiungi account**.
  3. Nella finestra visualizzata, nel campo **Collegamento** della scheda **Collegamenti**, immettere il percorso del programma o della pagina Web spostando il puntatore di Gestione delle password sulla finestra del programma o del browser.

SELEZIONARE UN METODO PER ASSOCIARE L'ACCOUNT

Per determinare i dati dell'account da immettere automaticamente a ogni avvio dell'applicazione o della pagina Web, Gestione delle password utilizza il percorso dell'applicazione o l'indirizzo Internet della pagina Web.

Dal momento che Gestione delle password consente di utilizzare diversi account per un'applicazione o un sito Web, è necessario specificare un ambito per ogni account.

In base al percorso dell'applicazione o all'indirizzo Internet della pagina Web, Gestione delle password consente di creare un ambito per qualsiasi account. L'ambito può essere configurato durante la creazione dell'account (vedere pagina 215). È possibile modificare le impostazioni in un secondo momento.

La modalità di utilizzo degli account varia a seconda dell'oggetto (applicazione o sito Web).

Per le applicazioni sono disponibili le seguenti opzioni:

- Utilizzo dell'account per l'applicazione. L'account verrà utilizzato per tutte le finestre di dialogo dell'applicazione che dispongono di campi per l'immissione di dati personali.
- Riconoscimento in base all'intestazione della finestra. L'account verrà utilizzato solo per la finestra dell'applicazione specificata.

  Ad esempio, una singola applicazione può utilizzare più account. Per differenti account, solo le intestazioni delle finestre varieranno all'interno di una singola applicazione. I dati per l'account verranno immessi automaticamente da Gestione delle password in base all'intestazione della finestra dell'applicazione.

Per l'utilizzo di un account per le pagine Web sono disponibili le seguenti opzioni:

- Solo per la pagina Web specificata. Gestione delle password aggiunge automaticamente il nome utente e la password solo nei campi di identificazione della pagina Web specificata.

  Ad esempio, se l'account è associato a una pagina Web all'indirizzo http://www.sito-web.com/login.html, non sarà valido per altri siti Web, come ad esempio http://www.sito-web.com/pointer.php.

- Per i siti Web di una directory. Gestione delle password aggiunge automaticamente il nome utente e la password nei campi di identificazione di tutte le pagine Web nella cartella più recente.

  Se ad esempio è stato immesso l'indirizzo del sito Web http://www.sito-web.com/cgi-bin/login.html, l'account verrà utilizzato per le pagine Web nella cartella *cgi-bin*.

- Per il sito Web: <nome di dominio di terzo livello e inferiore>. L'account viene utilizzato per qualsiasi pagina Web nel dominio (dominio di terzo livello e inferiore).

Ad esempio, Gestione delle password aggiunge automaticamente i dati relativi all'identità per i siti Web http://www.dominio1.dominio2.sito-web.com/login.html o http://www.dominio1.dominio2.sito-web.com/pointer.php. Tuttavia, l'account non verrà utilizzato per le pagine Web con indirizzi con differenti domini di quarto livello: http://www.dominio3.dominio2.sito-web.com/pointer.php o http://www.dominio4.dominio2.sito-web.com/pointer.php.

- Per il sito Web: <nome del sito Web>. L'account verrà utilizzato per tutte le pagine Web con campi per l'immissione di nomi utente e password.

  Ad esempio, Gestione delle password aggiunge automaticamente schede di identità per le pagine Web: http://www.dominio1.dominio2.sito-web.com/login.html, http://www.dominio2.dominio2.sito-web.com/pointer.php, http://www.dominio3.dominio2.sito-web.com/pointer.php o http://www.dominio4.dominio2.sito-web.com/pointer.php.

Per impostare parametri per l'utilizzo di un account, eseguire le operazioni seguenti:

1. Nel menu di scelta rapida dell'applicazione selezionare **Gestione delle password**.
2. Nella scheda **Modifica** della finestra **Gestione delle password** selezionare l'account dall'elenco **Password**, quindi aprirlo facendo clic su **Modifica**.
3. Nella finestra visualizzata, nella scheda **Collegamenti**, selezionare una delle opzioni per l'utilizzo dell'account.

ATTIVAZIONE AUTOMATICA DELL'ACCOUNT

Per impostazione predefinita, l'attivazione automatica dell'account è abilitata. Gestione delle password immette solo il nome utente e la password nei campi di identificazione. È possibile modificare le impostazioni avanzate per l'attivazione dell'account (vedere pagina 215).

Per la pagina Web viene inoltre specificato un intervallo di indirizzi Web per cui viene utilizzata l'attivazione automatica.

Per l'attivazione dell'account sono disponibili le seguenti opzioni:

- Per la pagina Web selezionata. L'account viene attivato solo per la pagina Web specificata.
- Per il sito Web. L'account viene attivato per tutte le pagine Web del sito Web.

Per impostare l'attivazione automatica dell'account, eseguire le operazioni seguenti:

1. Nel menu di scelta rapida dell'applicazione selezionare **Gestione delle password**.
2. Nella scheda **Modifica** della finestra **Gestione delle password** selezionare l'account dall'elenco **Password**, quindi aprirlo facendo clic su **Modifica**.
3. Nella finestra visualizzata, nella scheda **Collegamenti**, selezionare la casella di controllo **Attiva automaticamente l'account dopo il caricamento**.

   Specificare inoltre uno dei metodi per l'attivazione dell'account per la pagina Web.

COMPILAZIONE DI CAMPI AGGIUNTIVI

Durante l'autorizzazione in un sito Web, spesso sono necessari altri dati oltre alla password e al nome utente. Gestione delle password può compilare automaticamente i campi aggiuntivi. È possibile impostare opzioni per la compilazione automatica dei campi aggiuntivi per l'account.

Le opzioni per i campi aggiuntivi possono essere impostate se è specificato il percorso dell'applicazione o l'indirizzo del sito Web.

Per impostare le opzioni per i campi, Gestione delle password carica temporaneamente il sito Web e analizza tutti i campi e i pulsanti. Campi e pulsanti vengono uniti in gruppi per ogni pagina Web.

Gestione delle password salva temporaneamente file e immagini nel computer dalla pagina Web caricata.

Per impostare le opzioni per i campi aggiuntivi, eseguire le operazioni seguenti:

1. Nel menu di scelta rapida dell'applicazione selezionare **Gestione delle password**.
2. Nella scheda **Modifica** della finestra **Gestione delle password** selezionare l'account dall'elenco **Password**, quindi aprirlo facendo clic su **Modifica**.
3. Nella finestra visualizzata, nella scheda **Modifica manuale modulo**, fare clic sul collegamento **Modifica campi modulo**.
4. Nella finestra **Modifica manuale modulo** visualizzata selezionare la casella accanto al campo o al pulsante desiderato.
5. Attivare il campo **Valore** per il campo o il pulsante scelto facendo doppio clic con il mouse e quindi impostando i valori per il campo.

   Per tornare all'elenco di tutti i campi o i pulsanti, fare clic su **Modifica campo**. Per eliminare un valore, fare clic su **Elimina**. Per modificare nuovamente un valore del campo o del pulsante, fare clic su **Modifica**.

NOME UTENTE.

Spesso si utilizzano diversi nomi utente per particolari applicazioni o siti Web. Gestione delle password consente di salvare più nomi utente per un solo account. Gestione delle password riconosce automaticamente un nome utente quando viene utilizzato per la prima volta e offre la possibilità di aggiungerlo a un account per un'applicazione o un sito Web. È possibile aggiungere manualmente un nuovo nome utente per un account, quindi modificarlo (vedere pagina 220).

È possibile aggiungere un nuovo nome utente per un account nei seguenti modi:

- Facendo clic sul pulsante Titolo. A tale scopo, nel menu del pulsante Titolo selezionare **Gestisci account** → **Aggiungi nome di accesso**.
- Dalla .

Per aggiungere un nome utente per un account, eseguire le operazioni seguenti:

1. Nel menu di scelta rapida dell'applicazione selezionare **Gestione delle password**.
2. Nella finestra **Gestione delle password** visualizzata, nella scheda **Modifica**, selezionare l'account dall'elenco **Password**, quindi fare clic su **Aggiungi nome di accesso**.
3. Nella finestra visualizzata immettere il nome utente e la password. Il nome utente può essere formato da una o più parole. Per specificare parole chiave per un nome utente, fare clic su e quindi compilare il campo **Descrizione**.

   Per copiare un nome utente o una password negli Appunti, fare clic su . Per creare automaticamente una password, fare clic sul collegamento **Genera password** (vedere pagina 238).

IDENTITÀ

Oltre al nome utente e alla password, altri dati personali vengono spesso utilizzati per la registrazione ai siti Web, ad esempio nome e cognome, anno di nascita, sesso, indirizzo e-mail, numero di telefono, paese di residenza e così via. Gestione delle password può memorizzare tutti questi dati in un database delle password crittografato in forma di identità. Durante la registrazione in un nuovo sito Web, Gestione delle password compilerà il modulo di registrazione utilizzando i dati di un'identità selezionata. Per salvare le informazioni personali e professionali separatamente, è possibile utilizzare diverse schede di identità. È possibile modificare i parametri delle identità in un secondo momento (vedere pagina 220).

Per creare una scheda di identità, eseguire le operazioni seguenti:

1. Nel menu di scelta rapida dell'applicazione selezionare **Gestione delle password**.
2. Nella finestra **Gestione delle password**, nella scheda **Modifica**, fare clic su **Aggiungi identità**.
3. Nella finestra visualizzata, nel campo **Nome**, immettere il nome dell'identità.
4. Immettere i valori per i campi desiderati e attivarlo facendo doppio clic con il mouse.

GRUPPI DI ACCOUNT

L'utilizzo di gruppi di account aiuta a organizzare le informazioni nel database delle password. Un gruppo è formato da una cartella e dagli account aggiunti ad essa.

I gruppi creati più di recente sono visualizzati nel menu di scelta rapida di Gestione delle password, in **Account** → **<Nome gruppo>**.

Per creare un gruppo di account, eseguire le operazioni seguenti:

1. Nel menu di scelta rapida dell'applicazione selezionare **Gestione delle password**.
2. Nella finestra **Gestione delle password**, nella scheda **Modifica**, fare clic su **Aggiungi gruppo**.
3. Immettere il nome della cartella creata.
4. Aggiungere account dall'elenco **Password** trascinandole nella cartella creata.

MODIFICA DI DATI PERSONALI

Nel database delle password è possibile modificare qualsiasi dato personale: account, nome utente, scheda di identità o gruppo di account. Durante la modifica delle impostazioni di ciascun elemento, è possibile eseguire le operazioni seguenti:

- Per l'account:
  - modificare il nome dell'account, il valore del nome utente e la password, se l'account dispone di un solo nome utente;
  - modificare il percorso dell'applicazione o della pagina Web che utilizza l'account;
  - selezionare le regole per l'utilizzo dell'account;
  - impostare l'attivazione automatica;
  - modificare ulteriori campi dell'account;
  - modificare i commenti per l'account.
- Per il nome utente – modificare il valore del nome utente e la password.
- Per l'identità – modificare il nome dell'identità e il valore dei campi desiderati.
- Per il gruppo di account – modificare il nome e l'icona del gruppo.

Poiché Gestione delle password è incorporato nelle finestre delle applicazioni e delle pagine Web per cui viene utilizzato, è possibile modificare le impostazioni di account o nomi utente direttamente dalla finestra dell'applicazione o del browser.

È possibile modificare le impostazioni dell'account o del nome utente nei seguenti modi:

- Dal . A tale scopo, aprire il menu di scelta rapida dell'applicazione, quindi selezionare **Account** → **<Nome gruppo di account>** → **<Nome account>** → **Modifica account**.
- Dalla .
- Facendo clic sul pulsante Titolo. A tale scopo, aprire il menu del pulsante Titolo, quindi selezionare **Gestisci account** → **Modifica account**.

Per modificare i parametri e i valori dei campi di un elemento dalla finestra principale, eseguire le operazioni seguenti:

1. Nel menu di scelta rapida dell'applicazione selezionare **Gestione delle password**.
2. Nella finestra **Gestione delle password**, nella scheda **Modifica**, selezionare l'elemento dall'elenco **Password**.
3. Nella finestra visualizzata modificare le impostazioni per l'elemento.

UTILIZZO DI DATI PERSONALI

Gestione delle password associa gli account alle applicazioni/pagine Web in cui vengono utilizzati. Il database delle password cerca automaticamente gli account associati all'avvio delle applicazioni/pagine Web. Se viene trovato un account, i dati personali vengono immessi automaticamente. Se nel database delle password non viene trovato alcun account associato, Gestione delle password suggerisce automaticamente l'aggiunta di un account al database delle password (vedere pagina 215).

Alcune applicazioni/siti Web possono utilizzare più nomi utente. Gestione delle password consente di salvare più nomi utente per lo stesso account. Se durante l'autorizzazione viene utilizzato un nuovo nome utente, Gestione delle password ne suggerirà l'aggiunta all'account (vedere pagina 219) dell'applicazione/pagina Web aperta. Quando l'applicazione/pagina Web viene aperta di nuovo, accanto ai campi di input dei dati personali verrà visualizzata una finestra con l'elenco dei nomi utente correlati all'account.

Oltre al nome utente e alla password, altri dati personali vengono spesso utilizzati nel sito Web per la registrazione. Tra questi vi sono, ad esempio, nome completo, sesso, paese, città, numero di telefono, indirizzo di posta elettronica e così via. Gestione delle password può archiviare tali dati in un database delle password crittografato sotto forma di identità. Per separare le informazioni private da quelle aziendali, è possibile creare più identità (vedere pagina 219). Quando si esegue la registrazione al programma/sito Web, Gestione delle password utilizzerà automaticamente la scheda selezionata per compilare il modulo di registrazione. L'utilizzo delle identità velocizza la compilazione di moduli di registrazione identici.

Durante l'autorizzazione nell'applicazione/pagina Web, Gestione delle password immette automaticamente i dati personali solo se il database delle password è sbloccato.

Un account può essere utilizzato nei modi seguenti:

- Avviare l'applicazione/pagina Web. Il modulo di autorizzazione verrà compilato automaticamente utilizzando i dati dell'account.
- Utilizzare il puntatore di Gestione delle password. A tale scopo, spostare il cursore del mouse sull'icona dell'applicazione nell'area di notifica della barra delle applicazioni, quindi attivare l'account trascinando il puntatore di Gestione delle password sulla finestra dell'applicazione o del browser desiderata.
- Selezionare l'account dall'elenco degli account utilizzati di frequente. A tale scopo, aprire il menu di scelta rapida di Gestione delle password e selezionare il record desiderato tra gli account utilizzati di frequente.
- Utilizzare il menu di scelta rapida di Gestione delle password. A tale scopo, aprire il menu di scelta rapida di Gestione delle password e selezionare la voce **Account** → **<nome account>**.

Per utilizzare un'identità, eseguire le operazioni seguenti:

1. Fare clic sul pulsante Titolo nell'angolo superiore destro della finestra dell'applicazione o del browser.

2. Nel menu visualizzato, selezionare la voce **Identità** → **<nome identità>**. Gestione delle password compila automaticamente i campi di registrazione della pagina Web utilizzando i dati dell'identità.

RICERCA DI PASSWORD

La ricerca dei dati personali potrebbe essere ostacolata nei casi seguenti:

- Alcune password non sono associate ad applicazioni o siti Web.
- Il database delle password contiene un numero elevato di account.

Gestione delle password trova rapidamente le password in base ai parametri seguenti:

- nome account;
- nome utente;
- parole chiave (vedere pagina 216) (per ogni nome utente vengono anche impostati parametri di ricerca basati su parole chiave);
- indirizzo Web (per gli indirizzi Web).

La ricerca viene eseguita per nome completo, per lettere iniziali e per ogni carattere incluso nel collegamento o nel nome account.

Per trovare un account/password, eseguire le operazioni seguenti:

1. Nel menu di scelta rapida dell'applicazione selezionare **Gestione delle password**.
2. Immettere il testo nel campo di ricerca della finestra **Gestione delle password** visualizzata.

   Per visualizzare i dati dell'account per il quale è stata immessa la password, premere **INVIO**.

ELIMINAZIONE DI DATI PERSONALI

Prima di apportare qualsiasi modifica ai dati personali, Gestione delle password crea automaticamente una copia di backup del database delle password. Se tali dati vengono accidentalmente modificati o eliminati, utilizzare il Ripristino del database delle password (vedere pagina 224). È possibile eliminare uno o più elementi dal database delle password.

Per eliminare un elemento dal database delle password, eseguire le operazioni seguenti:

1. Nel menu di scelta rapida dell'applicazione selezionare **Gestione delle password**.
2. Nella finestra **Gestione delle password**, nella scheda **Modifica**, selezionare l'elemento dall'elenco **Password**, quindi fare clic su **Elimina** o premere **CANC**.

Per eliminare tutti gli elementi dal database delle password, eseguire le operazioni seguenti:

1. Nel menu di scelta rapida dell'applicazione selezionare **Gestione delle password**.
2. Nella finestra **Gestione delle password**, nella scheda **Modifica**, fare clic su **Elimina tutto**.

IMPORTAZIONE ED ESPORTAZIONE DI PASSWORD

Gestione delle password consente di importare ed esportare le password.

L'applicazione consente l'aggiunta di password da database delle password non protetti (non crittografati). È possibile importare sia password da altre applicazioni di gestione delle password (ad esempio, password di Internet Explorer,

Mozilla Firefox, KeePass) che password esportate in precedenza da Gestione delle password. Le password vengono importate da file *.xml e *.ini.

Gestione delle password può esportare il database delle password in file *.xml, *.html o *.txt. L'esportazione è utile per aprire le password generali di accesso, stampare il database delle password o salvare una copia di backup del database delle password in un file di diverso formato in Gestione delle password.

Le password esportate vengono memorizzate in file non crittografati e non sono protette dall'accesso non autorizzato. Di conseguenza, è consigliabile valutare misure per proteggere preventivamente i file esportati.

Durante l'importazione, il database delle password viene modificato. È possibile scegliere di eseguire una delle seguenti azioni sul database delle password:

- **Sovrascrivi**. Il database delle password corrente verrà sostituito da quello importato (tutte le password memorizzate nel database delle password di Gestione delle password prima dell'importazione verranno eliminate).
- **Unisci**. Le password importate da database delle password non protetti verranno aggiunte al database delle password. Durante l'unione viene offerta la possibilità di importare gli account in Gestione delle password.
- **Annulla**. L'operazione di importazione delle password verrà annullata.

Per sostituire il database delle password corrente con un database delle password importato da un'altra applicazione, eseguire le operazioni seguenti:

1. Nel menu di scelta rapida dell'applicazione selezionare **Gestione delle password**.
2. Nella finestra **Gestione delle password** visualizzata fare clic sul pulsante **Importa** nella scheda **Ripristina**.
3. Nella finestra **Importa password** selezionare l'applicazione da cui importare le password, quindi fare clic su **Carica password**.
4. Nella finestra **File Gestione delle password** selezionare il file con le password che si desidera importare e fare clic su **Apri**. Per annullare la selezione, fare clic su **Annulla**.
5. Nella finestra visualizzata, fare clic sul pulsante **Sovrascrivi**.

Per unire il database delle password corrente con un database delle password importato da un'altra applicazione, eseguire le operazioni seguenti:

1. Nel menu di scelta rapida dell'applicazione selezionare **Gestione delle password**.
2. Nella finestra **Gestione delle password** visualizzata fare clic sul pulsante **Importa** nella scheda **Ripristina**.
3. Nella finestra **Importa password** selezionare l'applicazione da cui importare le password, quindi fare clic su **Carica password**.
4. Nella finestra **File Gestione delle password** selezionare il file con le password che si desidera importare e fare clic su **Apri**. Per annullare la selezione, fare clic su **Annulla**.
5. Nella finestra **Carica Gestione delle password** fare clic su **Unisci**.
6. Nella finestra **Importa password** selezionare la casella accanto agli account desiderati, quindi fare clic sul pulsante **Importa**.

   Per selezionare tutti gli account dall'elenco, selezionare la casella accanto all'applicazione desiderata.

Per esportare il database delle password, eseguire le operazioni seguenti:

1. Nel menu di scelta ra pida dell'applicazione selezionare **Gestione delle password**.

2. Nella finestra **Gestione delle password** visualizzata fare clic sul pulsante **Esporta in un file** nella scheda **Ripristina**.

3. Confermare che si desidera esportare il database delle password facendo clic su **OK**. Per evitare di confermare l'esportazione del database delle password in futuro, selezionare la casella **Non visualizzare più questa notifica**.

4. Nella finestra **Esporta database delle password in file non protetto** visualizzata specificare il nome, il percorso e il formato del file.

BACKUP E RIPRISTINO DEL DATABASE DELLE PASSWORD

Prima di apportare qualsiasi modifica al database delle password, viene automaticamente creata una copia di backup. Il percorso della copia di backup viene specificato per impostazione predefinita, ma è possibile modificarlo (vedere pagina 230). È utile ripristinare le password nei seguenti casi:

- se è necessario annullare le modifiche più recenti;
- se il database delle password è stato sovrascritto o eliminato;
- se il database delle password corrente è inaccessibile o danneggiato in seguito a un problema hardware o un errore di sistema.

Tutti i dati nella copia di backup sono memorizzati in formato crittografato. Gestione delle password registra tutte le modifiche apportate al database delle password. Nell'applicazione le copie di backup sono visualizzate in un elenco e ordinate per data, a partire dalla più recente. Per ogni copia di backup sono visualizzate le seguenti informazioni:

- percorso;
- data e ora di creazione;
- modifiche apportate rispetto alla versione precedente.

È possibile utilizzare le copie di backup per eseguire le seguenti attività:

- ripristinare un database delle password da una copia di backup;
- eliminare copie di un archivio di backup;
- modificare il percorso delle copie di backup (vedere pagina 230).

Per ripristinare il database delle password corrente, eseguire le operazioni seguenti:

1. Nel menu di scelta rapida dell'applicazione selezionare **Gestione delle password**.
2. Nella finestra **Gestione delle password** visualizzata fare clic sul pulsante **Importa** nella scheda **Ripristina**.
3. Nella finestra **Ripristino** visualizzata selezionare una copia di backup dall'elenco, quindi fare clic sul pulsante **Ripristina**.
4. Nella finestra visualizzata confermare il ripristino facendo clic su **OK**.

Per rimuovere le copie di backup non necessarie, eseguire le operazioni seguenti:

1. Nel menu di scelta rapida dell'applicazione selezionare **Gestione delle password**.
2. Nella finestra **Gestione delle password** visualizzata fare clic sul pulsante **Importa** nella scheda **Ripristina**.
3. Nella finestra **Ripristino** visualizzata, nell'elenco delle copie di backup, selezionare le versioni delle copie di backup da eliminare. Per selezionare più versioni, tenere premuto il tasto **CTRL**.
4. Fare clic su **Elimina**.
5. Confermare l'eliminazione dell'archivio di backup facendo clic su **OK**.

CONFIGURAZIONE DELLE IMPOSTAZIONI DELL'APPLICAZIONE

Le impostazioni dell'applicazione possono essere configurate solo se il database delle password è sbloccato (vedere pagina 213). Quando si modificano le impostazioni, è possibile eseguire le operazioni seguenti:

- impostare l'ora di avvio dell'applicazione (vedere pagina 235);
- attivare le notifiche (vedere pagina 236);
- specificare il nome utente (vedere pagina 226) da utilizzare per impostazione predefinita durante la creazione di un nuovo account;
- impostare il tempo per cui una password viene memorizzata negli Appunti (vedere pagina 237);
- creare un elenco degli account utilizzati più di frequente (vedere pagina 226);
- creare un elenco di siti Web ignorati (vedere pagina 227) per cui le funzioni di Gestione delle password non vengono utilizzate;
- creare un elenco di siti Web attendibili (vedere pagina 227) per cui Gestione delle password consentirà il reindirizzamento;
- specificare una combinazione di tasti per avviare rapidamente le funzioni di Gestione delle password (vedere pagina 228);
- modificare il percorso per la memorizzazione del database delle password (vedere pagina 229), e delle copie di backup (vedere pagina 230);
- modificare il metodo di crittografia dei dati (vedere pagina 231);
- impostare il blocco automatico del database delle password (vedere pagina 232);
- modificare la password master (vedere pagina 234);
- impostare l'accesso per il database delle password (vedere pagina 232);
- modificare la posizione del pulsante Titolo e creare un elenco di applicazioni che supportano il pulsante Titolo (vedere pagina 237);
- creare un elenco di applicazioni supportate (vedere pagina 234);

Per modificare le impostazioni di Gestione delle password, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella sezione **Protezione+** fare clic su **Gestione delle password**.
3. Nella parte sinistra della finestra **Impostazioni** selezionare la sezione da modificare.
4. Nella parte destra della finestra immettere le modifiche delle impostazioni per la sezione scelta.

IN QUESTA SEZIONE:

Nome utente predefinito 226

Elenco degli account utilizzati di frequente 226

Elenco degli indirizzi Web ignorati 227

Elenco degli indirizzi Web attendibili 228

Avvio veloce delle funzioni dell'applicazione 228

Percorso del database delle password 229

Creazione di un nuovo database delle password 230

Backup del database delle password 230

Selezione del metodo di crittografia 231

Blocco automatico del database delle password 232

Metodo di autorizzazione per Gestione delle password 232

Utilizzo di dispositivi USB e Bluetooth 233

Modifica della password master 234

Creazione di un elenco di browser supportati 234

Ulteriori impostazioni 235

NOME UTENTE PREDEFINITO

Gestione delle password consente di impostare un nome utente che verrà visualizzato automaticamente nel campo **Nome utente** quando si crea un nuovo account (vedere pagina 215).

Per impostare il nome utente predefinito, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella sezione **Protezione+** fare clic su **Gestione delle password**.
3. Nella parte sinistra della finestra **Impostazioni di Gestione delle password**, selezionare la sezione **Generale**.
4. Nella parte destra della finestra compilare il campo **Nome di accesso predefinito**.

ELENCO DEGLI ACCOUNT UTILIZZATI DI FREQUENTE

Gestione delle password consente di accedere velocemente agli account. Il menu dell'applicazione consente di visualizzare un elenco di account utilizzati di frequente. Questo elenco mostra i nomi delle applicazioni e delle pagine Web utilizzate più di frequente. Le voci dell'elenco sono ordinate alfabeticamente o per frequenza di utilizzo.

L'elenco degli account utilizzati di frequente è disponibile nel menu se il database delle password non è bloccato (vedere pagina 213).

È possibile impostare le seguenti opzioni per l'elenco:

- **Numero di voci nell'elenco** – numero massimo di account utilizzati di frequente visualizzati nel menu di scelta rapida dell'applicazione;
- **Visualizzazione dell'elenco nel menu dell'applicazione** – l'elenco di account utilizzati di frequente sarà accessibile nel menu di scelta rapida di Gestione delle password;
- **Visualizzazione dell'elenco nel menu del pulsante Titolo** – l'elenco di account utilizzati di frequente sarà accessibile nel menu del pulsante Titolo (dalla finestra dell'applicazione o del browser).

Per visualizzare gli account utilizzati di frequente nel menu, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella sezione **Protezione+** fare clic su **Gestione delle password**.
3. Nella parte sinistra della finestra **Impostazioni** selezionare **Account utilizzati di frequente**.
4. Nella parte destra della finestra selezionare la casella **Mostra l'elenco nel menu dell'area di notifica**.

   Per visualizzare l'elenco degli account utilizzati di frequente nel menu del pulsante Titolo, selezionare anche la casella di controllo **Visualizza nel menu del pulsante Titolo**.

   Se la casella di controllo **Mostra l'elenco nel menu dell'area di notifica** non è attivata, le opzioni rimanenti nell'elenco non possono essere modificate.

5. Specificare il numero di account nel campo **Dimensione elenco**.
6. Se necessario, modificare le voci dell'elenco manualmente. Per rimuovere una voce dall'elenco, selezionare l'account desiderato, quindi fare clic su **Elimina**. Per eliminare tutte le voci dall'elenco, fare clic su **Cancella**.

ELENCO DEGLI INDIRIZZI WEB IGNORATI

Gestione delle password in genere offre la possibilità di aggiungere un nuovo account alla prima autorizzazione in un sito Web. In questo modo, i dati personali verranno automaticamente reinseriti a ogni visita successiva al sito Web.

Per immettere manualmente i dati personali a ogni autorizzazione successiva, è possibile configurare un elenco di indirizzi Web per cui non verranno utilizzate le funzionalità di Gestione delle password. Per i siti Web in questo elenco l'immissione automatica di nome utente e password è disabilitata. Gestione delle password, inoltre, non richiederà se si desidera creare un nuovo account (vedere pagina 215)/ nome utente (vedere pagina 219).

Per creare l'elenco di indirizzi Web ignorati, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella sezione **Protezione+** fare clic su **Gestione delle password**.
3. Nella parte sinistra della finestra **Impostazioni**, selezionare la sezione **Indirizzi Web ignorati**.
4. Nella parte destra della finestra fare clic su **Aggiungi**, immettere l'indirizzo Web, quindi premere **INVIO**.

   Per modificare un indirizzo Web, selezionarlo nell'elenco, quindi fare clic su **Modifica**. Per eliminare un indirizzo Web dall'elenco, selezionarlo, quindi fare clic su **Elimina**.

ELENCO DEGLI INDIRIZZI WEB ATTENDIBILI

Gestione delle password protegge i dati personali dagli attacchi di phishing. Se durante l'autorizzazione si viene reindirizzati a un altro sito Web, l'applicazione invia una notifica all'utente.

Gli autori di attacchi di phishing spesso utilizzano il reindirizzamento dei siti Web che offrono accesso a conti bancari, come ad esempio siti di banking online, sistemi di pagamento e così via. Nella pagina ufficiale di autorizzazione dell'azienda, gli utenti vengono reindirizzati a un sito Web contraffatto, graficamente simile alla pagina ufficiale. Tutti i dati immessi nella pagina contraffatta cadono nelle mani degli autori dell'attacco.

Il reindirizzamento viene anche utilizzato di frequente nei siti Web legittimi. Se non si desidera che Gestione delle password consideri il reindirizzamento come un attacco di phishing, è possibile creare un elenco di indirizzi Web attendibili. L'elenco di indirizzi Web affidabili include i siti Web a cui vengono trasferiti i dati personali immessi. Durante l'autorizzazione, Gestione delle password notifica all'utente i dati personali trasmessi a un sito Web attendibile.

Gestione delle password consente il trasferimento di dati personali ai siti Web attendibili da altri siti Web. Prima di aggiungere un sito Web all'elenco di indirizzi Web attendibili, è importante verificare che sia completamente affidabile.

È possibile aggiungere un sito Web all'elenco degli indirizzi Web attendibili nei seguenti modi:

- direttamente durante l'autorizzazione nel sito Web;
- manualmente, dalla finestra **Impostazioni di Gestione delle password**.

Per aggiungere un sito Web all'elenco degli indirizzi Web attendibili durante l'autorizzazione nel sito Web, attendere che venga eseguito il reindirizzamento da un sito all'altro, quindi nella finestra Gestione delle password selezionare la casella di controllo **Considera sempre affidabile il sito Web <nome del sito>**.

Per creare manualmente un elenco di indirizzi Web attendibili, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella sezione **Protezione+** fare clic su **Gestione delle password**.
3. Nella parte sinistra della finestra **Impostazioni** selezionare **Indirizzi Web affidabili**.
4. Nella parte destra della finestra, fare clic su **Aggiungi**. Il campo nell'elenco **Indirizzi Web affidabili** diventerà attivo. Immettere l'indirizzo Web, quindi premere **INVIO**.

   Per modificare l'indirizzo Web, selezionarlo nell'elenco, quindi fare clic su **Modifica**. Per eliminare l'indirizzo Web dall'elenco, selezionarlo, quindi fare clic su **Elimina**.

AVVIO VELOCE DELLE FUNZIONI DELL'APPLICAZIONE

Per accedere rapidamente a determinate funzioni dell'applicazione, è possibile utilizzare i tasti di scelta rapida.

È possibile specificare i tasti di scelta rapida per le seguenti azioni:

- Blocco / sblocco di Gestione delle password (vedere pagina 213).
- Immettere la password.
- Visualizzazione della tastiera virtuale.

Per accedere velocemente alle funzioni, è possibile specificare un tasto o una combinazione di due o tre tasti.

Evitare le combinazioni di tasti utilizzate da Microsoft Windows per l'accesso alle funzioni.

Per modificare una combinazione di tasti, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella sezione **Protezione+** fare clic su **Gestione delle password**.
3. Nella parte sinistra della finestra **Impostazioni** selezionare **Tasti di scelta rapida**.
4. Nella parte destra della finestra impostare la combinazione desiderata per ciascuna azione.

PERCORSO DEL DATABASE DELLE PASSWORD

Il database delle password di Gestione delle password è un file crittografato (vedere pagina 231) in cui sono memorizzati tutti i dati personali (account, nomi utente, password e identità).

Per utilizzare il database delle password, è necessario sbloccarlo (vedere pagina 213) (ovvero ottenere l'autorizzazione per il suo utilizzo). Per impostazione predefinita, l'accesso ai dati personali è protetto tramite la password master. Inoltre, Gestione delle password protegge il database delle password utilizzando dispositivi USB o Bluetooth. È possibile modificare i parametri di accesso (vedere pagina 232) per ogni database delle password.

I percorsi predefiniti per le diverse versioni di Microsoft Windows sono i seguenti:

- Microsoft Windows XP: C:\Documents and Settings\Nome_utente\Documenti\Passwords Database\;
- Microsoft Windows Vista: C:\Users\Nome_utente\Documenti\Passwords Database\;
- Microsoft Windows 7: C:\Users\Nome_utente\Documenti\Passwords Database\.

È possibile utilizzare differenti supporti per memorizzare il database delle password: dischi rimovibili, il disco locale o unità di rete.

Quando si modifica il percorso o il nome del database delle password, è possibile eseguire le operazioni seguenti:

- **Copia** – crea una copia del database delle password nel percorso specificato. Questa copia diventerà un database delle password attivo.
- **Sposta** – il database delle password attivo verrà salvato nel percorso specificato.
- **Crea nuovo database delle password** – crea una copia vuota del database delle password, che diventerà attiva.

Per spostare o rinominare il database delle password, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella sezione **Protezione+** fare clic su **Gestione delle password**.
3. Nella parte sinistra della finestra **Impostazioni** selezionare **Password**.
4. Nella parte destra della finestra, in **Percorso**, fare clic su nella parte destra del campo **Percorso**.
5. Nella finestra **Selezionare il database delle password** specificare il nome e il percorso del file, quindi fare clic sul pulsante **Apri**.
6. Nella finestra **Percorso database delle password** selezionare l'azione che si desidera eseguire sul database delle password e confermarla facendo clic su **OK**.
7. Nella finestra **Gestione delle password** immettere la password master per confermare le modifiche.

Per cambiare il database delle password corrente, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella sezione **Protezione+** fare clic su **Gestione delle password**.
3. Nella parte sinistra della finestra **Impostazioni** selezionare **Password**.
4. Nella parte destra della finestra, in **Percorso**, fare clic su nella parte destra del campo **Percorso**.
5. Nella finestra **Selezionare il database delle password** selezionare il file del database delle password, quindi fare clic sul pulsante **Apri**.
6. Nella finestra **Gestione delle password** immettere la password master del database delle password ripristinato.

CREAZIONE DI UN NUOVO DATABASE DELLE PASSWORD

Gestione delle password consente di utilizzare diversi database delle password. Creando un nuovo database delle password, è possibile separare i dati personali e salvarli in due o più database delle password. Se necessario, è possibile ripristinare un database delle password precedente. Gestione delle password può creare un nuovo database delle password se il database delle password corrente è danneggiato o non può essere ripristinato da una copia di backup.

Per creare un nuovo database delle password, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella sezione **Protezione+** fare clic su **Gestione delle password**.
3. Nella parte sinistra della finestra **Impostazioni** selezionare **Password**.
4. Nella parte destra della finestra, in **Percorso**, fare clic su nella parte destra del campo **Percorso**.
5. Nella finestra **Selezionare il database delle password** specificare il percorso e il nome del file del database delle password, quindi fare clic su **Apri**.
6. In **Percorso database delle password** selezionare **Crea nuovo database delle password**, quindi fare clic su **OK**.
7. Nella finestra **Nuovo database delle password**, in **Password**, impostare la password per l'accesso al nuovo database e reimmetterla nel campo **Conferma password**.

   Se la password viene ridigitata in modo errato, verrà evidenziata in rosso.

   In **Algoritmo di crittografia** selezionare il provider di crittografia e metodo di crittografia necessario (vedere pagina 231).
8. Nella finestra visualizzata immettere la nuova password master per confermare la creazione di un nuovo database delle password.

BACKUP DEL DATABASE DELLE PASSWORD

Prima di salvare qualsiasi modifica ai dati personali, Gestione delle password crea automaticamente copie di backup del database delle password. Questo consente di evitare eventuali perdite di dati in caso di errori di sistema o problemi tecnici. Gestione delle password crea una copia completa del database delle password prima di implementare le modifiche. Se il database delle password è danneggiato, è possibile ripristinare i dati dalla più recente copia di backup del database delle password (vedere pagina 224).

È possibile utilizzare differenti supporti per memorizzare la copia di backup del database delle password: il disco locale, dischi rimovibili o unità di rete.

Per impostazione predefinita, a seconda del sistema operativo, la copia di backup viene salvata nel seguente percorso:

- Microsoft Windows XP: C:\Documents and Settings\Nome_utente\Documenti\Passwords Database\;
- Microsoft Windows Vista: C:\Users\Nome_utente\Documenti\Passwords Database\;
- Microsoft Windows 7: C:\Users\Nome_utente\Documenti\Passwords Database\.

Per cambiare il percorso del file di backup, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella sezione **Protezione+** fare clic su **Gestione delle password**.
3. Nella parte sinistra della finestra **Impostazioni** selezionare **Password**.
4. Nella parte destra della finestra, in **Backup**, fare clic sul pulsante a destra del campo **Percorso**.
5. Nella finestra **Sfoglia per cartelle** selezionare la copia di backup del database delle password.

SELEZIONE DEL METODO DI CRITTOGRAFIA

Il compito della crittografia è proteggere le informazioni dall'accesso e dalla distribuzione non autorizzati. La funzione principale della crittografia è trasferire messaggi crittografati tramite canali non protetti.

Per la crittografia e la decrittografia sono necessarie chiavi. Una chiave è un componente essenziale per la crittografia. Se viene utilizzata una sola chiave per la crittografia e la decrittografia, la chiave viene denominata simmetrica. Se vengono utilizzate due chiavi, la crittografia è asimmetrica. La crittografia simmetrica può essere a blocchi o flusso. Qualsiasi informazione, indipendentemente dal formato dei dati di origine, viene interpretata in codice binario. Nella crittografia a blocchi tutti i dati vengono suddivisi in blocchi, ognuno dei quali viene sottoposto a una trasformazione indipendente. Nella crittografia a flusso l'algoritmo viene applicato a ogni bit di informazioni.

Gestione delle password offre i seguenti algoritmi simmetrici:

- **DES**. Crittografia a blocchi con la chiave di dimensione standard di 56 bit. Per gli standard attuali, DES non offre un livello elevato di protezione. Questo algoritmo viene utilizzato quando l'affidabilità non è il requisito principale.
- **3DES**. Un algoritmo a blocchi creato sulla base di DES. Risolve il principale punto debole del suo predecessore: la piccola dimensione della chiave. Le chiavi 3DES sono tre volte più grandi di quelle utilizzate da DES (56*3=168 bit). La velocità operativa è tre volte inferiore a quella di DES, ma il livello di sicurezza è molto più alto. 3DES viene utilizzato più di frequente, dal momento che DES non è sufficientemente resistente alle moderne tecniche di cracking.
- **3DES TWO KEY**. Un algoritmo a blocchi creato sulla base di DES. È un algoritmo 3DES che utilizza una dimensione delle chiavi di 112 bit (56*2).
- **RC2**. Un algoritmo di crittografia a blocchi con una chiave di lunghezza variabile, che consente di elaborare velocemente una grande quantità di informazioni. È un algoritmo più veloce di DES. In termini di protezione e resistenza, è equivalente a 3DES.
- **RC4**. Un algoritmo di crittografia a flusso con chiave di lunghezza variabile. La dimensione della chiave può variare da 40 a 256 bit. I vantaggi di questo algoritmo sono la velocità elevata e la dimensione variabile della chiave. Per impostazione predefinita, Gestione delle password utilizza RC4 per la crittografia dei dati.
- **AES**. Un algoritmo simmetrico di crittografia a blocchi con una lunghezza della chiave di 128, 192 e 256 bit. Questo algoritmo garantisce un livello elevato di sicurezza ed è uno di quelli utilizzati più di frequente.

Microsoft Windows utilizza un provider di crittografia per eseguire le operazioni di crittografia. Ogni provider di crittografia supporta diversi algoritmi di crittografia con una lunghezza della chiave specificata. Gestione delle password utilizza i seguenti provider di crittografia disponibili in Microsoft Windows:

- Microsoft Base Cryptographic Provider;
- Microsoft Enhanced Cryptographic Provider;
- Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype);
- Microsoft RSA/Schannel Cryptographic Provider;
- Microsoft Strong Cryptographic Provider.

Per cambiare l'algoritmo di crittografia, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella sezione **Protezione+** fare clic su **Gestione delle password**.
3. Nella parte sinistra della finestra **Impostazioni** selezionare **Password**.
4. Nella parte destra della finestra, in **Crittografia dei dati**, fare clic su **Cambia**.
5. Nella finestra **Algoritmo di crittografia** specificare i parametri per l'algoritmo di crittografia.

BLOCCO AUTOMATICO DEL DATABASE DELLE PASSWORD

Gestione delle password blocca automaticamente il database delle password dopo l'avvio di un'applicazione e dopo un periodo di tempo specificato di inattività del computer. È possibile specificare l'intervallo di tempo al termine del quale il database delle password verrà bloccato. Il valore dell'intervallo varia da 1 a 60 minuti. È consigliabile bloccare il database delle password dopo 5-20 minuti di inattività del computer. È inoltre possibile disattivare il blocco automatico del database delle password.

Gestione delle password blocca automaticamente il database delle password dopo un periodo specificato di inattività del computer. Se il blocco automatico del computer è disattivato, i dati personali non verranno protetti se si lascia il computer senza bloccarlo manualmente.

Per modificare l'intervallo di tempo dopo il quale il database delle password viene bloccato, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella sezione **Protezione+** fare clic su **Gestione delle password**.
3. Nella parte sinistra della finestra **Impostazioni** selezionare **Password**.
4. Nella parte destra della finestra, in **Blocco automatico**, utilizzare l'elenco a discesa per selezionare il tempo dopo il quale Gestione delle password verrà bloccato.

   Per disattivare il blocco di Gestione delle password, selezionare **Mai**.

METODO DI AUTORIZZAZIONE PER GESTIONE DELLE PASSWORD

L'autorizzazione consente di controllare l'accesso ai propri dati personali. È possibile utilizzare uno dei seguenti metodi di autorizzazione:

- **Password master**. Per sbloccare il database delle password, è necessario immettere la password master. Questo è il metodo di autorizzazione predefinito.

- **Dispositivo USB**. Per accedere al database delle password, connettere un dispositivo USB al computer. È ad esempio possibile utilizzare come dispositivo USB schede flash, fotocamere, lettori MP3 e dischi rigidi esterni. Quando il dispositivo USB è disabilitato, il database delle password viene bloccato automaticamente.

- **Dispositivo Bluetooth**. Per accedere al database delle password, utilizzare un dispositivo Bluetooth. La connettività Bluetooth deve essere attivata sia nel telefono cellulare che nel computer che utilizza Gestione delle password. Quando si connettono un telefono cellulare e un computer tramite Bluetooth, Gestione delle password verrà sbloccato. Se il collegamento si interrompe, ad esempio perché si disattiva Bluetooth sul telefono cellulare, il database delle password verrà bloccato.

- **Nessuna autorizzazione**. L'accesso al database è privo di protezione.

  Senza autorizzazione, i dati personali sono accessibili a tutti gli utenti che utilizzano il computer.

Se si seleziona l'autorizzazione tramite un dispositivo USB o Bluetooth, è consigliabile memorizzare la password master. Se non è disponibile alcun dispositivo di autorizzazione, Gestione delle password consente di utilizzare la password master per l'accesso ai dati personali.

Per cambiare il metodo di autorizzazione, eseguire le operazioni seguenti:

1. Aprire la finestra principaledell'applicazione.
2. Nella sezione **Protezione+** fare clic su **Gestione delle password**.
3. Nella parte sinistra della finestra **Impostazioni** selezionare **Metodo di autorizzazione**.
4. Nella parte destra della finestra, in **Metodo di autorizzazione**, selezionare un'opzione di autorizzazione dall'elenco a discesa.

VEDERE ANCHE:

Utilizzo di dispositivi USB e Bluetooth 233

UTILIZZO DI DISPOSITIVI USB E BLUETOOTH

Per accedere al database delle password (vedere pagina 232), Gestione delle password consente di utilizzare vari dispositivi USB e Bluetooth.

Per utilizzare un dispositivo USB per accedere al database delle password, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella sezione **Protezione+** fare clic su **Gestione delle password**.
3. Nella parte sinistra della finestra **Impostazioni** selezionare **Metodo di autorizzazione**.
4. Nella parte destra della finestra, in **Metodo di autorizzazione**, selezionare il valore **Dispositivo USB** dall'elenco a discesa.
5. Connettere il dispositivo rimovibile al computer.
6. Selezionare un dispositivo dall'elenco **Unità disco**, quindi fare clic su **Imposta**. L'icona verrà visualizzata accanto al dispositivo selezionato. Se il dispositivo connesso non è visualizzato nell'elenco, selezionare la casella **Mostra ulteriori dispositivi**. Se necessario, è possibile modificare il dispositivo di autorizzazione facendo clic su **Reimposta**.

Per utilizzare un dispositivo Bluetooth per accedere al database delle password, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella sezione **Protezione+** fare clic su **Gestione delle password**.
3. Nella parte sinistra della finestra **Impostazioni** selezionare **Metodo di autorizzazione**.
4. Nella parte destra della finestra, in **Metodo di autorizzazione**, selezionare il valore **Dispositivo Bluetooth** dall'elenco a discesa.
5. Attivare la connettività Bluetooth nel computer, quindi nel dispositivo.
6. Selezionare un dispositivo dall'elenco **Telefoni e modem**, quindi fare clic su **Imposta**. L'icona verrà visualizzata accanto al dispositivo selezionato. Se necessario, è possibile modificare il dispositivo di autorizzazione facendo clic su **Reimposta**.

MODIFICA DELLA PASSWORD MASTER

Gestione delle password consente di utilizzare la password master per accedere al database delle password (vedere pagina 232). Di conseguenza, è sufficiente memorizzare una sola password. Per impostazione predefinita, una password master viene creata al primo avvio di Gestione delle password. È possibile modificarla in seguito. La sicurezza dei dati personali dipende in larga misura dall'affidabilità della password master. Quando si crea una password master, Gestione delle password valuta automaticamente la sua complessità e le assegna un particolare stato:

- complessità bassa;
- complessità normale;
- complessità elevata.

Per creare una password sicura, utilizzare simboli speciali, numeri e lettere maiuscole e minuscole. Non è consigliabile utilizzare come password informazioni che possono essere facilmente indovinate, ad esempio nomi o date di nascita di membri della famiglia.

Quando si modifica la password master, Gestione delle password richiede conferma della password immessa (la nuova password deve essere inserita nuovamente). Non è possibile salvare la nuova password senza conferma. Se la password di conferma non corrisponde alla password immessa, la password di conferma verrà visualizzata in rosso. In tal caso, verrà visualizzato un messaggio di avviso quando si tenta di salvare la nuova password.

Per cambiare la password master, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella sezione **Protezione+** fare clic su **Gestione delle password**.
3. Nella parte sinistra della finestra **Impostazioni** selezionare **Metodo di autorizzazione**.
4. Nella parte destra della finestra, in **Protezione tramite password**, fare clic su **Cambia**.
5. Nella finestra **Protezione tramite password** immettere la nuova password, quindi confermarla immettendola nuovamente nel campo **Conferma password**.

CREAZIONE DI UN ELENCO DI BROWSER SUPPORTATI

Per assicurare il corretto funzionamento dell'attivazione automatica dell'account e del pulsante Titolo (vedere pagina 237), Gestione delle password richiede l'installazione di ulteriori estensioni (plug-in) per diversi browser. Per impostazione predefinita, i plug-in sono installati al primo avvio di Gestione delle password. È possibile installare ulteriori plug-in.

Gestione delle password contiene un elenco di browser Web e di client di posta elettronica, in cui a ogni programma è assegnato lo stato **Installato** o **Non installato**, a seconda del fatto che il plug-in necessario sia installato o meno.

È consigliabile chiudere tutti i programmi in cui deve essere installato il plug-in.

Per installare un plug-in per un browser o un client di posta elettronica, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella sezione **Protezione+** fare clic su **Gestione delle password**.
3. Nella parte sinistra della finestra **Impostazioni** selezionare **Browser supportati**.
4. Nella parte destra della finestra selezionare un browser dall'elenco **Browser supportati ed estensioni disponibili**, quindi fare clic su **Installa**.
5. Seguire le istruzioni fornite nel corso dell'**Installazione guidata**. Quando il plug-in è installato, il browser verrà automaticamente spostato nel gruppo **Installato**. Al browser verrà assegnato lo stato **Installato**. È possibile eliminare un plug-in installato facendo clic su **Disinstalla**.

ULTERIORI IMPOSTAZIONI

È possibile impostare le seguenti impostazioni aggiuntive per Gestione delle password:

- l'ora di avvio dell'applicazione (vedere pagina 235);
- azione avviata facendo doppio clic (vedere pagina 235);
- invio di notifiche (vedere pagina 236);
- il tempo per cui una password viene memorizzata negli Appunti (vedere pagina 237);
- pulsante Titolo (vedere pagina)237.

MODALITÀ DI AVVIO DELL'APPLICAZIONE

Per impostazione predefinita, Gestione delle password viene caricato automaticamente all'avvio del sistema operativo. È possibile modificare i parametri di avvio dell'applicazione.

Per avviare l'applicazione manualmente, eseguire le operazioni seguenti:

1. Aprire la finestra principale finestra.
2. Nella sezione **Protezione+** fare clic su **Gestione delle password**.
3. Nella parte sinistra della finestra **Impostazioni di Gestione delle password**, selezionare la sezione **Generale**.
4. Nella parte destra della finestra, nella sezione **Impostazioni di Gestione delle password**, deselezionare la casella **Carica Gestione delle password all'avvio di Windows**.

AZIONE PER IL DOPPIO CLIC

Gestione delle password consente di impostare l'attività avviata facendo doppio clic sull'icona dell'applicazione nell'area di notifica della barra delle applicazioni di Microsoft Windows. In questo modo è possibile avviare una delle seguenti attività:

- aprire la finestra principale di Gestione delle password (vedere pagina 211);

- bloccare / sbloccare Gestione delle password (azione predefinita).

Per impostare l'attività avviata facendo doppio clic sull'icona dell'applicazione nell'area di notifica della barra delle applicazioni, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella sezione **Protezione+** fare clic su **Gestione delle password**.
3. Nella parte sinistra della finestra **Impostazioni di Gestione delle password**, selezionare la sezione **Generale**.
4. Nella parte destra della finestra selezionare l'azione dall'elenco a discesa **In caso di doppio clic**.

NOTIFICHE

Quando Gestione delle password è in esecuzione, possono verificarsi vari eventi di natura informativa. Per restare sempre aggiornati, è possibile utilizzare il servizio di notifica. Gli utenti ricevono notifiche degli eventi tramite messaggi di avviso e finestre a comparsa.

Nell'applicazione sono implementati i seguenti tipi di notifiche:

- **Avvio applicazione**. Viene visualizzato un messaggio al riavvio dell'applicazione quando l'applicazione è già stata avviata e il database delle password non è bloccato.
- **Attivazione account**. Viene visualizzato un messaggio all'attivazione dell'account.
- **Cancella Appunti**. Gestione delle password può memorizzare temporaneamente le password negli Appunti. Questo è utile quando è necessario copiare e incollare i dati nel campo selezionato. Al termine del periodo di tempo specificato (vedere pagina 237), la password verrà eliminata dagli Appunti.
- **Blocco automatico di Gestione delle password**. Questo messaggio viene visualizzato quando Gestione delle password blocca automaticamente il database delle password. Per impostazione predefinita, Gestione delle password blocca automaticamente il database delle password dopo l'avvio del sistema operativo e dopo un periodo di tempo specificato (vedere pagina 232) di inattività del computer.
- **Esportazione password in file crittografato**. Un messaggio di avviso che segnala che, dopo l'esportazione, le password verranno salvate in un file non crittografato e verranno quindi rese disponibili per qualsiasi utente che utilizza il computer. Prima di esportare i dati, è consigliabile valutare come proteggere il file che contiene le password.
- **Modifica manuale modulo**. Per impostare parametri per ulteriori campi, l'applicazione richiede l'autorizzazione di utilizzare il browser predefinito. Il messaggio segnala che immagini e file di sistema (cookie) verranno salvati nel computer.
- **Difficoltà a compilare le informazioni di accesso per l'account**. Questo messaggio indica che non è stato possibile immettere automaticamente i dati personali durante l'autorizzazione.

Per ricevere le notifiche, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella sezione **Protezione+** fare clic su **Gestione delle password**.
3. Nella parte sinistra della finestra **Impostazioni di Gestione delle password**, selezionare la sezione **Generale**.
4. Nella parte destra della finestra fare clic sul pulsante **Impostazioni notifica** nella sezione **Generale**.
5. Nella finestra visualizzata, selezionare o deselezionare la casella accanto ai tipi di notifiche desiderati.

TEMPO DI MEMORIZZAZIONE DELLE PASSWORD NEGLI APPUNTI

Gestione delle password consente di copiare le password negli Appunti per un periodo di tempo specificato. Si tratta di una funzionalità utile per eseguire rapidamente operazioni con le password, ad esempio quando è necessario utilizzare una password creata per eseguire la registrazione in un sito Web o un'applicazione. È possibile impostare il periodo di tempo per cui la password verrà memorizzata negli Appunti. Al termine di tale periodo, la password verrà automaticamente eliminata dagli Appunti. Questo impedisce l'intercettazione e il furto delle password, dal momento che non sarà possibile copiarle dagli Appunti al termine del periodo di tempo specificato.

Per modificare il tempo di memorizzazione della password negli Appunti, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella sezione **Protezione+** fare clic su **Gestione delle password**.
3. Nella parte sinistra della finestra **Impostazioni**, selezionare la sezione **Generale**.
4. Nella parte destra della finestra, in **Appunti**, specificare il tempo in secondi.

PULSANTE TITOLO

Gestione delle password può gestire gli account direttamente dalla finestra dell'applicazione o del browser tramite il pulsante Titolo disponibile nell'angolo superiore sinistro di tale finestra. Facendo clic sul pulsante Titolo viene visualizzato un menu con un elenco di nomi utente correlati all'applicazione o alla pagina Web. Quando si seleziona un nome utente, Gestione delle password compila automaticamente i campi di autorizzazione dal database delle password.

Il pulsante Titolo è accessibile se il database delle password non è bloccato (vedere pagina 213).

Se, oltre al menu di Program Manager, l'applicazione che si sta utilizzando dispone di altri menu incorporati, è possibile impostare la posizione del pulsante Titolo in relazione agli altri pulsanti. È inoltre possibile generare un elenco di browser per cui viene utilizzato il pulsante Titolo.

Per modificare i parametri del pulsante Titolo, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella sezione **Protezione+** fare clic su **Gestione delle password**.
3. Nella parte sinistra della finestra **Impostazioni** selezionare **Pulsante Titolo**.
4. Nella parte destra della finestra, in **Visualizzazione pulsante Titolo**, impostare i parametri desiderati a seconda dell'attività:
   - Per modificare la posizione del pulsante Titolo, in **Visualizzazione pulsante Titolo** immettere il numero di posizione del pulsante (ovvero il numero di pulsanti a destra del pulsante Titolo).
   - Per impedire la visualizzazione del pulsante Titolo quando il database delle password è bloccato, in **Visualizzazione pulsante Titolo** selezionare la casella ☑ **Non visualizzare il pulsante se Gestione delle password è bloccato**.
   - Per creare un elenco di browser in cui rendere disponibile il pulsante Titolo, in **Pulsante Titolo nei browser Web**, selezionare la casella ☑ accanto al browser desiderato nell'elenco.

FUNZIONI AVANZATE

Gestione delle password include numerosi altri strumenti:

- **Generatore di password** permette di creare password sicure per gli account.
- Il **puntatore di Gestione delle password** consente di selezionare velocemente un'applicazione o una pagina Web e quindi di definire automaticamente l'azione per l'oggetto scelto.

IN QUESTA SEZIONE:

Generatore di password 238

Puntatore di Gestione delle password 239

GENERATORE DI PASSWORD

La sicurezza dei dati dipende direttamente dalla complessità delle password. I dati possono essere a rischio nei seguenti casi:

- viene utilizzata una sola password per tutti gli account;
- la password è semplice;
- la password utilizza informazioni facili da indovinare, ad esempio, nomi o date di nascita di membri della famiglia.

Per garantire la sicurezza dei dati, Gestione delle password consente di creare password univoche e affidabili per gli account. Gestione delle password salva tutte le password generate, evitando all'utente di doverle memorizzare.

Una password viene considerata sicura se è formata da più di quattro caratteri e contiene simboli speciali, numeri e lettere maiuscole e minuscole.

La sicurezza delle password viene determinata tramite i seguenti parametri:

- **Lunghezza** – il numero di caratteri della password. Questo valore più variare da 4 a 99 caratteri. Maggiore è la lunghezza della password, più questa viene considerata sicura.
- **A-Z** – lettere maiuscole.
- **a-z** – lettere minuscole.
- **0-9** – numeri.
- **Simboli speciali** – simboli speciali.
- **Escludi simboli simili** – l'utilizzo di simboli identici in una password non è consentito.

È possibile utilizzare Generatore di password per eseguire le seguenti attività:

- durante la creazione di un nuovo account in un'applicazione o su un sito Web;
- durante l'aggiunta manuale di un account (vedere pagina 215) o un nome utente (vedere pagina 219) in Gestione delle password.

Per utilizzare Generatore di password durante la creazione di un nuovo account in un'applicazione o un sito Web, eseguire le operazioni seguenti:

1. Aprire il menu di scelta rapida di Gestione delle password e selezionare **Generatore di password**.
2. Nella finestra **Generatore di password** specificare il numero di caratteri della password nel campo **Lunghezza password**.
3. Se necessario, è possibile specificare ulteriori impostazioni per Generatore di password nella sezione **Avanzate**, selezionando o deselezionando la casella accanto alle impostazioni desiderate.
4. Fare clic su **Genera**. La password generata viene visualizzata nel campo **Password**. Per visualizzare la password generata, selezionare la casella **Mostra password**.
5. Incollare la password negli Appunti utilizzando il pulsante , quindi immettere la password nel campo di immissione della password nell'applicazione o nella pagina Web premendo **CTRL+V**. La password generata viene memorizzata negli Appunti per uno specifico periodo di tempo prima di essere eliminata.
6. Selezionare la casella **Predefinito** per salvare le impostazioni specificate.

PUNTATORE DI GESTIONE DELLE PASSWORD

Gestione delle password rende molto semplice utilizzare i propri account. Il puntatore di Gestione delle password consente di selezionare velocemente l'applicazione o la pagina Web per cui si desidera immettere dati personali.

Quando si avvia l'applicazione o la pagina Web, Gestione delle password cerca automaticamente un account permanente nel database delle password. Se viene individuato un account, i dati personali vengono immessi automaticamente nei campi di autorizzazione. Se non è disponibile alcun account permanente nel database delle password, Gestione delle password offre la possibilità di aggiungere un nuovo account. Nella finestra dell'applicazione o del browser viene automaticamente eseguita una ricerca di campi contenenti nome utente e password. Nella finestra dell'applicazione o del browser visualizzata, i campi vengono automaticamente compilati utilizzando i dati individuati nel database delle password. È necessario compilare solo i campi vuoti.

Per utilizzare il puntatore di Gestione delle password, eseguire le operazioni seguenti:

1. Posizionare il puntatore del mouse sull'icona Gestione delle password nell'area di notifica della barra delle applicazioni e attendere alcuni secondi.
2. Quando viene visualizzato, trascinare il puntatore di Gestione delle password nella finestra dell'applicazione o del browser desiderata. Gestione delle password definisce automaticamente l'azione da eseguire sull'applicazione o la pagina Web scelta.

CENTRO DI CONTROLLO

Centro di controllo è progettato per il controllo remoto di Kaspersky PURE installata in computer in rete. Il controllo viene eseguito dalla workstation di amministrazione.

L'amministratore di rete può eseguire le seguenti azioni tramite Centro di controllo:

- analisi del livello di protezione dei computer in rete;
- analisi delle minacce nell'intera rete o in singoli computer;
- aggiornamento centralizzato dei database anti-virus;
- modifica delle impostazioni di protezione per i computer in rete;
- Parental Control;
- backup dei dati nei computer in rete;
- visualizzazione di rapporti sul funzionamento dei sottosistemi di protezione.

Per avviare Centro di controllo, eseguire le operazioni seguenti:

Nella parte superiore della finestra di Kaspersky PURE fare clic sul collegamento **Centro di controllo**.

Al primo avvio viene eseguita automaticamente la Configurazione guidata controllo remoto (vedere la sezione "Configurazione della gestione remota" a pagina 240). In seguito sarà necessario immettere la password.

Per la gestione remota tramite la rete locale, la password di Centro di controllo deve essere identica in tutti i computer.

IN QUESTA SEZIONE:

Configurazione della gestione remota 240

Analisi della protezione della rete 241

Gestione dei componenti di protezione 242

Gestione delle licenze 242

Gestione di Parental Control 242

Scansione remota di virus e vulnerabilità 243

Aggiornamento dei database e dei moduli dell'applicazione 243

Backup remoto 244

CONFIGURAZIONE DELLA GESTIONE REMOTA

Il controllo remoto viene configurato tramite la procedura guidata. Al primo avvio di Centro di controllo, viene avviata automaticamente la Configurazione guidata.

La procedura guidata è costituita da una serie di schermate (passaggi) tra le quali è possibile spostarsi servendosi dei pulsanti **Avanti** e **Indietro**. Per chiudere la procedura guidata al completamento, utilizzare il pulsante **Fine**. Per interrompere la procedura in qualsiasi momento, utilizzare il pulsante **Annulla**.

È anche possibile spostarsi tra i passaggi della procedura guidata completati utilizzando i pulsanti di spostamento nella parte superiore della finestra.

Per configurare Centro di controllo, eseguire le operazioni seguenti:

1. Aprire la finestra principale applicazione e fare clic sul collegamento **Centro di controllo** nella parte superiore della finestra.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Verrà avviata la Configurazione guidata controllo remoto. Al primo avvio di Centro di controllo, viene avviata automaticamente la Configurazione guidata. I passaggi della procedura guidata sono descritti di seguito:
   a. Immettere o impostare la password di amministratore nella finestra **Protezione tramite password**.
   b. Selezionare una rete per il controllo remoto nella finestra **Scansione della rete**.
   c. Selezionare la modalità di aggiornamento per i database anti-virus nella finestra **Sorgente dell'aggiornamento**.
   d. Confermare le impostazioni selezionate nella finestra **Riepilogo**.

ANALISI DELLA PROTEZIONE DELLA RETE

Nella parte superiore della finestra Centro di controllo è visualizzato lo stato corrente della protezione della rete.

Esistono tre possibili valori per lo stato della protezione: ognuno di essi è indicato con un determinato colore, simili a quelli di un semaforo. Il verde indica che la protezione della rete è di livello adeguato, il giallo ed il rosso evidenziano la presenza di minacce alla protezione. Oltre ai programmi dannosi, le minacce comprendono il mancato aggiornamento dei database dell'applicazione obsoleti, la disabilitazione di componenti di protezione e la selezione di impostazioni di protezione minime. Le minacce alla protezione devono essere eliminate non appena compaiono.

Per ottenere informazioni dettagliate sui problemi di protezione della rete ed eliminarli, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul fare clic sul collegamento **Centro di controllo** nella parte superiore della finestra.
2. Nella finestra visualizzata fare clic sull'icona dello stato o sull'icona del riquadro in cui è visualizzata (vedere la figura precedente).

   Nella finestra **Stato di protezione della rete** visualizzata sono indicati i problemi correnti.

È inoltre possibile visualizzare l'elenco di problemi in singoli computer della rete ed eliminare alcuni di essi in remoto.

Per ottenere l'elenco dei problemi per un singolo computer della rete, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e farefare clic sul collegamento **Centro di controllo** nella parte superiore della finestra.
2. Nella finestra visualizzata selezionare il computer per cui si desidera visualizzare l'elenco dei problemi, quindi passare alla sezione **Informazioni**.

3. Nella parte destra della finestra visualizzata selezionare il comando **Elenco di problemi**.

   Nella finestra **Stato della protezione** visualizzata sono indicati i problemi correnti rilevati nel computer selezionato.

GESTIONE DEI COMPONENTI DI PROTEZIONE

Utilizzando Centro di controllo, è possibile attivare e disattivare in remoto i vari componenti di protezione nei computer della rete.

Per attivare o disattivare in remoto un componente di protezione, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Centro di controllo** nella parte superiore della finestra principale.

2. Nella finestra visualizzata selezionare il computer per cui si desidera gestire la protezione, quindi passare alla sezione **Informazioni**.

3. Nella parte destra della finestra selezionare **Stato componenti di protezione**.

4. Nella finestra visualizzata abilitare / disabilitare il componente di protezione facendo clic sul relativo nome.

GESTIONE DELLE LICENZE

Utilizzando Centro di controllo, è possibile controllare in remoto lo stato della licenza nei computer della rete, rinnovare la licenza o attivarne una nuova.

Per gestire la licenza in un computer della rete, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Centro di controllo** nella parte superiore della finestra principale.

2. Nella finestra visualizzata selezionare il computer per cui si desidera visualizzare l'elenco dei problemi, quindi passare alla sezione **Informazioni**.

3. Nella parte destra della finestra visualizzata selezionare il comando **Gestione delle licenze**.

4. Nella finestra **Gestione delle licenze** visualizzata eseguire le operazioni desiderate.

GESTIONE DI PARENTAL CONTROL

Utilizzando Centro di controllo, è possibile impostare in remoto restrizioni e visualizzare statistiche sugli eventi correlati alle attività degli utenti nei computer della rete e su Internet o relativi alla messaggistica immediata.

Per configurare Parental Control, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Centro di controllo** nella parte superiore della finestra.

2. Nella parte superiore della finestra visualizzata selezionare un computer e passare alla sezione **Parental Control**.

3. Nella parte destra della finestra selezionare un account, quindi fare clic sul pulsante **Configura**.

Per visualizzare le statistiche, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Centro di controllo** nella parte superiore della finestra principale.
2. Nella parte superiore della finestra visualizzata selezionare un computer e passare alla sezione **Parental Control**.
3. Nella parte destra della finestra selezionare un account, quindi fare clic sul pulsante **Rapporto dettagliato**.

SCANSIONE REMOTA DI VIRUS E VULNERABILITA

Utilizzando Centro di controllo, è possibile eseguire in remoto un'attività di scansione anti-virus per l'intera rete o per un singolo computer.

Per eseguire una scansione anti-virus dell'intera rete, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Centro di controllo** nella parte superiore della finestra principale.
2. Nella finestra visualizzata fare clic sul collegamento **Esegui scansione anti-virus** nella sezione **Azioni per la rete** nella parte superiore della finestra.
3. Nella finestra **Avvio di gruppo della scansione** visualizzata selezionare il tipo di scansione e i computer da esaminare.

Per eseguire una scansione alla ricerca di virus o vulnerabilità in un singolo computer, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Centro di controllo** nella parte superiore della finestra principale.
2. Nella parte superiore della finestra visualizzata selezionare un computer e passare alla sezione **Scansione**.
3. Nella parte destra della finestra selezionare l'attività di scansione desiderata.

AGGIORNAMENTO DEI DATABASE E DEI MODULI DELL'APPLICAZIONE

Utilizzando Centro di controllo, è possibile gestire in remoto l'aggiornamento di Kaspersky PURE nei computer in rete.

È possibile selezionare una delle modalità di aggiornamento seguenti:

- Aggiornamento indipendente dei database nei computer.
- Aggiornamento centralizzato tramite un server degli aggiornamenti dedicato.

Per modificare la modalità di aggiornamento per i computer della rete, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Centro di controllo** nella parte superiore della finestra principale.
2. Nella finestra visualizzata, fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
3. Nella procedura guidata per la configurazione di Centro di controllo visualizzata, procedere fino al passaggio **Server degli aggiornamenti**, quindi selezionare la modalità di aggiornamento desiderata.

Quando si seleziona l'aggiornamento centralizzato, uno dei computer della rete deve operare come server degli aggiornamenti. Gli altri computer scaricano gli aggiornamenti dal server selezionato.

- *Per selezionare il server degli aggiornamenti, eseguire le operazioni seguenti:*

  1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Centro di controllo** nella parte superiore della finestra principale.
  2. Nella parte superiore della finestra visualizzata selezionare un computer, quindi passare alla sezione **Aggiornamenti**.
  3. Fare clic sul pulsante **Seleziona come server degli aggiornamenti**.

È possibile eseguire in remoto un'attività di aggiornamento per l'intera rete o per un singolo computer.

- *Per eseguire l'aggiornamento su tutti i computer della rete, eseguire le operazioni seguenti:*

  1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Centro di controllo** nella parte superiore della finestra.
  2. Nella parte superiore della finestra visualizzata fare clic sul collegamento **Avvia aggiornamento** nel menu **Azioni per la rete**.
  3. Nella finestra **Avvio di gruppo dell'aggiornamento** visualizzata selezionare i computer in cui si desidera scaricare gli aggiornamenti.

- *Per eseguire l'aggiornamento in un singolo computer, eseguire le operazioni seguenti:*

  1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Centro di controllo** nella parte superiore della finestra principale.
  2. Nella parte superiore della finestra visualizzata selezionare un computer, quindi passare alla sezione **Aggiornamenti**.
  3. Nella parte destra della finestra, fare clic sul pulsante **Avvia aggiornamento**.

BACKUP REMOTO

Utilizzando Centro di controllo, è possibile eseguire in remoto attività di backup nei computer della rete, nonché visualizzare il rapporto sulle attività di backup e ripristino dei dati eseguite.

- *Per eseguire il backup di oggetti in remoto, eseguire le operazioni seguenti:*

  1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Centro di controllo** nella parte superiore della finestra principale.
  2. Nella parte superiore della finestra visualizzata selezionare un computer e passare alla sezione **Backup**.
  3. Nella parte destra della finestra selezionare un'attività di backup, quindi fare clic sul pulsante **Esegui**.

     È possibile sospendere o interrompere l'esecuzione dell'attività utilizzando i pulsanti corrispondenti nella parte superiore della finestra.

- *Per ottenere un rapporto sull'esecuzione delle attività di backup e ripristino dei dati, eseguire le operazioni seguenti:*

  1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Centro di controllo** nella parte superiore della finestra principale.
  2. Nella parte superiore della finestra visualizzata selezionare un computer e passare alla sezione **Backup**.
  3. Fare clic sul pulsante **Visualizza rapporto** nella parte superiore della finestra.
  4. Nella finestra **Rapporto** visualizzata specificare le impostazioni di visualizzazione degli eventi.

CONFIGURAZIONE DELLE IMPOSTAZIONI DI KASPERSKY PURE

La finestra delle impostazioni dell'applicazione consente di accedere rapidamente alle principali impostazioni di Kaspersky PURE.

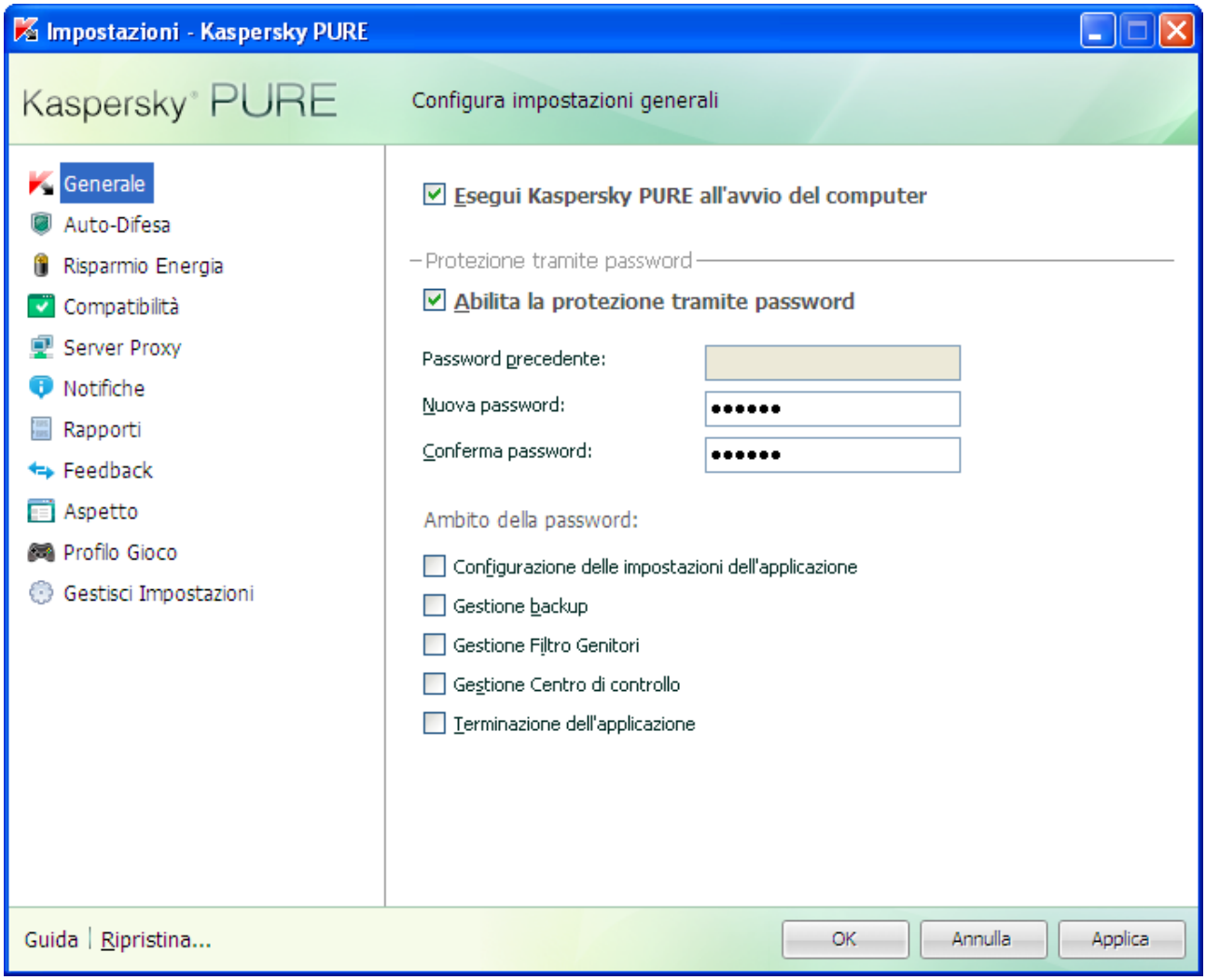


Figura 23. Configurazione Kaspersky Anti-Virus

La finestra delle impostazioni si compone di due parti:

- la parte sinistra della finestra consente di accedere a impostazioni di Kaspersky PURE, attività di scansione anti-virus, attività di aggiornamento e così via;
- la parte destra della finestra contiene un elenco di parametri relativi al componente o all'attività selezionati nella parte sinistra della finestra.

È possibile aprire questa finestra:

- Dalla finestra principale dell'applicazione (vedere pagina)44. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.

- Dal menu di scelta rapida (vedere pagina 42). A tale scopo, selezionare la voce **Impostazioni** dal menu di scelta rapida.

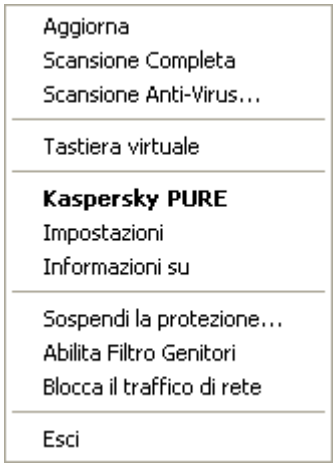


Figura 24. Menu di scelta rapida

IN QUESTA SEZIONE:

Impostazioni generali 246

Auto-Difesa 247

Risparmio energetico per funzionamento a batteria 248

Compatibilità 248

Server proxy 249

Notifiche 249

Rapporti 251

Commenti 252

Aspetto dell'applicazione 252

Profilo Gioco 253

Gestione delle impostazioni dell'applicazione 254

IMPOSTAZIONI GENERALI

In questa finestra è possibile utilizzare le seguenti funzioni avanzate di Kaspersky PURE:

- Esecuzione di Kaspersky PURE all'avvio del sistema (vedere pagina 247).
- Restrizione dell'accesso a Kaspersky PURE (vedere pagina 247).

ESECUZIONE DI KASPERSKY PURE ALL'AVVIO DI WINDOWS

Se è necessario arrestare completamente Kaspersky PURE per qualsiasi motivo, selezionare **Esci** dal menu di scelta rapida di Kaspersky PURE. L'applicazione non viene più caricata nella RAM. Ciò significa che il computer viene eseguito senza protezione.

È possibile attivare nuovamente la protezione del computer caricando Kaspersky PURE dal menu **Start** → **Programmi** → **Kaspersky PURE** → **Kaspersky PURE**.

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

Per abilitare questa modalità:

1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Impostazioni** nella parte superiore.
2. Nella finestra visualizzata selezionare la sezione **Generale**, quindi selezionare la casella **Esegui Kaspersky PURE all'avvio del computer**.

RESTRIZIONE DELL'ACCESSO A KASPERSKY PURE

Un personal computer può essere utilizzato da diversi utenti, con differenti livelli di esperienza in ambito informatico. Se si consente il libero accesso a Kaspersky PURE e alle relative impostazioni, il livello di protezione generale del computer potrebbe diminuire drasticamente.

Per aumentare il livello di protezione del computer, utilizzare una password per accedere a Kaspersky PURE. È possibile bloccare qualsiasi operazione di Kaspersky PURE ad eccezione delle notifiche di rilevamento di oggetti pericolosi o impedire l'esecuzione delle azioni seguenti:

- modifica delle impostazioni dell'applicazione;
- gestione dei backup;
- gestione di Parental Control;
- gestione remota della protezione della rete;
- chiusura dell'applicazione.

Per proteggere l'accesso a Kaspersky PURE tramite una password, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul. collegamento **Impostazioni** nella parte superiore.
2. Nella finestra visualizzata selezionare la sezione **Generale** e in **Protezione tramite password** selezionare la casella **Abilita la protezione tramite password**, quindi fare clic sul pulsante **Impostazioni**.
3. Nella finestra **Protezione dell'applicazione tramite password** visualizzata, immettere la password e specificare l'area da includere nella restrizione di accesso. In questo modo, ogni volta che un utente del computer cercherà di eseguire le azioni selezionate dovrà immettere la password.

AUTO-DIFESA

Kaspersky PURE garantisce la protezione del computer da programmi malware e, proprio per questo, può essere esso stesso oggetto di attacchi da parte di tali programmi che cercano di bloccarne l'attività o di eliminarlo.

Per garantire l'affidabilità del sistema di protezione del computer, Kaspersky PURE include funzionalità di auto-difesa e protezione dall'accesso remoto.

Nei computer che eseguono sistemi operativi a 64 bit e Microsoft Windows Vista, la funzionalità di auto-difesa è disponibile solo per impedire la modifica o l'eliminazione dei file di Kaspersky PURE nelle unità locali e nei record del Registro di sistema.

Accade di frequente che programmi di amministrazione remota come RemoteAdmin siano necessari durante l'utilizzo della protezione da accessi remoti. Per garantire il normale funzionamento, è necessario aggiungere questi programmi all'elenco di applicazioni attendibili e abilitare l'impostazione **Non monitorare l'attività dell'applicazione** per ciascuno di essi.

Per attivare i meccanismi di auto-difesa di Kaspersky PURE, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.

2. Nella finestra visualizzata, selezionare la sezione **Auto-Difesa**. Nella sezione **Auto-Difesa** selezionare la casella ☑ **Abilita Auto-Difesa** per attivare il meccanismo di Kaspersky PURE per la protezione dalla modifica o dall'eliminazione di file su disco, processi in memoria e record del Registro di sistema.

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

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

RISPARMIO ENERGETICO PER FUNZIONAMENTO A BATTERIA

Per risparmiare energia su un computer portatile, è possibile rimandare le attività di scansione anti-virus.

Poiché sia la scansione anti-virus che l'aggiornamento richiedono una notevole quantità di risorse e di tempo, è consigliabile disabilitare l'avvio pianificato di tali attività. In questo modo si prolunga la durata della batteria. Se necessario, è possibile aggiornare Kaspersky PURE o avviare una scansione anti-virus manuale.

Per utilizzare il servizio di risparmio energetico per funzionamento a batteria, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Impostazioni** nella parte superiore.

2. Nella finestra visualizzata selezionare la sezione **Risparmio Energia**, quindi selezionare la casella ☑ **Disabilita le scansioni programmate durante l'alimentazione a batteria**.

COMPATIBILITA

In questa finestra è possibile utilizzare le seguenti funzioni avanzate di Kaspersky PURE:

- Utilizzo della tecnologia di disinfezione avanzata (vedere pagina 248).
- Rinvio dell'esecuzione dell'attività di scansione anti-virus quando comporta una rallentamento di altre applicazioni (vedere pagina 249).

TECNOLOGIA AVANZATA DI DISINFEZIONE

I programmi dannosi moderni possono invadere i livelli più bassi di un sistema operativo, rendendone praticamente impossibile l'eliminazione. Quando l'attività dannosa viene rilevata nel sistema, Kaspersky PURE consente di eseguire una procedura avanzata di disinfezione che permette di eliminare la minaccia dal computer.

Al termine di questa procedura, è necessario riavviare il computer. Dopo aver riavviato il computer, si consiglia di eseguire una scansione anti-virus completa.

Per avviare la procedura avanzata di disinfezione, eseguire le operazioni seguenti:

1. Aprire la finestra principaledell'applicazione e fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.

2. Nella finestra visualizzata, selezionare la scheda **Compatibilità** e selezionare la casella **Abilita la tecnologia avanzata di disinfezione**.

PRESTAZIONI DEL COMPUTER DURANTE L'ESECUZIONE DELLE ATTIVITA

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

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

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

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

Per posticipare l'esecuzione di un'attività di scansione anti-virus quando rallenta altri programmi:

1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.

2. Nella finestra visualizzata, selezionare la scheda **Compatibilità** e selezionare la casella **Concedi risorse alle altre applicazioni**.

SERVER PROXY

Se la connessione a Internet del computer viene stabilita tramite un server proxy, potrebbe essere necessario modificarne le impostazioni di connessione. Kaspersky PURE utilizza queste impostazioni per determinati componenti di protezione e per l'aggiornamento di database e moduli dell'applicazione.

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 delle porte monitorate" a pagina 166).

Per configurare il server proxy, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Impostazioni** nella parte superiore.

2. Nella finestra visualizzata selezionare la sezione **Server Proxy** e configurare le impostazioni di connessione.

NOTIFICHE

Durante il funzionamento di Kaspersky PURE potrebbero verificarsi diversi eventi, di carattere informativo o contenenti dati importanti. Un evento può ad esempio informare l'utente del completamento con esito positivo di un aggiornamento

dell'applicazione o registrare un errore nel funzionamento di un determinato componente che deve essere eliminato immediatamente.

Per essere aggiornati sugli eventi che si verificano durante il funzionamento di Kaspersky PURE, utilizzare il servizio di notifica.

Per impostazione predefinita, l'utente riceve la notifica degli eventi attraverso messaggi a comparsa accompagnati da un segnale acustico.

Le notifiche possono essere inviate in uno dei seguenti modi:

- Messaggi a comparsa che vengono visualizzati al di sopra dell'icona dell'applicazione nell'area di notifica.
- Messaggio audio.
- Messaggi di posta elettronica.

Per disabilitare l'invio di notifiche, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la scheda **Notifiche** e deselezionare la casella **Attiva le notifiche degli eventi**.

Anche se l'invio di notifiche è disabilitato, le informazioni sugli eventi che si verificano durante il funzionamento di Kaspersky PURE verranno registrate nel rapporto sul funzionamento dell'applicazione.

Per selezionare il metodo di invio delle notifiche, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la scheda **Notifiche** e fare clic sul pulsante **Impostazioni**.
3. Nella finestra **Notifiche** visualizzata, selezionare il metodo di invio delle notifiche.

VEDERE ANCHE:

Disabilitazione delle notifiche acustiche 250

Invio di notifiche via posta elettronica 251

DISABILITAZIONE DELLE NOTIFICHE ACUSTICHE

Per impostazione predefinita, tutte le notifiche sono accompagnate da un segnale acustico per il quale viene utilizzata la combinazione di suoni Microsoft Windows. La casella **Usa i suoni standard di Microsoft Windows** consente di scegliere una combinazione diversa. Se la casella è deselezionata, verrà utilizzata la combinazione di suoni utilizzata nelle versioni precedenti dell'applicazione.

Per disabilitare le notifiche con segnali acustici, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la sezione **Notifiche**. Nella sezione **Messaggi audio** deselezionare la casella **Attiva le notifiche acustiche**.

INVIO DI NOTIFICHE VIA POSTA ELETTRONICA

Se le notifiche devono essere inviate tramite posta elettronica, modificare le impostazioni di invio.

Per modificare le impostazioni della posta elettronica per l'invio di notifiche, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento Impostazioni nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la sezione **Notifiche**.
3. Selezionare la casella **Attiva le notifiche via e-mail** e fare clic sul pulsante **Impostazioni e-mail**.
4. Nella finestra **Impostazioni delle notifiche via e-mail** visualizzata, specificare le impostazioni di invio.

RAPPORTI

In questa sezione è possibile configurare la creazione (vedere pagina)251 e l'archiviazione di rapporti (vedere pagina 251).

REGISTRAZIONE DEGLI EVENTI NEI RAPPORTI

È possibile aggiungere al rapporto informazioni su eventi non critici, eventi del Registro di sistema e relativi al file system. Per impostazione predefinita, tali eventi non vengono registrati nei rapporti.

Per aggiungere al rapporto informazioni su eventi non critici, eventi del Registro di sistema e relativi al file system:

1. Aprire la finestra principale dell'applicazione e fare clicsul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la scheda **Rapporti** e selezionare la casella desiderata.

CANCELLAZIONE DEL CONTENUTO DEI RAPPORTI DELL'APPLICAZIONE

Le informazioni sul funzionamento di Kaspersky PURE vengono registrate nei rapporti. È possibile cancellarle.

Per cancellare i rapporti*, eseguire le operazioni seguenti*:

1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la scheda **Rapporti** e fare clic sul pulsante **Cancella**.
3. Nella finestra **Eliminazione delle informazioni dai rapporti** visualizzata selezionare le caselle relative alle categorie di rapporti di cui cancellare il contenuto.

ARCHIVIAZIONE DI RAPPORTI

È possibile determinare la durata massima di archiviazione per i rapporti di eventi (casella **Mantieni i rapporti per non più di**). Per impostazione, tale valore è uguale a 30 giorni, periodo trascorso il quale gli oggetti vengono eliminati. È possibile modificare la durata massima di archiviazione o persino eliminare eventuali limiti imposti su tale valore. È inoltre possibile specificare la dimensione massima del file del rapporto (casella **Dimensione massima del file**). Per impostazione predefinita, la dimensione massima è di 1024 MB. Una volta raggiunte le dimensioni massime, il contenuto

del file verrà sovrascritto con le nuove voci. È possibile annullare eventuali limiti impostati sulla dimensione del rapporto o immettere un altro valore.

Per configurare le impostazioni dell'archiviazione dei rapporti, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Impostazioni** nella parte superiore.

2. Nella finestra visualizzata, selezionare la scheda **Rapporti** e selezionare le caselle desiderate. Modificare la dimensione e la durata massime di archiviazione del rapporto in base alle esigenze.

COMMENTI

In tutto il mondo appaiono quotidianamente numerose nuove minacce. Per facilitare la raccolta di statistiche sui nuovi tipi di minaccia, sulle relative origini, nonché sui metodi da utilizzare per eliminarle, Kaspersky Lab consiglia l'utilizzo del servizio *Kaspersky Security Network*.

L'utilizzo di Kaspersky Security Network richiede l'invio di determinate informazioni a Kaspersky Lab, tra le quali figurano le seguenti:

- Identificatore univoco assegnato al computer dall'applicazione di Kaspersky Lab. Questo identificatore caratterizza le impostazioni hardware del computer e non contiene informazioni riservate.

- Informazioni sulle minacce identificate dai componenti dell'applicazione. La struttura e il contenuto delle informazioni dipendono dal tipo di minaccia rilevata.

- Informazioni sul sistema operativo: versione del sistema operativo, service pack installati, servizi e driver scaricati, versioni del browser e del client di posta elettronica, estensioni del browser, numero di versione dell'applicazione Kaspersky Lab installata.

Per abilitare l'invio di statistiche in Kaspersky Security Network, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clicsul collegamento **Impostazioni** nella parte superiore della finestra.

2. Nella finestra visualizzata selezionare la sezione **Feedback**, quindi selezionare la casella **Accetto di partecipare al programma Kaspersky Security Network**.

ASPETTO DELL'APPLICAZIONE

È possibile modificare l'aspetto di Kaspersky PURE creando e utilizzando diversi schemi grafici e di colori. È inoltre possibile configurare l'uso di vari elementi attivi dell'interfaccia, come l'icona dell'applicazione nell'area di notifica della barra delle applicazioni di Microsoft Windows o i messaggi a comparsa.

VEDERE ANCHE:

Elementi attivi dell'interfaccia.....252

Interfaccia di Kaspersky PURE 253

ELEMENTI ATTIVI DELL'INTERFACCIA

Per configurare le impostazioni degli elementi attivi dell'interfaccia, quali l'icona di Kaspersky PURE nell'area di notifica e i messaggi a comparsa, è possibile utilizzare le funzioni seguenti dell'applicazione:

Anima l'icona sulla barra delle applicazioni durante l'esecuzione delle attività.

L'icona dell'applicazione nell'area di notifica cambia in base all'operazione eseguita dall'applicazione. Se ad esempio è in corso la scansione di un messaggio e-mail, sullo sfondo dell'icona viene visualizzata l'immagine di una lettera. L'icona di Kaspersky Pure è animata. In tal caso, verrà indicato solo lo stato di protezione del computer: se la protezione è abilitata, l'icona è colorata. Se, invece è sospesa o disabilitata, l'icona è grigia.

Utilizzo delle finestre semi-trasparenti.

Tutte le operazioni dell'applicazione che richiedono un'attenzione immediata o una decisione dell'utente vengono presentate come messaggi a comparsa visualizzati al di sopra dell'icona dell'applicazione nell'area di notifica. Le finestre del messaggio sono trasparenti in modo da non interferire con il lavoro. La trasparenza viene persa quando si posiziona il cursore sulla finestra del messaggio.

Attiva le notifiche delle notizie.

Per impostazione predefinita, quando vengono ricevute notizie, l'area di notifica visualizza un'icona speciale che, se selezionata mediante clic, raffigura una finestra contenente la notizia.

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

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

Se l'applicazione viene installata in un computer che utilizza Microsoft Windows Vista, questa opzione non è disponibile.

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

1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la sezione **Aspetto**.
3. Nella sezione **Icona nell'area di notifica della barra delle applicazioni**, selezionare o deselezionare le caselle appropriate.

INTERFACCIA DI KASPERSKY PURE

Tutti i colori, i caratteri, le icone e gli elementi di testo utilizzati nell'interfaccia di Kaspersky PURE possono essere modificati. È possibile creare interfacce personalizzate per l'applicazione o localizzarle in un'altra lingua.

Per utilizzare un'altra interfaccia per l'applicazione, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Impostazioni** nella parte superiore.
2. Nella finestra visualizzata, selezionare la sezione **Aspetto**.
3. Selezionare la casella **Usa un'interfaccia alternativa** nella sezione **Interfacce** per attivare un'interfaccia. Specificare la cartella con le impostazioni dell'interfaccia nel campo di immissione. Per salvare la cartella, fare clic sul pulsante **Sfoglia**.

PROFILO GIOCO

L'utilizzo di alcune applicazioni in modalità schermo intero, ad esempio i giochi, potrebbe rendere necessaria la disabilitazione di determinate funzioni di Kaspersky PURE, come il servizio di notifica. Inoltre, poiché tali applicazioni richiedono una notevole quantità di risorse del sistema, l'esecuzione di alcune attività di Kaspersky PURE potrebbe rallentarne le prestazioni.

Per evitare di dover disabilitare manualmente le notifiche e sospendere le attività a ogni avvio di applicazioni a schermo intero, Kaspersky PURE include la possibilità di modificare temporaneamente le impostazioni mediante il profilo di gioco.

Tale profilo consente di modificare simultaneamente le impostazioni di tutti i componenti durante il passaggio alla modalità a schermo intero e di ripristinare le modifiche apportate una volta usciti da tale modalità.

Nel passaggio alla modalità a schermo intero, le notifiche degli eventi verranno disabilitate automaticamente. È inoltre possibile specificare le impostazioni seguenti:

- **Scegli l'azione automaticamente**. Se questa impostazione è selezionata, la selezione automatica dell'azione verrà applicata di conseguenza a tutti i componenti, anche se l'opzione **Chiedi di scegliere un'azione** è selezionata nelle rispettive impostazioni. Pertanto l'azione da eseguire sulle minacce rilevate verrà selezionata automaticamente e non verrà richiesto all'utente di farlo.

- **Non eseguire gli aggiornamenti**, **Non eseguire le attività di scansione pianificate** e **Non eseguire attività di backup**. È consigliabile utilizzare queste impostazioni per evitare di rallentare le prestazioni delle applicazioni a schermo intero.

Per abilitare il profilo di gioco, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Impostazioni** nella parte superiore.
2. Nella finestra visualizzata, selezionare la sezione **Profilo Gioco**.
3. Selezionare la casella **Usa Profilo Gioco** e specificare le impostazioni richieste.

GESTIONE DELLE IMPOSTAZIONI DELL'APPLICAZIONE

In questa finestra è possibile utilizzare le seguenti funzioni avanzate di Kaspersky PURE:

- Esportazione/importazione delle impostazioni di Kaspersky PURE (vedere pagina 254).
- Ripristino delle impostazioni predefinite di Kaspersky PURE (vedere pagina 255).

ESPORTAZIONE E IMPORTAZIONE DELLE IMPOSTAZIONI DI KASPERSKY PURE

Kaspersky PURE offre la possibilità di importare ed esportare le proprie impostazioni.

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

Per esportare le impostazioni correnti di Kaspersky PURE, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare la scheda **Gestione delle impostazioni dell'applicazione** e fare clic sul pulsante **Salva**.
3. Nella finestra visualizzata, immettere il nome del file di configurazione e il percorso in cui salvarlo.

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

1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Impostazioni** nella parte superiore.

2. Nella finestra visualizzata, selezionare la scheda **Gestione delle impostazioni dell'applicazione** e fare clic sul pulsante **Importa**.

3. Nella finestra visualizzata selezionare il file da cui si desidera importare le impostazioni di Kaspersky PURE.

RIPRISTINO DELLE IMPOSTAZIONI PREDEFINITE

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

Nella finestra visualizzata, verrà chiesto di stabilire quali impostazioni salvare durante il ripristino del livello di protezione consigliato e per quali componenti.

L'elenco mostra i componenti di Kaspersky PURE le cui impostazioni sono diverse da quelle predefinite perché modificate dall'utente o durante l'addestramento di Kaspersky PURE (Firewall o Anti-Spam). Se sono state create impostazioni speciali per uno o più componenti, anche queste verranno visualizzate nell'elenco.

Esempi di impostazioni speciali includono: liste bianche e nere di frasi e indirizzi utilizzati da Anti-Spam, elenchi di indirizzi e di numeri di telefono ISP attendibili, regole di esclusione create per i componenti dell'applicazione e regole di filtraggio delle applicazioni e dei pacchetti di Firewall.

Tali elenchi vengono creati durante l'utilizzo di Kaspersky PURE in base alle singole attività e ai requisiti di protezione. La relativa creazione può richiedere molto tempo, pertanto si consiglia di salvarli prima di ripristinare le impostazioni predefinite dell'applicazione.

Al termine della Configurazione guidata, viene impostato il livello di protezione **Consigliato** per tutti i componenti, tranne che per le impostazioni che si è deciso di mantenere personalizzate durante il ripristino. Verranno inoltre applicate le impostazioni specificate durante l'esecuzione della procedura guidata.

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

1. Aprire la finestra principaleapplicazione e fare clic sul collegamento **Impostazioni** nella parte superiore della finestra.

2. Nella finestra visualizzata, selezionare la scheda **Gestione delle impostazioni dell'applicazione** e fare clic sul pulsante **Ripristina**.

3. Nella finestra visualizzata, selezionare le caselle relative alle impostazioni da salvare. Fare clic sul pulsante **Avanti**. La Configurazione guidata dell'applicazione verrà eseguita. Seguirne le istruzioni.

NOTIFICHE

Quando si verificano eventi di runtime, vengono visualizzati messaggi di notifica speciali. A seconda della criticità dell'evento per la protezione del computer, potrebbero essere visualizzati i tipi di notifica seguenti:

- **Allarme**. Si è verificato un evento critico, ad esempio è stato rilevato un oggetto dannoso o un'attività pericolosa nel sistema. È necessario decidere subito come affrontare la minaccia. La finestra di notifica di questo tipo è di colore rosso.

- **Attenzione**. Si è verificato un evento potenzialmente pericoloso. Ad esempio, nel sistema sono stati rilevati file potenzialmente infetti o un'attività sospetta. È necessario stabilire quanto è pericolosa l'azione in questione. La finestra di notifica di questo tipo è di colore giallo.

- **Informazioni**. Questa notifica fornisce informazioni su eventi non critici. La finestra di notifica di questo tipo è di colore verde.

La finestra di notifica si compone di quattro parti:

1. *Intestazione della finestra*. L'intestazione della finestra di notifica contiene una breve descrizione dell'evento, ad esempio: richiesta di privilegi, attività sospetta, nuova rete, allarme, virus.

2. *Descrizione dell'evento*. La sezione di descrizione dell'evento visualizza informazioni dettagliate sulla ragione per cui è apparsa la notifica: nome dell'applicazione che ha causato l'evento, nome del thread rilevato, impostazioni della connessione di rete rilevata e così via.

3. *Area di selezione dell'azione*. In questa sezione è possibile selezionare una delle azioni disponibili per l'evento. Le opzioni consigliate per l'azione dipendono dal tipo di evento, ad esempio: **Disinfetta**, **Elimina**, **Ignora**: se è stato rilevato un virus, **Consenti**, **Blocca**: se l'applicazione richiede di ottenere privilegi per l'esecuzione di azioni potenzialmente dannose. L'azione consigliata dagli esperti di Kaspersky Lab verrà contraddistinta dalla dicitura "(consigliato)".

   Se si seleziona **Consenti** o **Blocca**, verrà aperta una finestra e sarà possibile selezionare la *modalità di applicazione dell'azione*. Per l'azione **Consenti** è possibile selezionare una delle modalità seguenti:

   - **Consenti sempre**. Selezionare questa opzione per consentire le attività del programma apportando modifiche alla regola di accesso del programma alle risorse di sistema.

   - **Consenti ora**. Selezionare questa opzione per applicare l'azione selezionata a tutti gli eventi analoghi rilevati durante la sessione dell'applicazione. La sessione dell'applicazione è l'intervallo tra il suo avvio e il momento in cui è stata arrestata o riavviata.

   - **Rendi attendibile**. Selezionare questa opzione per spostare l'applicazione nel gruppo **Attendibili**.

   Per l'azione **Blocca** è possibile selezionare una delle modalità seguenti:

   - **Blocca sempre**. Selezionare questa opzione per bloccare le attività del programma apportando modifiche alla regola di accesso del programma alle risorse di sistema.

   - **Blocca ora**. Selezionare questa opzione per applicare l'azione selezionata a tutti gli eventi analoghi rilevati durante la sessione dell'applicazione. La sessione dell'applicazione è l'intervallo tra il suo avvio e il momento in cui è stata arrestata o riavviata.

   - **Termina**. Selezionare questa opzione per interrompere il funzionamento del programma.

4. *Area di selezione di ulteriori azioni*. Questa sezione consente di selezionare un'azione ulteriore:

   - **Aggiungi alle esclusioni**. Se si è certi che l'oggetto rilevato non sia dannoso, si consiglia di aggiungerlo all'area attendibile per evitare che il programma rilevi falsi positivi ripetuti durante l'utilizzo dell'oggetto.

- **Applica a tutti gli oggetti**. Selezionare questa opzione per fare in modo che l'azione specificata sia applicata a tutti gli oggetti con lo stesso stato in situazioni analoghe.

IN QUESTA SEZIONE:

Impossibile disinfettare l'oggetto 257

Server degli aggiornamenti non disponibile 258

Rilevamento di un oggetto dannoso 258

Rilevamento di un oggetto pericoloso nel traffico 258

Rilevamento di un oggetto sospetto 259

Rilevamento di un'attività pericolosa nel sistema 260

Rilevamento di processi nascosti 260

Rilevamento di un tentativo di accesso al Registro di sistema 261

Rilevamento dell'attività di rete di un'applicazione 261

Rilevamento di una nuova rete 262

Rilevamento di un attacco di phishing 263

Rilevamento di un collegamento sospetto 263

Rilevamento di un certificato non valido 263

Limitazione dell'utilizzo dell'applicazione 264

Richiesta di esecuzione di una procedura speciale 264

File già esistente 264

IMPOSSIBILE DISINFETTARE L'OGGETTO

In alcuni casi può risultare impossibile disinfettare un oggetto dannoso. Questo può succedere se un file è talmente danneggiato che diventa impossibile eliminarne il codice dannoso e ripristinarne l'integrità. La procedura di disinfezione di questi casi non può essere eseguita su diversi tipi di oggetti pericolosi, ad esempio i Trojan.

In queste situazioni verrà visualizzata una notifica speciale con le informazioni seguenti:

- Il tipo di minaccia, ad esempio *virus*, *Trojan*, e il nome dell'oggetto dannoso così come è elencato nell'Enciclopedia dei Virus di Kaspersky Lab. Il nome dell'oggetto pericoloso viene specificato come collegamento al sito www.viruslist.com, in cui è possibile trovare informazioni dettagliate sul tipo di minaccia rilevata nel computer.

- Il nome completo dell'oggetto dannoso e il relativo percorso.

Viene richiesto di selezionare una delle risposte seguenti all'oggetto:

- **Elimina**: l'oggetto dannoso viene eliminato. Prima dell'eliminazione, viene creata una copia di backup dell'oggetto che potrebbe risultare utile per ripristinare l'oggetto o una descrizione della sua infezione.

- **Ignora**: l'accesso all'oggetto viene bloccato e non viene eseguita alcuna azione su di esso. Verranno semplicemente registrate informazioni sull'oggetto in un rapporto.

Successivamente sarà possibile tornare agli oggetti dannosi ignorati nella finestra del rapporto. Non sarà tuttavia possibile rimandare l'elaborazione degli oggetti rilevati nei messaggi di posta elettronica.

Per applicare l'azione selezionata a tutti gli oggetti con lo stesso stato rilevato nella sessione corrente del componente o di un'attività di protezione, selezionare la casella **Applica a tutti**. La sessione corrente corrisponde all'intervallo di tempo dall'avvio del componente fino alla relativa disabilitazione o al relativo riavvio o all'intervallo di tempo dall'inizio di un'attività di scansione anti-virus fino al relativo completamento.

SERVER DEGLI AGGIORNAMENTI NON DISPONIBILE

Se uno o più computer della rete utilizzano un server degli aggiornamenti attualmente non disponibile, è impossibile eseguire l'aggiornamento periodico di Kaspersky PURE. In questo caso, la protezione della rete è a rischio e Kaspersky PURE visualizza un messaggio per segnalare il problema nel rapporto sullo stato della protezione della rete.

Per garantire la sicurezza della rete, accendere il computer non disponibile o assegnare un'altra sorgente di aggiornamento.

RILEVAMENTO DI UN OGGETTO DANNOSO

Se Anti-Virus File, Anti-Virus Posta o una scansione anti-virus rileva un codice dannoso, viene visualizzata una notifica speciale.

Tale notifica indica:

- Il tipo di minaccia, ad esempio *virus*, *Trojan*, e il nome dell'oggetto dannoso così come è elencato nell'Enciclopedia dei Virus di Kaspersky Lab. Il nome dell'oggetto pericoloso viene specificato come collegamento al sito www.viruslist.com, in cui è possibile trovare informazioni dettagliate sul tipo di minaccia rilevata nel computer.

- Il nome completo dell'oggetto dannoso e il relativo percorso.

Viene richiesto di selezionare una delle risposte seguenti all'oggetto:

- **Disinfetta**: viene eseguito un tentativo di disinfezione dell'oggetto dannoso. Prima del trattamento, viene eseguita una copia di backup dell'oggetto che potrebbe risultare utile per ripristinare l'oggetto o una descrizione della sua infezione.

- **Elimina**: l'oggetto dannoso viene eliminato. Prima dell'eliminazione, viene creata una copia di backup dell'oggetto che potrebbe risultare utile per ripristinare l'oggetto o una descrizione della sua infezione.

- **Ignora**: l'accesso all'oggetto viene bloccato e non viene eseguita alcuna azione su di esso. Verranno semplicemente registrate informazioni sull'oggetto in un rapporto.

  Successivamente sarà possibile tornare agli oggetti dannosi ignorati nella finestra del rapporto. Non sarà tuttavia possibile rimandare l'elaborazione degli oggetti rilevati nei messaggi di posta elettronica.

Per applicare l'azione selezionata a tutti gli oggetti con lo stesso stato rilevato nella sessione corrente del componente o di un'attività di protezione, selezionare la casella **Applica a tutti**. La sessione corrente corrisponde all'intervallo di tempo dall'avvio del componente fino alla sua disabilitazione o al suo riavvio o all'intervallo di tempo dall'inizio di una scansione anti-virus fino al suo completamento.

RILEVAMENTO DI UN OGGETTO PERICOLOSO NEL TRAFFICO

Quando Anti-Virus Web rileva un oggetto dannoso nel traffico, viene visualizzata una notifica speciale.

La notifica contiene le informazioni seguenti:

- Il tipo di minaccia, ad esempio *variante virus*, e il nome dell'oggetto pericoloso così come è elencato nell'Enciclopedia dei Virus di Kaspersky Lab. Il nome dell'oggetto viene specificato come collegamento al sito www.viruslist.com, in cui è possibile trovare informazioni dettagliate sul tipo di minaccia rilevata.

- Il nome completo dell'oggetto pericoloso con il percorso della pagina Web.

Viene richiesto di selezionare una delle risposte seguenti all'oggetto:

- **Consenti**: il download dell'oggetto continua.

- **Blocca**: il download dell'oggetto dalla risorsa Web viene bloccato.

Per applicare l'azione selezionata a tutti gli oggetti con lo stesso stato rilevato nella sessione corrente del componente o di un'attività di protezione, selezionare la casella **Applica a tutti**. La sessione corrente corrisponde all'intervallo di tempo dall'avvio del componente fino alla sua disabilitazione o al suo riavvio o all'intervallo di tempo dall'inizio di una scansione anti-virus fino al suo completamento.

RILEVAMENTO DI UN OGGETTO SOSPETTO

Se Anti-Virus File, Anti-Virus Posta o una scansione anti-virus rilevano un oggetto contenente il codice di un virus sconosciuto o il codice modificato di un virus noto, viene visualizzata una notifica speciale.

Tale notifica indica:

- Il tipo di minaccia, ad esempio *virus*, *Trojan*, e il nome dell'oggetto così come è elencato nell'Enciclopedia dei Virus di Kaspersky Lab. Il nome dell'oggetto pericoloso viene specificato come collegamento al sito www.viruslist.com, in cui è possibile trovare informazioni dettagliate sul tipo di minaccia rilevata nel computer.

- Il nome completo dell'oggetto e il relativo percorso.

Viene richiesto di selezionare una delle risposte seguenti all'oggetto:

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

  Successivamente, quando si esegue la scansione della cartella Quarantena con firme delle minacce aggiornate, lo stato dell'oggetto potrebbe cambiare. L'oggetto può ad esempio essere identificato come infetto ed essere elaborato utilizzando un database aggiornato. In caso contrario, è possibile assegnare all'oggetto lo stato *non infetto* e quindi ripristinarlo.

  > Se un file viene messo in Quarantena manualmente e dopo una successiva scansione risulta non infetto, lo stato non passerà a *OK* immediatamente dopo la scansione. Questo si verificherà solo se la scansione è stata eseguita dopo un determinato intervallo di tempo (almeno tre giorni) in seguito alla messa in quarantena del file.

- **Elimina**: l'oggetto viene eliminato. Prima dell'eliminazione, viene creata una copia di backup dell'oggetto che potrebbe risultare utile per ripristinare l'oggetto o una descrizione della sua infezione.

- **Ignora**: l'accesso all'oggetto viene bloccato e non viene eseguita alcuna azione su di esso. Verranno semplicemente registrate informazioni sull'oggetto in un rapporto.

  Successivamente sarà possibile tornare agli oggetti ignorati nella finestra del rapporto. Non sarà tuttavia possibile rimandare l'elaborazione degli oggetti rilevati nei messaggi di posta elettronica.

Per applicare l'azione selezionata a tutti gli oggetti con lo stesso stato rilevato nella sessione corrente del componente o di un'attività di protezione, selezionare la casella **Applica a tutti**. La sessione corrente corrisponde all'intervallo di tempo dall'avvio del componente fino alla sua disabilitazione o al suo riavvio o all'intervallo di tempo dall'inizio di una scansione anti-virus fino al suo completamento.

Se si è certi che l'oggetto rilevato non sia dannoso, si consiglia di aggiungerlo all'area attendibile per evitare che il programma rilevi falsi positivi ripetuti durante l'utilizzo dell'oggetto.

RILEVAMENTO DI UN'ATTIVITA PERICOLOSA NEL SISTEMA

Quando Difesa Proattiva rileva nel sistema un'attività pericolosa dell'applicazione, viene visualizzata una notifica speciale con le informazioni seguenti:

- Il nome della minaccia così come è elencata nell'Enciclopedia dei Virus di Kaspersky Lab. Il nome della minaccia viene specificato come collegamento al sito www.viruslist.com, in cui è possibile trovare informazioni dettagliate sul tipo di minaccia rilevata.
- Il nome completo del file del processo che ha avviato l'attività pericolosa e il relativo percorso.
- Risposte possibili:
  - **Quarantena**: il processo viene arrestato e il file eseguibile viene messo in quarantena. Quando un oggetto viene messo in Quarantena, viene solo spostato, non copiato. I file in Quarantena vengono salvati in un formato speciale e non sono pericolosi.

    Successivamente, quando si esegue la scansione della cartella Quarantena con firme delle minacce aggiornate, lo stato dell'oggetto potrebbe cambiare. L'oggetto può ad esempio essere identificato come infetto ed essere elaborato utilizzando un database aggiornato. In caso contrario, è possibile assegnare all'oggetto lo stato *non infetto* e quindi ripristinarlo.

    Se un file viene messo in Quarantena manualmente e dopo una successiva scansione risulta non infetto, lo stato non passerà a *OK* immediatamente dopo la scansione. Questo si verificherà solo se la scansione è stata eseguita dopo un determinato intervallo di tempo (almeno tre giorni) in seguito alla messa in quarantena del file.
  - **Termina**: arresta il processo.
  - **Consenti**: consente l'esecuzione del processo.

Per applicare l'azione selezionata a tutti gli oggetti con lo stesso stato rilevato nella sessione corrente del componente o di un'attività di protezione, selezionare la casella **Applica a tutti**. La sessione corrente corrisponde all'intervallo di tempo dall'avvio del componente fino alla sua disabilitazione o al suo riavvio o all'intervallo di tempo dall'inizio di una scansione anti-virus fino al suo completamento.

Se si è certi che il programma rilevato non sia pericoloso, si consiglia di aggiungerlo all'area attendibile per evitare che Protezione del computer generi falsi positivi ripetuti quando lo rileva.

RILEVAMENTO DI PROCESSI NASCOSTI

Quando Difesa Proattiva rileva nel sistema un'attività nascosta, viene visualizzata una notifica speciale con le informazioni seguenti:

- Il nome della minaccia così come è elencata nell'Enciclopedia dei Virus di Kaspersky Lab. Il nome della minaccia viene specificato come collegamento al sito www.viruslist.com, in cui è possibile trovare informazioni dettagliate sul tipo di minaccia rilevata.
- Il nome completo del file del processo nascosto e il relativo percorso.
- Risposte possibili:
  - **Quarantena**: il file eseguibile del processo viene messo in quarantena. Quando un oggetto viene messo in Quarantena, viene solo spostato, non copiato. I file in Quarantena vengono salvati in un formato speciale e non sono pericolosi.

Successivamente, quando si esegue la scansione della cartella Quarantena con firme delle minacce aggiornate, lo stato dell'oggetto potrebbe cambiare. L'oggetto può ad esempio essere identificato come infetto ed essere elaborato utilizzando un database aggiornato. In caso contrario, è possibile assegnare all'oggetto lo stato *non infetto* e quindi ripristinarlo.

Se un file viene messo in Quarantena manualmente e dopo una successiva scansione risulta non infetto, lo stato non passerà a *OK* immediatamente dopo la scansione. Questo si verificherà solo se la scansione è stata eseguita dopo un determinato intervallo di tempo (almeno tre giorni) in seguito alla messa in quarantena del file.

- **Termina**: arresta il processo.
- **Consenti**: consente l'esecuzione del processo.

Per applicare l'azione selezionata a tutti gli oggetti con lo stesso stato rilevato nella sessione corrente del componente o di un'attività di protezione, selezionare la casella **Applica a tutti**. La sessione corrente corrisponde all'intervallo di tempo dall'avvio del componente fino alla sua disabilitazione o al suo riavvio o all'intervallo di tempo dall'inizio di una scansione anti-virus fino al suo completamento.

Se si è certi che il programma rilevato non sia pericoloso, si consiglia di aggiungerlo all'area attendibile per evitare che Protezione del computer generi falsi positivi ripetuti quando lo rileva.

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 speciale con le informazioni seguenti:

- La chiave del Registro di sistema alla quale si sta tentando di accedere.
- Il nome completo del file del processo che ha avviato il tentativo di accesso alle chiavi del Registro di sistema e il relativo percorso.
- Risposte possibili:
  - **Consenti**: l'esecuzione dell'azione pericolosa viene consentita una volta;
  - **Blocca**: l'azione pericolosa viene bloccata una volta.

Per eseguire l'azione selezionata automaticamente ogni volta che l'attività viene avviata nel computer, 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.

RILEVAMENTO DELL'ATTIVITA DI RETE DI UN'APPLICAZIONE

Se vengono rilevate attività di rete di un'applicazione (opzione predefinita per le applicazioni incluse nel gruppo **Restrizione bassa** o **Restrizione alta**) (vedere la sezione "Gruppi di applicazioni" a pagina 82), sullo schermo viene visualizzata una notifica.

La notifica viene visualizzata se Protezione del computer viene eseguito in modalità interattiva (vedere la sezione "Utilizzo della modalità di protezione interattiva" a pagina 152), e se non sono state create regole per i pacchetti per l'applicazione di cui è stata rilevata attività di rete (vedere pagina 97).

La notifica contiene le informazioni seguenti:

- *Descrizione dell'attività*: nome dell'applicazione e funzionalità generali della connessione che essa avvia. In genere, vengono specificati il tipo di connessione, la porta locale da cui è stata avviata, la porta remota e l'indirizzo di connessione.
- *Sequenza di avvio dell'applicazione*.
- *Azione*: serie di operazioni che Protezione del computer deve eseguire per l'attività di rete rilevata.

Viene richiesto di selezionare una delle azioni seguenti:

- **Consenti**.
- **Nega**.
- **Crea una regola**. Quando viene selezionata questa opzione, viene avviata la *Creazione guidata regole* (vedere pagina 98), che guida l'utente nella creazione di una regola che controlla l'attività di rete dell'applicazione.

È possibile:

- Eseguire un'azione una sola volta. A tal fine, selezionare **Consenti** o **Nega**.
- Applicare un'azione alla sessione dell'applicazione di cui è stata rilevata attività di rete. A tal fine, selezionare **Consenti** o **Nega** e selezionare la casella **Applica alla sessione corrente**.
- Applicare l'azione selezionata per l'applicazione a tutte le sessioni. A tal fine, selezionare **Consenti** o **Nega** e selezionare la casella **Applica in modo definitivo**.
- Creare una regola per la gestione dell'attività di rete di un'applicazione. A tal fine, selezionare **Crea una regola**.

RILEVAMENTO DI UNA NUOVA RETE

Ogni volta che il computer si connette a una nuova area, ad esempio una rete, viene visualizzata una notifica speciale.

La parte superiore della notifica contiene una breve descrizione della rete, che specifica l'indirizzo IP e la maschera di sottorete.

Nella parte inferiore della finestra viene richiesto di assegnare uno stato all'area e l'attività di rete viene consentita in base a tale stato:

- **Rete pubblica (blocca l'accesso esterno al computer)**. Una rete ad alto rischio in cui il computer è esposto a qualsiasi tipo di minaccia. Si consiglia di selezionare questo stato per le reti non protette da applicazioni anti-virus, firewall, filtri e così via. Quando si seleziona questo stato, il programma garantisce la protezione massima per l'area in questione.
- **Rete locale (consente l'accesso a file e stampanti)**. Questo stato è consigliabile per le aree con un fattore di rischio medio, ad esempio le reti LAN aziendali.
- **Rete attendibile (consente qualsiasi attività di rete)**. Si consiglia di applicare questo stato alle aree che si ritiene siano assolutamente sicure e in cui il computer non è soggetto ad attacchi e tentativi di accesso ai dati.

RILEVAMENTO DI UN ATTACCO DI PHISHING

Ogni volta che Protezione del computer rileva un attacco di phishing, viene visualizzata una notifica speciale.

La notifica contiene le informazioni seguenti:

- Il nome della minaccia (*attacco di phishing*) come collegamento all'Enciclopedia dei Virus di Kaspersky Lab con una panoramica dettagliata della minaccia stessa.
- L'indirizzo Web dell'attacco di phishing.
- Risposte possibili:
  - **Consenti**: il download del sito di phishing continua.
  - **Blocca**: il download del sito di phishing viene bloccato.

Per applicare l'azione selezionata a tutti gli oggetti con lo stesso stato rilevato nella sessione corrente del componente o di un'attività di protezione, selezionare la casella **Applica a tutti**. La sessione corrente corrisponde all'intervallo di tempo dall'avvio del componente fino alla sua disabilitazione o al suo riavvio o all'intervallo di tempo dall'inizio di una scansione anti-virus fino al suo completamento.

RILEVAMENTO DI UN COLLEGAMENTO SOSPETTO

Ogni volta che Protezione del computer rileva un tentativo di apertura di un sito Web il cui indirizzo è contenuto nell'elenco di indirizzi Web sospetti, viene visualizzata una notifica speciale a comparsa.

La notifica contiene le informazioni seguenti:

- Indirizzo del sito Web.
- Risposte possibili:
  - **Consenti**: il download dal sito Web continua.
  - **Blocca**: il download dal sito Web viene bloccato.

Per applicare l'azione selezionata a tutti gli oggetti con lo stesso stato rilevato nella sessione corrente del componente o di un'attività di protezione, selezionare la casella **Applica a tutti**. La sessione corrente corrisponde all'intervallo di tempo dall'avvio del componente fino alla sua disabilitazione o al suo riavvio o all'intervallo di tempo dall'inizio di una scansione anti-virus fino al suo completamento.

RILEVAMENTO DI UN CERTIFICATO NON VALIDO

Il controllo di protezione per la connessione mediante il protocollo SSL viene eseguito utilizzando il 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 conterrà le informazioni sulla possibile causa dell'errore e identificherà l'indirizzo e la porta remoti. Verrà richiesto di decidere se continuare o meno la connessione con un certificato non valido:

- **Accetta certificato**: la connessione al sito Web continua;
- **Nega certificato**: la connessione al sito Web viene interrotta;
- **Visualizza certificato**: vengono visualizzate informazioni sul certificato.

LIMITAZIONE DELL'UTILIZZO DELL'APPLICAZIONE

Se in Parental Control è stata specificata una restrizione temporale per l'utilizzo dell'applicazione, una volta scaduto il tempo specificato viene visualizzata una speciale notifica.

Nella notifica sono visualizzate le seguenti informazioni:

- nome dell'applicazione;
- tempo restante prima della chiusura dell'applicazione o motivo della chiusura dell'applicazione.

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 visualizzato un messaggio per richiedere l'esecuzione di una speciale procedura avanzata di disinfezione.

Gli specialisti di Kaspersky Lab consigliano di accettare l'esecuzione di tale procedura avanzata. A tale scopo, fare clic sul pulsante **OK**. Tenere presente, tuttavia, che il computer verrà riavviato al termine della procedura e pertanto si consiglia di salvare il lavoro corrente e chiudere tutte le applicazioni prima di eseguire la procedura.

Durante l'esecuzione della procedura di disinfezione, non è possibile avviare sessioni di modifica del Registro del sistema operativo o del client di posta. Dopo aver riavviato il computer, si consiglia di eseguire una scansione anti-virus completa.

FILE GIA ESISTENTE

Se durante il ripristino di un file dalla copia di backup esiste già un file con lo stesso nome nella cartella selezionata, viene visualizzata una speciale notifica.

Nella parte superiore della finestra di notifica sono specificati il nome e il percorso del file.

Nella parte inferiore della finestra viene richiesto di specificare il metodo di ripristino del file:

- **Sostituisci**. Il file di cui è in corso il ripristino sostituirà il file esistente.
- **Ignora**. Verrà salvata la versione corrente del file.
- **Salva entrambi i file**. Al file di cui è in corso il ripristino verrà assegnato un altro nome.

ELIMINAZIONE DEI PROBLEMI

Se si sono verificati problemi durante l'utilizzo di Kaspersky PURE, il modo più immediato per risolverli è utilizzare la Guida o la Knowledge Base di Kaspersky Lab all'indirizzo http://support.kaspersky.com. La *Knowledge Base* è una sezione apposita del sito Web del Supporto tecnico di Kaspersky Lab che contiene i consigli per i prodotti Kaspersky Lab e le risposte alle domande più frequenti. Si può provare a trovare una risposta alla propria domanda o una soluzione al proprio problema utilizzando questa risorsa.

Per accedere alla Knowledge Base:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte inferiore della finestra, fare clic sul collegamento **Assistenza**.
3. Nella finestra **Assistenza** visualizzata, fare clic sul collegamento **Knowledge Base**.

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

Pr aprire il forum degli utenti:

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

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

IN QUESTA SEZIONE:

Creazione di un rapporto sullo stato del sistema 265

Invio di file di dati 266

Esecuzione di script AVZ 267

Creazione di un file di traccia 267

CREAZIONE DI UN RAPPORTO SULLO STATO DEL SISTEMA

Per risolvere i problemi dell'utente, gli specialisti di Kaspersky Lab potrebbero aver bisogno di un rapporto sullo stato del sistema. Tale rapporto contiene informazioni dettagliate sui processi in esecuzione, i moduli e i driver caricati, i plug-in di Microsoft Internet Explorer e Microsoft Windows Explorer, le porte aperte, gli oggetti sospetti rilevati e così via.

Quando viene creato un rapporto sullo stato del sistema, non vengono raccolte informazioni personali dell'utente.

Per creare un rapporto sullo stato del sistema:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte inferiore della finestra, fare clic sul collegamento **Assistenza**.

3. Nella finestra **Assistenza** visualizzata, fare clic sul collegamento **Strumenti di assistenza**.

4. Nella finestra **Informazioni per il servizio di Assistenza tecnica** visualizzata, fare clic 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*. Una volta terminato il processo di raccolta delle informazioni, è possibile visualizzare il rapporto.

Per visualizzare il rapporto:

1. Aprire la finestra principaledell'applicazione.

2. Nella parte inferiore della finestra, fare clic sul collegamento **Assistenza**.

3. Nella finestra **Assistenza** visualizzata, fare clic sul collegamento **Strumenti di assistenza**.

4. Nella finestra **Informazioni per il servizio di Assistenza tecnica** visualizzata, fare clic sul pulsante **Visualizza**.

5. Aprire l'archivio *sysinfo.zip*, contenente i file del rapporto.

INVIO DI 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 dell'Assistenza tecnica, sarà necessario fornire un numero di richiesta. Tale numero è disponibile nella Pagina Personale del sito Web 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. Nella parte inferiore della finestra, fare clic sul collegamento **Assistenza**.

3. Nella finestra **Assistenza** visualizzata, fare clic sul collegamento **Strumenti di assistenza**.

4. Nella finestra **Informazioni per il servizio di Assistenza tecnica** visualizzata, sezione **Azioni**, fare clic sul pulsante **Invia informazioni sul sistema al servizio di Assistenza**.

5. Nella finestra visualizzata, selezionare le caselle accanto ai file di traccia che si desidera inviare al servizio di Assistenza tecnica e fare clic sul pulsante **Invia**.

6. Nella finestra **Inserire il numero della richiesta** visualizzata, specificare il numero assegnato alla richiesta durante il completamento del modulo elettronico nel sito Web del servizio di assistenza.

I file di traccia selezionati verranno compressi e inviati al server del servizio di Assistenza tecnica.

Se per qualsiasi motivo non si riesce a contattare l'Assistenza tecnica, è possibile salvare i file di dati nel computer.

Per salvare i file di dati su disco:

1. Aprire la finestra principale dell'applicazione.

2. Nella parte inferiore della finestra, fare clic sul collegamento **Assistenza**.

3. Nella finestra **Assistenza** visualizzata, fare clic sul collegamento **Strumenti di assistenza**.

4. Nella finestra **Informazioni per il servizio di Assistenza tecnica** visualizzata, sezione **Azioni**, fare clic sul pulsante **Invia informazioni sul sistema al servizio di Assistenza**.

5. Nella finestra visualizzata, selezionare le caselle accanto ai file di traccia che si desidera inviare al servizio di Assistenza tecnica e fare clic sul pulsante **Invia**.

6. Nella finestra **Inserire il numero della richiesta** visualizzata, fare clic sul pulsante **Annulla** e confermare il salvataggio dei file sul disco.

7. Nella finestra che viene visualizzata specificare il nome dell'archivio.

Successivamente, sarà possibile inviare i file salvati all'Assistenza tecnica con l'aiuto della Pagina personale (https://support.kaspersky.com/en/personalcabinet?LANG=it).

ESECUZIONE DI SCRIPT AVZ

Gli esperti di Kaspersky Lab analizzeranno il problema rilevato dall'utente utilizzando i file di traccia e il rapporto sullo stato del sistema ricevuti. Il risultato dell'analisi è una sequenza di azioni mirate a eliminare i problemi rilevati. L'elenco di azioni può essere piuttosto lungo.

Per semplificare la procedura, si utilizzano script AVZ. Uno script AVZ è un insieme di istruzioni che consentono di modificare le chiavi di registro, mettere in quarantena i file, ricercare classi di file e in alcuni casi metterne in quarantena i file a esse correlati, bloccare gli intercettori UserMode e KernelMode e così via.

Per eseguire gli script, l'applicazione include una *procedura guidata per l'esecuzione di script AVZ*. La procedura guidata è costituita da una serie di schermate (passaggi) tra le quali è possibile spostarsi servendosi dei pulsanti **Avanti** e **Indietro**. Per chiudere la procedura guidata al completamento, utilizzare il pulsante **Fine**. Per interrompere la procedura in qualsiasi momento, utilizzare il pulsante **Annulla**.

Non è consigliabile modificare il testo dello script AVZ ricevuto dagli esperti di Kaspersky Lab. Se il problema si verifica durante l'esecuzione dello script, contattare il servizio di Assistenza tecnica.

➡ *Per avviare la procedura guidata:*

1. Aprire la finestra principale dell'applicazione.

2. Nella parte inferiore della finestra, fare clic sul collegamento **Assistenza**.

3. Nella finestra **Assistenza** visualizzata, fare clic sul collegamento **Strumenti di assistenza** nella parte inferiore della finestra.

4. Nella finestra **Informazioni per il servizio di Assistenza tecnica** visualizzata, fare clic 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 il messaggio di errore corrispondente.

CREAZIONE DI UN FILE DI TRACCIA

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

Per creare il file di traccia:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte inferiore della finestra, fare clic sul collegamento **Assistenza**.
3. Nella finestra **Assistenza** visualizzata, fare clic sul collegamento **Strumenti di assistenza**.
4. Nella finestra **Informazioni per il servizio di Assistenza tecnica** visualizzata, utilizzare l'elenco a discesa nella sezione **Tracce** per selezionare il livello di traccia. Tale livello deve essere impostato in base alle indicazioni dello specialista dell'Assistenza tecnica. In assenza di indicazioni da parte dell'Assistenza tecnica, si consiglia di utilizzare il livello di traccia **500**.
5. Per iniziare il processo di creazione di una traccia, fare clic sul pulsante **Abilita**.
6. Riprodurre la situazione che ha causato il problema.
7. Per arrestare il processo di creazione della traccia, fare clic sul pulsante **Disabilita**.

È quindi possibile passare al caricamento dei risultati della traccia sul server di Kaspersky Lab.

COME CONTATTARE IL SERVIZIO DI ASSISTENZA TECNICA

Una volta acquistato Kaspersky PURE, è possibile ottenere tutte le informazioni desiderate dal servizio di assistenza tecnica telefonicamente o via Internet.

Gli specialisti dell'Assistenza tecnica chiariranno tutti i dubbi sull'installazione e sull'utilizzo dell'applicazione e forniranno consigli preziosi per risolvere i problemi causati dalle attività del malware qualora il computer sia stato infettato.

Prima di contattare il servizio di Assistenza tecnica, consultare le regole dell'Assistenza tecnica (http://support.kaspersky.com/it/support/rules).

Richiesta al servizio di assistenza tecnica via posta elettronica

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

Il servizio di assistenza tecnica risponderà alla richiesta all'account personale Kaspersky (https://my.kaspersky.com/en/index.html?LANG=it) e all'indirizzo di posta elettronica specificato nella richiesta.

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

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

Assistenza tecnica telefonica

Per sottoporre un problema urgente, è possibile contattare telefonicamente il servizio di Assistenza tecnica locale al numero +7 (495) 663-81-47. Prima di contattare gli esperti dell'Assistenza tecnica, raccogliere informazioni (http://support.kaspersky.com/it/support/details) sulla configurazione del computer e sul software anti-virus installato. Ciò consentirà agli esperti di fornire assistenza più rapidamente.

INFORMATIVA SULLA RACCOLTA DATI PER KASPERSKY SECURITY NETWORK

A. INTRODUZIONE

Leggere attentamente il presente documento. In quanto contiene informazioni utili per poter continuare a utilizzare i servizi o il software messi a disposizione da Kaspersky Lab. L'uso prolungato dei suddetti servizi e del software comporta l'accettazione delle condizioni illustrate nella presente informativa sulla raccolta dei dati. Kaspersky Lab si riserva il diritto di modificare l'Informativa sulla raccolta dei dati in qualsiasi momento e di comunicare gli eventuali cambiamenti in questa pagina. La data di revisione riportata in basso consente di determinare se sono state apportate modifiche dall'ultima consultazione del documento. L'uso prolungato dei servizi Kaspersky Lab a seguito della pubblicazione degli aggiornamenti dell'Informativa sulla raccolta dei dati costituisce implicita accettazione delle modifiche apportate.

L'obiettivo della presente Informativa sulla raccolta dei dati creata da Kaspersky Lab e relativi consociati (collettivamente definiti "Kaspersky Lab") è di informare l'utente sulle pratiche di raccolta e diffusione dei dati adottate per il prodotto Kaspersky PURE.

Gli impegni assunti da Kaspersky Lab

L'impegno costante di Kaspersky Lab nell'offerta di un servizio qualitativamente elevato a tutti i clienti si concentra soprattutto sulle procedure di raccolta dei dati. Per rispondere a tutte le domande e fugare gli eventuali dubbi che potrebbero sorgere relativamente alle procedure adottate dal servizio Kaspersky Security Network per la raccolta dei dati, è stata creata la presente "Informativa sulla raccolta dei dati" (definita anche semplicemente "Informativa").

In questo documento vengono descritte, in termini generali e con numerosi dettagli tecnici, tutte le precauzioni adottate per garantire un corretto uso dei dati raccolti. L'organizzazione dei contenuti per procedure e aree principali facilita una rapida identificazione e lettura delle informazioni desiderate. L'obiettivo primario di Kaspersky Lab è di soddisfare le esigenze e le aspettative dei propri clienti e la protezione dei dati raccolti rappresenta uno degli impegni prioritari.

La raccolta dei dati e delle informazioni viene effettuata direttamente da Kaspersky Lab. Per domande o dubbi sul contenuto dell'Informativa, inviare un messaggio e-mail all'indirizzo support@kaspersky.com.

Kaspersky Security Network

Il servizio Kaspersky Security Network consente agli utenti dei prodotti per la protezione Kaspersky Lab di tutto il mondo di identificare più facilmente i rischi sempre più numerosi e di ridurre il tempo necessario per garantire la protezione del computer. Per identificare le nuove minacce e le relative fonti e migliorare la protezione dell'utente e le funzionalità del prodotto, Kaspersky Security Network raccoglie dati selezionati sulla protezione e sull'applicazione e li invia a Kaspersky Lab per l'analisi. Tali informazioni non contengono dati che consentono l'identificazione personale dell'utente e vengono utilizzate da Kaspersky Lab al solo scopo di migliorare i prodotti per la protezione e perfezionare le soluzioni sviluppate per contrastare minacce e virus. Qualora si verifichi una trasmissione accidentale di dati personali dell'utente, Kaspersky Lab adotterà tutte le misure di protezione necessarie, in conformità con quanto sancito nella presente Informativa.

Partecipando a Kaspersky Security Network, tutti gli utenti dei prodotti per la protezione Kaspersky Lab in tutto il mondo contribuiscono in modo significativo al miglioramento della sicurezza di Internet.

Aspetti legali

Kaspersky Security Network può essere soggetto a diverse giurisdizioni, inclusa quella degli Stati Uniti d'America, a seconda del paese in cui vengono utilizzati i servizi. Kaspersky Lab divulgherà le informazioni personali senza previa notifica se richiesto per legge o nella ferma convinzione che tale azione sia necessaria per approfondire la natura di determinate attività dannose o proteggere dalle stesse ospiti, visitatori, associati Kaspersky Lab o altri utenti. Come descritto in precedenza, la legislazione relativa ai dati e alle informazioni raccolte da Kaspersky Security Network può variare da paese a paese. Ad esempio, alcune informazioni che consentono l'identificazione personale raccolte nell'Unione Europea e negli Stati membri sono soggette alle Direttive relative a dati personali, privacy e comunicazioni elettroniche, incluse, a titolo esemplificativo, la Direttiva 2002/58/CE del Parlamento Europeo e del Consiglio del 12 luglio 2002 relativa all'elaborazione dei dati personali e alla protezione della privacy nel settore delle comunicazioni elettroniche

e la Direttiva 95/46/CE del Parlamento Europeo e del Consiglio del 24 ottobre 1995 sulla protezione degli individui con riferimento all'elaborazione dei dati personali e alla libera circolazione di tali dati e alla successiva legislazione adottata negli Stati membri dell'Unione Europea, la decisione della Commissione Europea 497/2001/CE sulle clausole contrattuali-tipo (trasferimento di dati personali verso paesi terzi) e la legislazione successiva adottata negli Stati membri.

Kaspersky Security Network avviserà gli utenti interessati, durante la raccolta iniziale delle informazioni appena descritte, dell'eventuale condivisione di tali informazioni, soprattutto se è previsto un impiego per uno sviluppo commerciale e offrirà a tali utenti Internet la possibilità di accettare (negli Stati membri dell'Unione Europea e in altri paesi che richiedono la procedura di opt-in) o di rinunciare (per tutti gli altri paesi) online all'uso commerciale di tali dati e/o la trasmissione degli stessi a terze parti.

Kaspersky Lab potrebbe essere obbligata per legge o da autorità giudiziarie a fornire alcune informazioni che consentono l'identificazione personale agli enti governativi appropriati. Nei casi sopra citati, tali informazioni verranno fornite previa ricezione della documentazione appropriata. Kaspersky Lab potrebbe anche essere tenuta per legge a fornire informazioni per proteggere la proprietà oltre che il benessere e la sicurezza degli individui.

Le dichiarazioni alle autorità degli Stati membri per la protezione dei dati personali verranno effettuate in base alla legislazione successiva degli Stati membri dell'Unione Europea in vigore. Le informazioni su tali dichiarazioni saranno accessibili nei servizi Kaspersky Security Network.

B. INFORMAZIONI RACCOLTE

Tipologie di dati raccolti

Gli utenti hanno il diritto di concedere i dati in base alla presente informativa. Il servizio Kaspersky Security Network raccoglie e invia a Kaspersky Lab due categorie di dati sui rischi di protezione potenziali che minacciano il computer, ovvero:

- Dati principali:
    - informazioni sul software e l'hardware installato sul computer, compreso il sistema operativo ed i service pack installati, gli oggetti kernel, i driver, i servizi, le estensioni di Internet Explorer, le estensioni del sistema di stampa, le estensioni di Esplora risorse, i programmi scaricati, elementi di impostazione attivi, gli applet del pannello di controllo, le voci del file Host e del registro, gli indirizzi IP, i tipi di browser, i client di posta elettronica ed il numero di versione dei prodotti di Kaspersky Lab, che sono di solito informazioni non personalmente identificabili.
    - una ID univoca generata dal prodotto di Kaspersky Lab per identificare le singole macchine senza identificare l'utente, che non contiene informazioni personali.
    - informazioni sullo stato della protezione anti-virus del computer, e dati su qualsiasi file o attività per cui esista il sospetto di programma nocivo (es. nome virus, data/ora di rilevamento, nomi/percorsi e dimensione dei file infetti, IP e porta dell'attacco di rete, nome dell'applicazione sospettata di essere nociva). Tenere presente che i dati raccolti appena descritti non contengono informazioni che consentono l'identificazione personale.
- Dati estesi:
    - informazioni sulle applicazioni firmate digitalmente scaricate dell'utente (URL, dimensione file, nome firmatario);
    - informazioni sulle applicazioni eseguibili (dimensioni, attributi, data di creazione, informazioni sulle intestazioni PE, regione, nome, ubicazione e utilità di compressione utilizzata).
- File e/o loro parti. Il servizio Kaspersky Security Network può raccogliere e inviare file interi e/o loro parti a Kaspersky Lab per sottoporli a un'ulteriore analisi. I trasferimenti di file e/o loro parti vengono eseguiti solo se l'Informativa sulla raccolta dei dati di Kaspersky Lab è stata accettata dall'utente.

Protezione della trasmissione e dell'archiviazione dei dati

Kaspersky Lab garantisce la protezione delle informazioni che raccoglie. Le informazioni raccolte vengono archiviate in server con accesso limitato e controllato. Kaspersky Lab gestisce reti di dati protette da firewall standard del settore e sistemi con password di protezione. Utilizza inoltre una vasta gamma di procedure e tecnologie di protezione delle informazioni raccolte da minacce come l'uso, la divulgazione o accessi non autorizzati. I criteri di protezione vengono periodicamente aggiornati e migliorati se necessario e solo le persone autorizzate possono accedere ai dati raccolti. Kaspersky Lab adotta tutte le misure necessarie per garantire che le informazioni vengano gestite all'insegna della protezione e in conformità con la presente Informativa. Sfortunatamente, nessuna trasmissione di dati può essere considerata sicura al 100%. Di conseguenza, sebbene il nostro impegno nella protezione dei dati sia molto forte, non è possibile garantire la protezione completa dei dati trasmessi dall'utente o derivanti dai prodotti o dai servizi, incluso il programma Kaspersky Security Network, e tutti questi servizi vengono utilizzati a rischio dell'utente.

I dati raccolti possono essere trasferiti nei server di Kaspersky Lab e Kaspersky Lab ha adottato tutte le precauzioni necessarie per garantire che le informazioni raccolte, se trasferite, ricevano un livello appropriato di protezione. I dati raccolti vengono considerati informazioni riservate e in quanto tali sono soggetti alle procedure di sicurezza e ai criteri aziendali relativi alla protezione e all'uso di informazioni riservate. Una volta giunti presso Kaspersky Lab, i dati raccolti vengono archiviati in un server con caratteristiche di sicurezza fisiche ed elettroniche standard del settore, incluso l'utilizzo di procedure di accesso/password e firewall elettronici progettati per bloccare l'accesso non autorizzato dall'esterno di Kaspersky Lab. I dati raccolti da Kaspersky Security Network descritti nella presente Informativa vengono elaborati e archiviati negli Stati Uniti e in altre giurisdizioni e in altri paesi in cui Kaspersky Lab ha interessi commerciali. Tutti i dipendenti Kaspersky Lab sono a conoscenza dei criteri di protezione. I dati forniti dagli utenti sono accessibili solo ai dipendenti che ne prendono visione per svolgere il proprio lavoro. Tutti i dati archiviati non verranno associati a informazioni che consentono l'identificazione personale. Kaspersky Lab non combina i dati archiviati da Kaspersky Security Network ad altri dati, elenchi di contatti o informazioni sull'abbonamento raccolti da Kaspersky Lab a scopo promozionale o per altre finalità.

C. USO DEI DATI RACCOLTI

Uso dei dati personali

Kaspersky Lab raccoglie i dati per analizzare e identificare la fonte dei rischi potenziali della protezione e per migliorare la capacità dei prodotti di Kaspersky Lab di rilevare comportamenti dannosi, siti Web fraudolenti, crimeware e altri tipi di minacce alla protezione di Internet per offrire il miglior livello possibile di protezione ai clienti Kaspersky Lab nel futuro.

Diffusione delle informazioni a terze parti

Kaspersky Lab può divulgare le informazioni raccolte per legge o in risposta a una citazione in giudizio o a un altro processo legale o nella ferma convinzione che tale azione sia necessaria per ottemperare a un obbligo di legge, rispondere a una citazione in giudizio o a un altro processo legale o richiesta governativa. Kaspersky Lab può inoltre diffondere informazioni che consentono l'identificazione personale nei casi in cui ritenga che tali informazioni siano necessarie per identificare, contattare o avviare un'azione legale contro chiunque violi tale Informativa, i termini degli accordi con la società o per proteggere la sicurezza degli utenti e gli accordi pubblici o di riservatezza con determinate terze parti che collaborano con Kaspersky nello sviluppo e nella gestione di Kaspersky Security Network. Per favorire la consapevolezza, il rilevamento e la prevenzione dei rischi della protezione di Internet, Kaspersky Lab può condividere determinate informazioni con organizzazioni di ricerca e altri fornitori di software per la protezione. Può altresì utilizzare le statistiche derivate dalle informazioni raccolte per registrare e pubblicare rapporti sulle tendenze dei rischi della protezione.

Opzioni disponibili all'utente

La partecipazione al programma Kaspersky Security Network è facoltativa. È possibile attivare e disattivare il servizio Kaspersky Security Network in qualsiasi momento modificando le impostazioni Feedback nella pagina delle opzioni del prodotto Kaspersky Lab in uso. È tuttavia importante ricordare che se si sceglie di disattivare il servizio Kaspersky Security Network, potrebbe non essere possibile offrire alcuni dei servizi dipendenti dalla raccolta dei dati. Al termine del periodo di validità del prodotto Kaspersky Lab, alcune funzioni del software Kaspersky Lab potrebbero essere ancora attive, ma le informazioni non verranno più inviate automaticamente a Kaspersky Lab.

Kaspersky Lab si riserva anche il diritto di inviare messaggi di avviso occasionali agli utenti per informarli di modifiche specifiche che potrebbero influire sulla propria capacità di utilizzare i servizi per i quali è stato sottoscritto un abbonamento. Si riserva inoltre il diritto di contattare gli utenti se obbligata nell'ambito di un procedimento legale o se si è verificata una violazione di un accordo di licenza, garanzia o acquisto.

Kaspersky Lab mantiene tali diritti in quanto in casi limitati potrebbe essere necessario contattare l'utente per un obbligo di legge o per discutere di questioni importanti per l'utente stesso. Tali diritti non consentono di contattare l'utente per la promozione e la vendita di prodotti nuovi o esistenti in assenza di un consenso esplicito e l'invio di questi tipi di comunicazioni è raro.

D. RACCOLTA DEI DATI – DOMANDE E RECLAMI CORRELATI

Kaspersky Lab gestisce ed esamina con il massimo rispetto e la più grande attenzione le perplessità dei clienti sulla raccolta dei dati. Per segnalare un caso di mancata conformità alla presente Informativa relativamente al trattamento dei propri dati o per porre domande sulla gestione dei dati riservati, è possibile scrivere all'indirizzo e-mail: support@kaspersky.com.

Spiegare la natura della richiesta utilizzando il maggior numero di dettagli possibile. Alla domanda verrà fornita una risposta in tempi brevi.

La fornitura delle informazioni è facoltativa. L'opzione relativa alla raccolta dei dati può essere disattivata dall'utente in qualsiasi momento nella sezione "Feedback" della pagina "Impostazioni" del prodotto Kaspersky in uso.

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

UTILIZZO DI CODICE DI TERZE PARTI

Il codice di terze parti è stato utilizzato durante la fase di sviluppo di Kaspersky PURE.

IN QUESTA SEZIONE:

Libreria Agava-C 276
Libreria di software per la protezione dei dati Crypto C 276
Libreria Fastscript 1.9 276
Libreria Pcre 7.4, 7.7 276
Libreria del parser Bison GNU 277
Libreria AGG 2.4 277
Libreria OpenSSL 0.9.8d 277
Libreria Gecko SDK 1.8 279
Libreria Zlib 1.2 279
Libreria Libpng 1.2.8, 1.2.29 279
Libreria Libnkfm 2.0.5 279
Libreria Expat 1.2, 2.0.1 279
Libreria Info-ZIP 5.51 280
Libreria Windows Installer XML (WiX) 2.0 280
Libreria Passthru 283
Libreria Filter 283
Libreria Netcfg 283
Libreria Pcre 3.0 283
Libreria RFC1321-based (RSA-free) MD5 284
Libreria Windows Template (WTL 7.5) 284
Libreria Libjpeg 6b 286
Libreria Libungif 3.0 288
Libreria Libxdr 288
Libreria Tiniconv - 1.0.0 288
Libreria Bzip2/libbzip2 1.0.5 293
Libreria Libspf2-1.2.9 294
Libreria Protocol Buffer 294
Libreria Sqlite 3.5.9 295
Libreria Icu 4.0 295
Altre informazioni 295

LIBRERIA AGAVA-C

La libreria Agava-C, sviluppata da OOO "R-Alpha", è utilizzata per controllare le firme digitali.

LIBRERIA DI SOFTWARE PER LA PROTEZIONE DEI DATI CRYPTO C

Per la creazione e il controllo delle firme digitali, viene utilizzata la libreria software di protezione dei dati Crypto C, sviluppata da "CryptoEX", http://www.cryptoex.ru.

LIBRERIA FASTSCRIPT 1.9

Durante la creazione dell'applicazione è stata utilizzata la libreria FastScript (copyright © Fast Reports Inc.). Tutti i diritti riservati.

LIBRERIA PCRE 7.4, 7.7

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria PCRE 7.4 copyright © 1997-2008 University of Cambridge in base ai termini della licenza BSD.

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 5 of PCRE is distributed under the terms of the "BSD" license, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

Written by: Philip Hazel <ph10@cam.ac.uk>

University of Cambridge Computing Service,

Cambridge, England. Phone: +44 1223 334714.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the University of Cambridge nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

LIBRERIA DEL PARSER BISON GNU

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria dello scheletro del parser Bison 2.3 copyright © GNU Project http://ftp.gnu.org/gnu/bison/ in base a un'eccezione speciale.

As a special exception, you may create a larger work that contains part or all of the Bison parser skeleton and distribute that work under terms of your choice, so long as that work isn't itself a parser generator using the skeleton or a modified version thereof as a parser skeleton. Alternatively, if you modify or redistribute the parser skeleton itself, you may (at your option) remove this special exception, which will cause the skeleton and the resulting Bison output files to be licensed under the GNU General Public License without this special exception.

LIBRERIA AGG 2.4

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria AGG (Anti-Grain Geometry) 2.4 copyright © 2002-2005 Maxim Shemanarev. All rights reserved, su licenza BSD modificata.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 2004 Alberto Demichelis

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

LIBRERIA OPENSSL 0.9.8D

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria OpenSSL 0.9.8d copyright © 1998-2007 The OpenSSL Project. All rights reserved, su licenza OpenSSL License e Original SSLeay License (http://www.openssl.org/).

OpenSSL License

Copyright (c) 1998-2007 The OpenSSL Project. Tutti i diritti riservati.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com). Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

LIBRERIA GECKO SDK 1.8

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria Gecko SDK 1.8 Copyright © Mozilla Foundation. All rights reserved, su licenza MPL 1.1 (http://www.mozilla.org/MPL/MPL-1.1.html). Sito Web e collegamento del pacchetto di distribuzione: http://developer.mozilla.org/en/docs/Gecko_SDK.

LIBRERIA ZLIB 1.2

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria zlib 1.2 copyright © 1995-2005 Jean-loup Gailly and Mark Adler. All rights reserved, su licenza zlib/libpng.

LIBRERIA LIBPNG 1.2.8, 1.2.29

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria libpng 1.2.8, 1.2.29 copyright © 2004, 2006-2008 Glenn Randers-Pehrson. All rights reserved, su licenza zlib/libpng.

LIBRERIA LIBNKFM 2.0.5

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria libnkfm 2.0.5 Copyright (c) KUBO Takehiro. Tutti i diritti riservati.

LIBRERIA EXPAT 1.2, 2.0.1

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria Expat 1.2, 2.0.1 Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd. All rights reserved. Utilizzo in base alle condizioni seguenti:

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LIBRERIA INFO-ZIP 5.51

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria Info-ZIP 5.51 Copyright (c) 1990-2007. All rights reserved, su licenza Info-ZIP.

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the above disclaimer and the following restrictions:

1. Redistributions of source code (in whole or in part) must retain the above copyright notice, definition, disclaimer, and this list of conditions.

2. Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.

3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP--must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip", "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions.

4. Info-ZIP retains the right to use the names "Info-ZIP", "Zip", "UnZip", "UnZipSFX", "WiZ", "Pocket UnZip", "Pocket Zip", and "MacZip" for its own source and binary releases.

LIBRERIA WINDOWS INSTALLER XML (WIX) 2.0

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria Windows Installer XML (WiX) 2.0 Copyright (c) Microsoft Corporation. All rights reserved, su licenza CPL 1.0 (http://sourceforge.net/projects/wix/).

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. **DEFINITIONS**

   "Contribution" means:

   a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

b) in the case of each subsequent Contributor:

i) changes to the Program, and

ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents" mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. **GRANT OF RIGHTS**

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. **REQUIREMENTS**

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. **COMMERCIAL DISTRIBUTION**

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. **NO WARRANTY**

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. **DISCLAIMER OF LIABILITY**

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. **GENERAL**

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

LIBRERIA PASSTHRU

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria Ndis Intermediate Miniport driver sample Copyright (c) 1992-2000 Microsoft Corporation. Tutti i diritti riservati.

LIBRERIA FILTER

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria Ndis Sample NDIS Lightweight filter driver Copyright (c) 2004-2005 Microsoft Corporation. Tutti i diritti riservati.

LIBRERIA NETCFG

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria Network Configuration Sample Copyright (c) 1997 Microsoft Corporation. Tutti i diritti riservati.

LIBRERIA PCRE 3.0

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria pcre 3.0 copyright © 1997-1999 University of Cambridge in base alla PCRE LICENSE. Tutti i diritti riservati.

LIBRERIA RFC1321-BASED (RSA-FREE) MD5

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria RFC1321-based (RSA-free) MD5. Copyright (c) 1999, 2002 Aladdin Enterprises. Tutti i diritti riservati. Distribuita su licenza zlib/libpng.

LIBRERIA WINDOWS TEMPLATE (WTL 7.5)

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria Windows Template Library 7.5 Copyright (c) 2005 Microsoft Corporation. All rights reserved, su licenza Common Public License 1.0, http://sourceforge.net/projects/wtl/.

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. **DEFINITIONS**

   "Contribution" means:

   a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

   b) in the case of each subsequent Contributor:

   i) changes to the Program, and

   ii) additions to the Program;

   where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

   "Contributor" means any person or entity that distributes the Program.

   "Licensed Patents" mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

   "Program" means the Contributions distributed in accordance with this Agreement.

   "Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. **GRANT OF RIGHTS**

   a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

   b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

   c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any

other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. **REQUIREMENTS**

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. **COMMERCIAL DISTRIBUTION**

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. **NO WARRANTY**

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. **DISCLAIMER OF LIABILITY**

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. **GENERAL**

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

LIBRERIA LIBJPEG 6B

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria libjpeg 6b. Copyright (c) 1991-1998, Thomas G. Lane. All Rights. L'utilizzo si basa sulle condizioni seguenti:

LEGAL ISSUES

In plain English:

We don't promise that this software works. (But if you find any bugs, please let us know!)

You can use this software for whatever you want. You don't have to pay us.

You may not pretend that you wrote this software. If you use it in a program, you must acknowledge somewhere in your documentation that you've used the IJG code.

In legalese:

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided "AS IS", and you, its user, assume the entire risk as to its quality and accuracy.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

(1) If any part of the source code for this software is distributed, then this README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.

(2) If only executable code is distributed, then the accompanying documentation must state that "this software is based in part on the work of the Independent JPEG Group".

(3) Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name in advertising or publicity relating to this software or products derived from it. This software may be referred to only as "the Independent JPEG Group's software".

We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

ansi2knr.c is included in this distribution by permission of L. Peter Deutsch, sole proprietor of its copyright holder, Aladdin Enterprises of Menlo Park, CA. ansi2knr.c is NOT covered by the above copyright and conditions, but instead by the usual distribution terms of the Free Software Foundation; principally, that you must include source code if you redistribute it. (See the file ansi2knr.c for full details.) However, since ansi2knr.c is not needed as part of any program generated from the IJG code, this does not limit you more than the foregoing paragraphs do.

The Unix configuration script "configure" was produced with GNU Autoconf. It is copyright by the Free Software Foundation but is freely distributable. The same holds for its supporting scripts (config.guess, config.sub, ltconfig, ltmain.sh). Another support script, install-sh, is copyright by M.I.T. but is also freely distributable.

It appears that the arithmetic coding option of the JPEG spec is covered by patents owned by IBM, AT&T, and Mitsubishi. Hence arithmetic coding cannot legally be used without obtaining one or more licenses. For this reason, support for arithmetic coding has been removed from the free JPEG software.

(Since arithmetic coding provides only a marginal gain over the unpatented Huffman mode, it is unlikely that very many implementations will support it.) So far as we are aware, there are no patent restrictions on the remaining

code.

The IJG distribution formerly included code to read and write GIF files. To avoid entanglement with the Unisys LZW patent, GIF reading support has been removed altogether, and the GIF writer has been simplified to produce "uncompressed GIFs". This technique does not use the LZW algorithm; the resulting GIF files are larger than usual, but are readable by all standard GIF decoders.

We are required to state that "The Graphics Interchange Format(c) is the Copyright property of CompuServe Incorporated. GIF(sm) is a Service Mark property of CompuServe Incorporated."

LIBRERIA LIBUNGIF 3.0

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria libungif 3.0. Copyright (c) 1997 Eric S. Raymond. L'utilizzo si basa sulle condizioni seguenti:

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LIBRERIA LIBXDR

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria libxdr copyright © Sun Microsystems, Inc. L'utilizzo si basa sulle condizioni seguenti:

Sun RPC is a product of Sun Microsystems, Inc. and is provided for unrestricted use provided that this legend is included on all tape media and as a part of the software program in whole or part.

Users may copy or modify Sun RPC without charge, but are not authorized to license or distribute it to anyone else except as part of a product or program developed by the user.

SUN RPC IS PROVIDED AS IS WITH NO WARRANTIES OF ANY KIND INCLUDING THE WARRANTIES OF DESIGN, MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

Sun RPC is provided with no support and without any obligation on the part of Sun Microsystems, Inc. to assist in its use, correction, modification or enhancement.

SUN MICROSYSTEMS, INC. SHALL HAVE NO LIABILITY WITH RESPECT TO THE INFRINGEMENT OF COPYRIGHTS, TRADE SECRETS OR ANY PATENTS BY SUN RPC OR ANY PART THEREOF.

In no event will Sun Microsystems, Inc. be liable for any lost revenue or profits or other special, indirect and consequential damages, even if Sun has been advised of the possibility of such damages.

Sun Microsystems, Inc.

2550 Garcia Avenue

Mountain View, California 94043

LIBRERIA TINICONV - 1.0.0

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria tiniconv – 1.0.0. Copyright (C) Free Software Foundation, Inc. author Roman Rybalko (http://sourceforge.net/projects/tiniconv/) con licenza GNU LGPL 2.1 (http://www.gnu.org/).

GNU LESSER GENERAL PUBLIC LICENSE v.2.1

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of

software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

LIBRERIA BZIP2/LIBBZIP2 1.0.5

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria bzip2/libbzip2 1.0.5. Copyright (C) 1996-2007 Julian R Seward. Tutti i diritti riservati. L'utilizzo si basa sulle condizioni seguenti:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

3. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Julian Seward, jseward@bzip.org

LIBRERIA LIBSPF2-1.2.9

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria libspf2-2/1/09. Copyright 2005 by Shevek and Wayne Schlitt. All rights reserved. Utilizzo in base alle condizioni della licenza The two-clause BSD:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

LIBRERIA PROTOCOL BUFFER

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria Protocol Buffer. Copyright 2008, Google Inc. All rights reserved. Distribuita in base alle condizioni della licenza New BSD.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

- Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)

HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Code generated by the Protocol Buffer compiler is owned by the owner of the input file used when generating it. This code is not standalone and requires a support library to be linked with it. This support library is itself covered by the above license.

LIBRERIA SQLITE 3.5.9

Per la creazione dell'applicazione è stata utilizzata la libreria sqlite 3.5.9. Copyright (C) Dan Kennedy, D. Richard Hipp, http://www.sqlite.org/copyright.html.

LIBRERIA ICU 4.0

Per la creazione dell'applicazione è stata utilizzata la libreria icu 4.0. Copyright (c) 1995-2009 International Business Machines Corporation e altri. Tutti i diritti riservati.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

All trademarks and registered trademarks mentioned herein are the property of their respective owners.

ALTRE INFORMAZIONI

Questo prodotto contiene o può contenere programmi concessi in licenza o in sublicenza all'utente in base alla licenza GNU Public License o altre licenze Open Source analoghe, che, in aggiunta a ulteriori diritti, consentono all'utente di copiare, modificare o ridistribuire determinati programmi o componenti e accedere al codice sorgente (software Open Source). Se tale licenza prevede di rendere disponibile il codice sorgente agli utenti che ricevono il software nel formato di codice binario eseguibile, il codice sorgente può essere richiesto tramite posta elettronica all'indirizzo source@kaspersky.com o è fornito con il prodotto.

GLOSSARIO

A

Aggiornamenti

Procedura di sostituzione/aggiunta di nuovi file (database o moduli dell'applicazione) recuperati dai server degli aggiornamenti di Kaspersky Lab.

Aggiornamenti del database

Una delle funzioni eseguite da un'applicazione Kaspersky Lab che consente di tenere sempre aggiornata la protezione. I database vengono scaricati dai server degli aggiornamenti di Kaspersky Lab nel computer e collegati automaticamente all'applicazione.

Aggiornamenti disponibili

Gruppo di aggiornamenti per i moduli dell'applicazione Kaspersky Lab, inclusi gli aggiornamenti critici accumulati in un periodo di tempo e le modifiche apportate all'architettura dell'applicazione.

Aggiornamenti urgenti

Aggiornamenti critici ai moduli dell'applicazione Kaspersky Lab.

Analisi euristica

Tecnologia di rilevamento delle minacce che non possono essere identificate dai database Anti-Virus. Consente di rilevare gli oggetti sospettati di essere stati colpiti da un virus sconosciuto o da una variante nuova di virus noti.

L'utilizzo dell'analisi euristica consente di rilevare fino al 92% delle minacce. Questo meccanismo è estremamente efficace e determina falsi positivi molto raramente.

I file rilevati dall'analisi euristica sono considerati sospetti.

Applicazione non compatibile

Applicazione anti-virus di uno sviluppatore di terze parti o applicazione Kaspersky Lab che non supporta la gestione attraverso Protezione del computer.

Archivio

File "contenente" uno o diversi altri oggetti che possono anche essere archivi.

Attacco di virus

Serie di attacchi intenzionali per infettare un computer con un virus.

Attivazione dell'applicazione

La procedura di attivazione consiste nell'immissione di un codice di attivazione e nell'ottenimento di una chiave che consentirà all'applicazione di determinare se l'utente dispone di diritti sufficienti per utilizzarla e di verificare la data di scadenza della licenza.

Attivita

Le funzioni eseguite dall'applicazione Kaspersky Lab vengono implementate come attività, ad esempio: Protezione in tempo reale, Scansione Completa, Aggiornamento del database.

B

BACKUP

Creazione di una copia di backup di un file prima di qualsiasi elaborazione. La copia viene archiviata nella memoria di backup e consente di ripristinare il file in seguito, ad esempio per eseguire una scansione con database aggiornati.

BLACKLIST DEI FILE CHIAVE

Database contenente informazioni sui file chiave Kaspersky Lab inseriti nella blacklist i cui proprietari hanno violato i termini del Contratto di licenza e informazioni sui file chiave creati ma per qualche motivo non venduti o sostituiti. Un file della blacklist è necessario per il funzionamento delle applicazioni di Kaspersky Lab. Il contenuto del file viene aggiornato insieme ai database.

BLOCCO DELL'OGGETTO

Negazione dell'accesso a un oggetto da parte di applicazioni esterne. Un oggetto bloccato non può essere letto, eseguito, modificato o eliminato.

C

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 e viene memorizzato nella sottocartella Cert della cartella di installazione dell'applicazione.

CONTATORE DEGLI ATTACCHI DI 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 dell'attività del virus, la modalità di diffusione e il testo nei messaggi da inviare.

D

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. Il DNS funziona in reti TCP/IP. In particolare può anche 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.

DATABASE

Database creati dagli esperti di Kaspersky Lab contenenti una descrizione dettagliata di tutte le minacce alla sicurezza del computer attualmente esistenti nonché dei metodi per rilevarle ed eliminarle. I database vengono costantemente aggiornati da Kaspersky Lab al presentarsi di nuove minacce. Per ottenere una migliore qualità di rilevamento delle minacce, è consigliabile copiare regolarmente i database dai server degli aggiornamenti di Kaspersky Lab.

DATABASE DELLA POSTA

Database contenenti messaggi di posta elettronica in un formato speciale salvati nel computer. Ogni messaggio di posta in entrata e in uscita viene inserito nel database della posta dopo essere stato ricevuto/inviato. I database vengono esaminati durante la scansione completa del computer.

I messaggi in entrata e in uscita vengono analizzati per verificare la presenza di virus in tempo reale al momento dell'invio e della ricezione se la protezione in tempo reale è abilitata.

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 come potenzialmente pericoloso. L'elenco viene creato dagli specialisti di Kaspersky Lab, 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. La disinfezione degli oggetti viene eseguita in base alle voci dei database. Durante la disinfezione è possibile che parte dei dati venga 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 riavvio successivo del sistema.

E

ELENCO DEGLI INDIRIZZI WEB BLOCCATI

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 DEGLI INDIRIZZI WEB CONSENTITI

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 DEGLI INDIRIZZI WEB DA 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 DEGLI INDIRIZZI CONSENTITI

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 ad alcune voci dell'elenco, per verificare la presenza di oggetti dannosi.

ELENCO DEI MITTENTI BLOCCATI

(noto anche come elenco "Bloccati")

Elenco di indirizzi di posta elettronica che inviano i messaggi che dovrebbero essere bloccati da Kaspersky Internet Security, indipendentemente dal contenuto.

ELENCO DEI MITTENTI CONSENTITI

(noto anche come elenco "Consentiti")

Elenco di indirizzi di posta elettronica che inviano i messaggi che non è necessario sottoporre a scansione da parte dell'applicazione Kaspersky Lab.

ELIMINAZIONE DEL MESSAGGIO

Metodo di elaborazione di un messaggio di posta contenente tracce di spam che consente di eliminare il messaggio fisicamente. Si consiglia di applicarlo ai messaggi che contengono inequivocabilmente spam. Prima di eliminare un messaggio, ne viene salvata una copia nella cartella di backup (a meno che questa opzione non sia disabilitata).

ELIMINAZIONE DI UN OGGETTO

Metodo di elaborazione dell'oggetto che implica la sua eliminazione fisica dalla posizione originaria (disco rigido, cartella, risorsa di rete). Si consiglia di applicare questo metodo agli oggetti pericolosi che, per qualsiasi ragione, non possono essere disinfettati.

ESCLUSIONE

Per esclusione si intende un oggetto escluso dalla scansione da parte dell'applicazione Kaspersky Lab. È possibile escludere dalla scansione determinati formati di file, utilizzare una maschera 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 l'estensione key, che rappresenta la "chiave" personale che consente di utilizzare l'applicazione Kaspersky Lab. Un file chiave viene incluso nel prodotto acquistato presso i distributori Kaspersky Lab o inviato tramite posta elettronica se l'acquisto avviene online.

FILE COMPRESSO

File di archivio contenente un programma di decompressione e istruzioni di esecuzione per il sistema operativo.

FLUSSI NTFS ALTERNATIVI

Flussi di dati NTFS (flussi di dati alternativi) destinati a contenere attributi aggiuntivi o informazioni sul file.

Ogni file nel file system NTFS è un insieme di flussi. Uno di essi include il contenuto del file che sarà possibile visualizzare dopo aver aperto il file, altri flussi (definiti alternativi) sono destinati a contenere meta informazioni e garantire, ad esempio, la compatibilità 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 fornito di due schede di rete, ciascuna delle quali collegata a reti diverse, che trasferisce i dati da una rete all'altra.

I

IP (INTERNET PROTOCOL)

Il protocollo 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 il NAT e il mascheramento consente di nascondere un gran numero di reti private attraverso 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.

IMPOSTAZIONI ATTIVITA

Impostazioni dell'applicazione specifiche per ogni tipo di attività.

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.

INSTALLAZIONE CON UNO SCENARIO DI AVVIO

Metodo di installazione remota delle applicazioni di Kaspersky Lab che consente di assegnare l'avvio dell'attività di installazione remota a un singolo account utente o a 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.

INTERCETTORE

Sottocomponente dell'applicazione responsabile della scansione di tipi specifici di messaggi di posta elettronica. Il set di intercettori specifico dell'installazione dipende dal ruolo o dalla combinazione di ruoli per i quali l'applicazione è stata distribuita.

INTESTAZIONE

Informazioni all'inizio di un file o di un messaggio, composte da dati di basso livello sullo stato e l'elaborazione del file (o del messaggio). In particolare, l'intestazione del messaggio di posta elettronica contiene dati come le informazioni sul mittente e sul destinatario, nonché la data.

L

LICENZA AGGIUNTIVA

Licenza 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 offrire il livello ottimale di protezione per il computer. Questo livello viene impostato per essere utilizzato per impostazione predefinita.

LIVELLO DI GRAVITÀ DELL'EVENTO

Descrizione dell'evento, registrato durante il funzionamento dell'applicazione Kaspersky Lab. Esistono quattro livelli di gravità:

Eventi critici.

Errori funzionali.

Attenzione.

Messaggio informativo.

Eventi dello stesso tipo possono avere livelli di gravità diversi, in base alla situazione in cui si sono verificati.

LIVELLO DI PROTEZIONE

Il livello di protezione viene definito come una configurazione del componente predeterminata.

M

MASCHERA DI FILE

Rappresentazione di un'estensione e di un nome file 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. Notare che il nome e l'estensione sono sempre separati da un punto.

MEMORIA DI BACKUP

Memoria speciale destinata al salvataggio delle copie di backup di oggetti creati prima della disinfezione o eliminazione iniziale.

MESSAGGIO OSCENO

Messaggio di posta 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 diffusione e il testo dei messaggi da inviare.

MODULI DELL'APPLICAZIONE

File inclusi nel pacchetto di installazione di Kaspersky Lab responsabili dell'esecuzione delle attività principali. Un determinato modulo eseguibile corrisponde a ciascun 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 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 verrà esaminata come oggetto OLE.

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 sconsiglia l'uso di oggetti di questo tipo poiché potrebbero causare un'infezione nel computer.

OGGETTO MONITORATO

File trasferito mediante i protocolli HTTP, FTP o SMTP attraverso il firewall e inviato all'applicazione Kaspersky Lab per essere sottoposto a scansione.

OGGETTO PERICOLOSO

Oggetto contenente un virus. Si sconsiglia di accedere a questo tipo di oggetto per evitare di causare un'infezione del computer. Una volta rilevato un oggetto infetto, si consiglia di disinfettarlo tramite una delle applicazioni di Kaspersky Lab o di eliminarlo se non è possibile eseguire l'operazione.

OGGETTO POTENZIALMENTE INFETTABILE

Oggetto che, a causa della sua struttura o formato, può essere utilizzato dagli intrusi come "contenitore" per memorizzare e distribuire un oggetto dannoso. Di regola, si tratta di file eseguibili, ad esempio file con estensione .com, .exe, .dll e così via. Il rischio di attivare codice dannoso in tali file è estremamente alto.

OGGETTO POTENZIALMENTE INFETTO

Oggetto contenente codice modificato di un virus noto, oppure codice che ricorda quello di un virus, ma non ancora noto a Kaspersky Lab. I file potenzialmente infetti vengono rilevati tramite l'analisi euristica.

OGGETTO SOSPETTO

Oggetto contenente codice modificato di un virus noto, oppure codice che ricorda quello di un virus, ma non ancora noto a Kaspersky Lab. Gli oggetti sospetti vengono rilevati mediante l'analisi euristica.

P

PACCHETTO DI AGGIORNAMENTO

Pacchetto di file per l'aggiornamento del software. Viene scaricato da Internet e installato nel computer.

PERIODO DI VALIDITÀ DELLA LICENZA

Periodo di tempo durante il quale è possibile utilizzare tutte le funzionalità dell'applicazione Kaspersky Lab. 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 ridotto di funzioni e non è più possibile aggiornarne i database.

PORTA DI INPUT/OUTPUT

Viene utilizzata nei processori, ad esempio Intel, per lo scambio di dati con componenti hardware. Una porta di input/output viene 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 tramite una rete e che rende possibile l'esecuzione di vari programmi su un host unico 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 su un componente hardware di un computer al quale è possibile collegare un cavo o una porta (porta LPT, porta seriale, porta USB).

PROCESSO ATTENDIBILE

Processo dell'applicazione le cui operazioni non sono monitorate dall'applicazione di Kaspersky Lab nella modalità di protezione in tempo reale. In altre parole, nessun oggetto eseguito, aperto o salvato dal processo considerato attendibile verrà esaminato.

PROTEZIONE IN TEMPO REALE

Modalità operativa dell'applicazione che consente di eseguire la scansione degli oggetti per verificare la presenza di codice dannoso in tempo reale.

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 restituiti all'utente, quelli contenenti minacce o per i quali si sospetta la presenza di una minaccia vengono elaborati in base alle impostazioni dell'attività e quindi disinfettati, eliminati o messi in Quarantena.

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 ad essi associati includono HTTP (WWW), FTP e NNTP (news).

Q

QUARANTENA

Cartella nella quale vengono conservati tutti gli oggetti potenzialmente infetti rilevati durante le scansioni o la protezione in tempo reale.

R

RIPRISTINO

Spostamento di un oggetto originale dalla sezione Quarantena o Backup alla cartella in cui era stato inizialmente trovato prima di essere disinfettato, eliminato, spostato nella Quarantena o in una cartella diversa specificata dall'utente.

S

SOCKS

Protocollo del server proxy che consente di stabilire una connessione punto-punto tra computer nelle reti interne ed esterne.

SCANSIONE DEL TRAFFICO

Scansione in tempo reale che utilizza informazioni dell'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 una parte indipendente del programma (funzione) che in genere viene sviluppata per eseguire un'attività specifica di portata ridotta. Viene spesso utilizzato con programmi incorporati in ipertesti. Gli script vengono eseguiti, ad esempio, all'apertura di determinati siti Web.

Se è abilitata la protezione in tempo reale, l'applicazione controllerà gli script all'avvio, intercettandoli ed esaminandoli per verificare la presenza di virus. In funzione dei risultati della scansione, è possibile bloccarne o consentirne l'esecuzione.

SERVER DEGLI AGGIORNAMENTI DI KASPERSKY LAB

Elenco dei server HTTP e FTP di Kaspersky Lab da cui l'applicazione scarica database e aggiornamenti dei moduli nel computer.

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. Quindi il server proxy si connette 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 definiti di conseguenza 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.

SOGLIA DI ATTIVITA DEI VIRUS

Livello massimo consentito per un tipo specifico di evento in un periodo di tempo limitato che, se superato, verrà considerato come attività eccessiva del virus e minaccia di un attacco di virus. Questa funzionalità è molto importante durante gli attacchi di virus e consente a un amministratore di reagire con tempestività alle minacce di attacchi che si presentano.

SPAM

Invio di massa di messaggi di posta elettronica non richiesti, spesso contenenti messaggi pubblicitari.

SPOSTAMENTO DI OGGETTI NELLA QUARANTENA

Metodo di elaborazione di un oggetto potenzialmente infetto attraverso il blocco dell'accesso al file e lo spostamento dalla posizione originale alla cartella Quarantena, in cui viene salvato in forma crittografata, in modo da eliminare la minaccia di infezione.

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 anti-virus escludendo gli oggetti che non hanno subito modifiche dall'ultima scansione, sempre che i parametri di scansione, ovvero le impostazioni e il database anti-virus, non siano cambiati. Le informazioni di ogni file vengono archiviate in un database speciale. Questa tecnologia viene utilizzata nelle modalità di protezione in tempo reale e di scansione manuale.

Si supponga, ad esempio, che a un archivio esaminato da Kaspersky Internet Security sia stato assegnato lo stato non infetto. Alla scansione successiva, l'applicazione ignorerà questo archivio, a meno che non sia stato modificato o non siano state modificate le impostazioni di scansione. Se il contenuto dell'archivio è stato modificato aggiungendo un nuovo oggetto, oppure sono state modificate le impostazioni di scansione o è stato aggiornato il database anti-virus, l'archivio verrà esaminato nuovamente.

Limitazioni della tecnologia iChecker:

questa tecnologia non rappresenta la scelta ideale con i file di grandi dimensioni in quanto risulta più veloce esaminare un file che controllare se sia stato modificato dall'ultima scansione;

la tecnologia supporta un numero limitato di formati (exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar).

V

VIRUS DI BOOT

Virus che infetta i settori di avvio dell'unità disco rigido di un computer. Il caricamento del virus all'interno del sistema viene forzato durante il riavvio dal virus stesso e il codice del virus assume il controllo diretto al posto del codice del programma di avvio originale.

VIRUS SCONOSCIUTO

Nuovo virus su cui non sono disponibili informazioni nei database. In genere i virus sconosciuti vengono rilevati dall'applicazione negli oggetti mediante l'analisi euristica e tali oggetti vengono classificati come potenzialmente infetti.

KASPERSKY LAB

Fondata nel 1997, Kaspersky Lab rappresenta oggi una delle aziende leader nello sviluppo di una vasta gamma di prodotti software a elevate prestazioni destinati alla protezione delle informazioni, tra cui sistemi anti-virus, anti-spam e anti-hacking.

Kaspersky Lab è una società internazionale. La sede centrale si trova nella Federazione russa e gli uffici di rappresentanza sono nel Regno Unito, in Francia, Germania, Giappone, nei paesi del Benelux, in Cina, Polonia, Romania e negli USA (California). Recentemente è stata inaugurata una nuova sede, l'European Anti-Virus Research Centre, in Francia. La rete di partner di Kaspersky Lab è costituita da oltre 500 aziende in tutto il mondo.

Degli oltre 1000 specialisti qualificati che lavorano presso Kaspersky Lab, 10 hanno conseguito un Master di specializzazione post laurea in Business Administration e 16 un dottorato di ricerca. Tutti gli esperti anti-virus Kaspersky Lab senior sono membri dell'organizzazione CARO (Computer Anti-Virus Researchers Organization).

I punti di forza dell'azienda sono la notevole competenza e la significativa esperienza maturata in quattordici di anni di intensa attività di sviluppo di soluzioni anti-virus efficaci. Un'analisi approfondita delle attività dei virus informatici consente agli specialisti dell'azienda di anticipare le tendenze nello sviluppo di malware e di offrire agli utenti una protezione efficace e tempestiva contro nuovi tipi di attacchi. Questo vantaggio sta alla base dei prodotti e dei servizi offerti da Kaspersky Lab. I prodotti dell'azienda sono sempre un passo avanti rispetto a quelli della concorrenza nell'ambito della protezione anti-virus.

L'esperienza maturata in anni di duro lavoro hanno rafforzato nel tempo la posizione dominante raggiunta oggi. Kaspersky Lab è stata la prima azienda a sviluppare molti degli standard per software anti-virus moderni. Il prodotto di punta, Kaspersky Anti-Virus®, protegge in modo efficace tutti i tipi di sistemi dagli attacchi dei virus, incluse le workstation, i file server, i sistemi di posta, i firewall, i gateway Internet e i computer palmari. Gli strumenti di facile gestione di cui è fornito consentono di automatizzare la protezione anti-virus di computer e reti aziendali. Un gran numero di sviluppatori di fama internazionale utilizza il kernel di Kaspersky Anti-Virus nei propri prodotti, inclusi Nokia ICG (USA), Aladdin (Israele), Sybari (USA), G Data (Germania), Deerfield (USA), Alt-N (USA), Microworld (India) e BorderWare (Canada).

I clienti di Kaspersky Lab possono usufruire di una vasta gamma di servizi aggiuntivi che garantiscono il funzionamento costante dei prodotti e una compatibilità completa con i propri requisiti specifici. L'azienda progetta, implementa e supporta sistemi anti-virus aziendali. Il database anti-virus di Kaspersky Lab viene aggiornato ogni ora. Il servizio di supporto tecnico offerto ai clienti è disponibile 24 ore su 24, in diverse lingue.

Per porre domande, fare commenti o ricevere consigli, è possibile contattarci tramite i rivenditori o direttamente presso Kaspersky Lab. Tutta l'assistenza necessaria in relazione alle questioni sollevate sui prodotti Kaspersky verrà fornita tramite telefono o posta elettronica. Viene sempre garantita una risposta completa e dettagliata a qualsiasi domanda.

Sito ufficiale di Kaspersky Lab:	http://www.kaspersky.it
Enciclopedia dei Virus:	http://www.viruslist.com
Anti-Virus Lab:	newvirus@kaspersky.com (solo per l'invio di oggetti sospetti negli archivi) http://support.kaspersky.com/virlab/helpdesk.html?LANG=it (per domande agli analisti anti-virus)
Forum Web Kaspersky Lab:	http://forum.kaspersky.com

CONTRATTO DI LICENZA

AVVERTENZA LEGALE IMPORTANTE PER TUTTI GLI UTENTI: LEGGERE ATTENTAMENTE IL SEGUENTE CONTRATTO PRIMA DI INIZIARE A USARE IL SOFTWARE.

FACENDO CLIC SUL PULSANTE ACCETTO NELLA FINESTRA DEL CONTRATTO DI LICENZA O IMMETTENDO IL/I SIMBOLO/I CORRISPONDENTE/I, LEI ACCETTA DI ESSERE VINCOLATO AL RISPETTO DEI TERMINI E DELLE CONDIZIONI DI QUESTO CONTRATTO. **TALE AZIONE EQUIVALE AD APPORRE LA SUA FIRMA E SIGNIFICA CHE ACCETTA DI ESSERE VINCOLATO E DI DIVENTARE UNA PARTE CONTRAENTE DEL PRESENTE CONTRATTO E CHE ACCETTA LA VALIDITÀ LEGALE DEL PRESENTE CONTRATTO COME QUALSIASI ACCORDO STIPULATO PER ISCRITTO E DA LEI FIRMATO.** SE NON È D'ACCORDO CON TUTTI I TERMINI E LE CONDIZIONI DEL PRESENTE CONTRATTO, ANNULLI L'INSTALLAZIONE DEL SOFTWARE E NON LO INSTALLI.

DOPO AVER CLICCATO IL PULSANTE "ACCETTO" NELLA FINESTRA DEL CONTRATTO DI LICENZA O DOPO AVER IMMESSO IL/I SIMBOLO/I CORRISPONDENTE/I LEI HA IL DIRITTO DI USARE IL SOFTWARE SECONDO I TERMINI E LE CONDIZIONI DEL PRESENTE CONTRATTO.

1. Definizioni

1.1. **Per Software** si intende il software, compresi gli aggiornamenti e i relativi materiali.

1.2. **Per Titolare** (titolare di tutti i diritti, sia esclusivi che non, relativi al Software) si intende Kaspersky Lab ZAO, una società regolarmente costituita ai sensi delle leggi della Federazione Russa.

1.3. **Per Computer** si intende l'hardware, ivi compresi i personal computer, i laptop, le postazioni di lavoro, i personal digital assistant, gli "smart phone", i dispositivi palmari o gli altri dispositivi elettronici per cui il Software è stato progettato su cui il Software verrà installato e/o utilizzato.

1.4. **Per Utente Finale (Lei/Suo)** si intende il soggetto o i soggetti che installano o utilizzano il Software per proprio conto e che sta/stanno utilizzando legalmente una copia del Software; o, se il Software è stato scaricato o installato per conto di un'organizzazione, ad esempio da un dipendente, *"Lei"* sta a intendere anche l'organizzazione per cui il Software è stato scaricato o installato e si dichiara con il presente che tale organizzazione ha autorizzato quel soggetto ad accettare questo contratto, scaricando e installando il Software per conto dell'organizzazione stessa. Ai fini del presente contratto il termine "*organizzazione"* include, a titolo esemplificativo e non limitativo, qualsiasi società di persone, società a responsabilità limitata, persona giuridica, associazione, società per azioni, trust, joint venture, organizzazione sindacale, organizzazione non registrata o autorità governativa.

1.5. **Per Partner** si intendono le organizzazioni o il soggetto/i soggetti che distribuiscono il Software al Titolare sulla base di un contratto e di una licenza.

1.6. **Per Aggiornamento/i** si intendono tutti gli aggiornamenti, le revisioni, le patch, i perfezionamenti, le correzioni, le modifiche, le copie, le aggiunte o i pacchetti di manutenzione, ecc.

1.7. **Per Manuale dell'Utente** si intende il manuale dell'utente, la guida per l'amministratore, il libro di riferimento e i relativi materiali di tipo illustrativo o di altro tipo.

2. Concessione della licenza

2.1. Con il presente il Titolare Le concede licenza di uso non esclusivo per la memorizzazione, il caricamento, l'installazione, l'esecuzione e la visualizzazione (l'"uso") del Software su di una quantità specificata di Computer al fine di fornire un supporto per la protezione del Suo Computer, sul quale è installato il Software, contro le minacce descritte nel Manuale dell'Utente, in osservanza di tutti i requisiti tecnici descritti nel Manuale dell'Utente e secondo i termini e le condizioni di questo Contratto (la "Licenza") e Lei accetta questa Licenza:

Versione di prova. Se ha ricevuto, scaricato e/o installato la versione di prova del Software e se ha aderito alla licenza di valutazione del Software, può utilizzare il Software solo a scopo dimostrativo e soltanto per il periodo dimostrativo consentito, salvo laddove diversamente indicato, a partire dalla data della prima installazione. È severamente proibito l'uso del Software per scopi diversi o per un periodo più lungo del periodo di valutazione consentito.

Software per ambiente multiplo; Software a linguaggio multiplo; Software a doppio supporto magnetico; Copie multiple; Servizi aggiuntivi. Qualora Lei utilizzi diverse versioni del Software o edizioni del Software di lingua diversa, o riceva il Software su diversi supporti magnetici, o comunque riceva copie multiple del Software, ovvero qualora in cui Lei abbia acquistato il Software insieme a software aggiuntivi, il numero massimo di Computer su cui il Software può essere installato equivale al numero di licenze ricevuto dal Titolare *sempre che* ogni licenza acquistata Le dia diritto a installare e utilizzare il Software sulla quantità numero di Computer specificata nei paragrafi 2.2 e 2.3, salvo laddove diversamente stabilito dai termini della licenza.

2.2. Se il Software è stato acquistato su un supporto fisico, Lei ha il diritto di utilizzare il Software per proteggere la quantità di Computer specificata nel pacchetto Software.

2.3. Se il Software è stato acquistato via Internet, Lei ha il diritto di utilizzare il Software per la protezione della quantità di Computer specificata all'atto dell'acquisto della Licenza del Software.

2.4. Lei ha diritto di copiare il Software soltanto a scopo di back-up e solo a titolo di sostituzione della copia di Sua legale proprietà, qualora essa vada persa, distrutta o diventi inutilizzabile. Questa copia di back-up non può essere utilizzata per fini diversi e deve essere distrutta quando viene meno il diritto d'uso del Software o alla scadenza della Sua licenza o qualora questa venga meno per qualsiasi altro motivo, ai sensi dalla legislazione in vigore nel principale paese di residenza o nel paese in cui Lei fa uso del Software.

2.5. Lei ha la facoltà di trasferire il diritto non esclusivo di licenza d'uso del Software ad altri soggetti o persone giuridiche previste dalla licenza concessaLe dal Titolare, purché il beneficiario accetti di essere vincolato da tutti i termini e dalle condizioni del presente Contratto e La sostituisca in toto nel godimento della licenza concessa dal Titolare. In caso di trasferimento di tutti i diritti d'uso del Software concessi dal Titolare, Lei è tenuto a distruggere tutte le copie del Software, ivi compresa la copia di back-up. Se Lei è il beneficiario della licenza così trasferita, deve accettare di osservare tutti i termini e le condizioni del presente Contratto. Se Lei non accetta di essere vincolato da tutti i termini e le condizioni del presente Contratto, non Le è permesso installare e/o fare uso del Software. In qualità di beneficiario della licenza trasferita, Lei riconosce inoltre di non detenere altri diritti o diritti migliori rispetto a quelli che spettavano all'Utente Finale che ha acquistato il Software dal Titolare.

2.6. Dal momento in cui si procede all'attivazione del Software o dopo l'installazione del file della chiave di licenza (a eccezione della versione di prova del Software), Lei ha diritto di ricevere i seguenti servizi per il periodo di tempo specificato sul pacchetto Software (se il Software è stato acquistato su supporto fisico) o specificato durante l'acquisto (se il Software è stato acquistato via Internet):

- Aggiornamenti del Software via Internet quando e nel momento in cui il Titolare li pubblica sul suo sito o attraverso altri servizi online. Qualsiasi Aggiornamento di cui Lei possa essere destinatario costituisce parte del Software e a esso si applicano i termini e le condizioni di questo Contratto;

- Supporto Tecnico via Internet e Hotline telefonica di Supporto Tecnico.

3. Attivazione e validità

3.1. Nel caso in cui Lei apportasse modifiche al Suo computer o al software di altri fornitori installato su di esso, il Titolare ha la facoltà di chiederLe di ripetere l'attivazione del Software o l'installazione del file della chiave di licenza. Il Titolare si riserva il diritto di utilizzare qualsiasi mezzo e qualsiasi procedura per verificare la validità della Licenza e/o la validità legale della copia del Software installata e/o utilizzata sul Suo Computer.

3.2. Se il Software è stato acquistato su supporto fisico, esso può essere utilizzato previa accettazione del presente Contratto per il periodo specificato sulla confezione a far data dalla data di accettazione del presente Contratto.

3.3. Se il Software è stato acquistato via Internet, il Software può essere utilizzato previa accettazione del presente Contratto per il periodo specificato durante l'acquisto.

3.4. Lei ha diritto di usare la versione di prova del Software secondo quanto disposto dal Paragrafo 2.1 senza alcun addebito unicamente per il periodo di valutazione (30 giorni) concesso dal momento della sua attivazione ai sensi del presente Contratto, *purché* la versione di prova non dia diritto ad Aggiornamenti e a Supporto Tecnico via Internet e tramite Hotline telefonica.

3.5. La Sua Licenza d'Uso del Software è limitata al periodo di tempo specificato nei Paragrafi 3.2 o 3.3 (secondo quanto applicabile) e nel periodo restante può essere visionata utilizzando i supporti descritti nel Manuale dell'Utente.

3.6. Nel caso in cui Lei abbia acquistato il Software per un utilizzo su più di un Computer, la Sua Licenza d'Uso del Software è limitata al periodo di tempo che ha inizio alla data di attivazione del Software o l'installazione del file della chiave di licenza sul primo Computer.

3.7. Fatto salvo qualsiasi altro rimedio previsto dalla legge o basato sui principi di opportunità, giustizia e onesta composizione ("equity") a cui il Titolare possa legittimamente fare ricorso, nel caso di una Sua violazione dei termini e delle condizioni del presente Contratto, il Titolare avrà diritto in ogni momento e senza obbligo di preavviso di rescindere questa Licenza d'uso del Software senza rimborsare il prezzo d'acquisto né parte di esso.

3.8. Lei accetta di fare uso del Software e utilizzare qualsiasi rapporto o informazione derivante dall'utilizzo di questo Software in modo conforme a tutte le leggi applicabili internazionali, nazionali, statali, regionali e locali e a qualsiasi normativa, ivi compresa, a titolo esemplificativo e non limitativo, le leggi sulla privacy, sui diritti d'autore, sul controllo delle esportazioni e sulle oscenità.

3.9. Fatte salve eventuali disposizioni contrarie specificamente previste in questa sede, Lei non ha la facoltà di trasferire né di assegnare alcuno dei diritti che le sono stati concessi ai sensi del presente Contratto né alcuno degli obblighi che da esso Le derivano.

4. Supporto Tecnico

Il Supporto Tecnico descritto al Paragrafo 2.6 del presente Contratto Le viene fornito quando è stato installato l'Aggiornamento più recente del Software (a eccezione della versione di prova del Software).Servizio di assistenza tecnica: http://support.kaspersky.com

5. Raccolta di informazioni

5.1. Avendo accettato i termini e le condizioni del presente Contratto, Lei accetta di fornire informazioni al Titolare sui file eseguibili e sulle relative *checksum* allo scopo di migliorare il livello degli accorgimenti di sicurezza a Sua disposizione.

5.2. Allo scopo di migliorare la consapevolezza in materia di sicurezza circa le nuove minacce e le loro origini e allo scopo di migliorare il livello degli accorgimenti di sicurezza a Sua disposizione, con il Suo consenso, che è stato esplicitamente confermato nella Dichiarazione della Raccolta dei Dati del Kaspersky Security Network, Lei ha espressamente il diritto di ottenere tali informazioni. Lei può disattivare il servizio Kaspersky Security Network durante l'installazione. Inoltre, Lei può attivare e disattivare il servizio Kaspersky Security Network in qualsiasi momento nella pagina delle opzioni del Software.

Inoltre, Lei dichiara e accetta che qualsiasi informazione raccolta dal Titolare possa essere usata per monitorare e pubblicare relazioni sui trend relativi ai rischi per la sicurezza, a sola e unica discrezione del Titolare.

5.3. Il Software non elabora alcun dato che possa essere personalmente identificabile e non abbina i dati in elaborazione ad alcuna informazione personale.

5.4. Se non desidera che le informazioni raccolte dal Software vengano inviate al Titolare, non deve attivare e/o disattivare il servizio Kaspersky Security Network.

6. Restrizioni

6.1. Le è fatto divieto di emulare, clonare, locare, dare in prestito, noleggiare, vendere, modificare, decompilare o reingegnerizzare il Software, disassemblarlo o creare opere accessorie basate sul Software o su una porzione di esso con la sola eccezione di diritti non rinunciabili previsti dalla legislazione applicabile, e Le è fatto comunque divieto di ridurre parte del Software in forma decifrabile o trasferire il Software tutelato da licenza o qualsivoglia sottoinsieme dello stesso, o permettere a terzi di fare quanto sopra, salvo nella misura in cui le limitazioni sopra illustrate siano espressamente proibite dal diritto applicabile. È fatto divieto di utilizzare o reingegnerizzare qualsivoglia codice binario o origine del Software allo scopo di ricreare l'algoritmo del programma, che è proprietario. Tutti i diritti non espressamente concessi attraverso il presente Contratto sono riservati al Titolare e/o ai suoi fornitori, secondo quanto applicabile. L'uso non autorizzato del Software produrrà la rescissione immediata e automatica del presente Contratto e della Licenza concessa in virtù dello stesso e può determinare l'apertura di un procedimento legale nei Suoi confronti.

6.2. Fatto salvo quanto disposto al Paragrafo 2.5 del presente Contratto, Lei non ha diritto di trasferire i diritti d'uso del Software a terzi.

6.3. Le è fatto divieto di mettere a conoscenza di terzi il codice di attivazione e/o il file chiave della licenza o di consentire l'accesso al codice di attivazione e/o di licenza, i quali rappresentano dati riservati del Titolare; Lei sarà inoltre tenuto a usare ogni ragionevole cautela per la protezione del codice di attivazione e/o di licenza riservati, qualora Lei abbia la facoltà di trasferire il codice di attivazione e/o di licenza a terzi secondo quanto illustrato al Paragrafo 2.5 del presente Contratto.

6.4. Non è consentito concedere a noleggio, in locazione o in prestito a terzi il Software.

6.5. Non è consentito utilizzare il Software per la creazione di dati o di software che servono a individuare, bloccare o gestire le minacce descritte nel Manuale dell'Utente.

6.6. In caso di violazione dei termini e delle condizioni del presente Contratto, il Titolare ha il diritto di bloccare il file di codice o di annullare la Sua licenza d'uso del Software senza obbligo di rimborso.

6.7. Se si usa la versione di prova del Software non si ha il diritto di ricevere il Supporto Tecnico specificato al Paragrafo 4 del presente Contratto, né il diritto di trasferire la licenza o i diritti d'uso del software a terzi

7. <u>Garanzia limitata e clausola di esclusione della responsabilità</u>

7.1. Il Titolare garantisce che il Software eseguirà sostanzialmente le prestazioni illustrate nelle specifiche e descritte nel Manuale dell'Utente *fermo restando, tuttavia, che* tale garanzia limitata non si applica a quanto segue: (w) lacune del Suo Computer e relative violazioni per le quali il Titolare declina espressamente qualsiasi responsabilità di garanzia; (x) malfunzionamenti, difetti o guasti conseguenti a cattivo uso, abuso, incidente, negligenza, difetti di installazione, funzionamento o manutenzione, furto, atto vandalico, evento di forza maggiore, atti di terrorismo, interruzione di tensione o momentanea sovratensione, infortunio, alterazione, modifica non consentita o riparazioni eseguite da soggetti diversi dal Titolare o qualsiasi azione o causa, a opera Sua o di qualsiasi altro soggetto terzo, ragionevolmente fuori del controllo del Titolare; (y) qualsiasi difetto da Lei tenuto nascosto al Titolare anche dopo la comparsa della prima anomalia; e (z) incompatibilità provocata da componenti hardware e/o software installati sul Suo computer.

7.2. Lei riconosce, accetta e concorda che nessun software è esente da errori e che Lei è stato informato che è necessario fare il back-up del Computer, con la frequenza e secondo le modalità per Lei più indicate.

7.3. In caso di violazione dei termini descritti nel Manuale dell'Utente o nel presente Contratto, il Titolare non garantisce il corretto funzionamento del Software.

7.4. Il Titolare non garantisce che il Software funzionerà correttamente se Lei non scarica regolarmente gli Aggiornamenti specificati nel Paragrafo 2.6 del presente Contratto.

7.5. Il Titolare non garantisce la protezione dalle minacce descritte nel Manuale dell'Utente una volta scaduto il periodo specificato nei Paragrafi 3.2 or 3.3 del presente Contratto o una volta scaduta, per qualsiasi motivo, la Licenza d'uso del Software.

7.6. IL SOFTWARE VIENE FORNITO "COSÌ COM'È" E IL TITOLARE NON FA ALCUNA DICHIARAZIONE E NON FORNISCE ALCUNA GARANZIA IN QUANTO A USO O PRESTAZIONI. FATTE SALVE LE GARANZIE, LE CONDIZIONI, LE DICHIARAZIONI O I TERMINI CHE NON POSSONO ESSERE ESCLUSI O LIMITATI DAL DIRITTO APPLICABILE, IL TITOLARE E I SUOI PARTNER, NON FORNISCONO ALCUNA GARANZIA, CONDIZIONE, DICHIARAZIONE O TERMINE (NÉ ESPLICITO NÉ IMPLICITI NÉ PREVISTO DALLA LEGGE, DALLA *COMMON LAW*, DALLE CONSUETUDINI O DAGLI USI O ALTRO) IN MERITO A QUALSIVOGLIA QUESTIONE, IVI COMPRESE, A TITOLO ESEMPLIFICATIVO E NON LIMITATIVO, LA NON VIOLAZIONE DEI DIRITTI DI TERZI, LA COMMERCIABILITÀ, LA QUALITÀ SODDISFACENTE, L'INTEGRAZIONE O L'APPLICABILITÀ PER UN FINE SPECIFICO. LEI SI ASSUME LA RESPONSABILITÀ DI TUTTI GLI ERRORI E TUTTI I RISCHI RELATIVI ALLE PRESTAZIONI NONCHÉ LA RESPONSABILITÀ DI AVER SCELTO IL SOFTWARE ALLO SCOPO DI RAGGIUNGERE I RISULTATI DESIDERATI NONCHÉ DELL'INSTALLAZIONE DEL SOFTWARE, DEL RELATIVO USO E DEI RISULTATI OTTENUTI DALLO STESSO. SENZA LIMITARE LE DISPOSIZIONI DI CUI SOPRA, IL TITOLARE NON FORNISCE ALCUNA DICHIARAZIONE E NON FORNISCE ALCUNA GARANZIA CHE IL SOFTWARE SARÀ ESENTE DA ERRORI O ESENTE DA INTERRUZIONI O ALTRI DIFETTI DI FUNZIONAMENTO NÉ CHE IL SOFTWARE SARÀ IN GRADO DI SODDISFARE IN TOTO O IN PARTE LE SUE ESIGENZE, SIANO ESSE STATE COMUNICATE AL TITOLARE O MENO.

8. Esclusione e limite della responsabilità

NELLA MASSIMA MISURA CONSENTITA DAL DIRITTO APPLICABILE, IN NESSUN CASO IL TITOLARE O I SUOI PARTNER SARANNO RESPONSABILI DI DANNI SPECIALI, MARGINALI, PUNITIVI, INDIRETTI O DI DANNI INDIRETTI DI QUALSIASI TIPO (IVI COMPRESI, A TITOLO ESEMPLIFICATIVO E NON LIMITATIVO, I DANNI PER PERDITA DI UTILI O PER PERDITA DI INFORMAZIONI RISERVATE O DI ALTRE INFORMAZIONI, PER INTERRUZIONE DELL'ATTIVITÀ LAVORATIVA, PER PERDITA DI PRIVACY, PER CORRUZIONE, DANNO E PERDITA DI DATI O DI PROGRAMMI, PER MANCATA OSSERVANZA DI UN OBBLIGO IVI COMPRESO QUALSIASI ONERE IMPOSTO PER LEGGE, DOVERE DI BUONA FEDE O DOVERE DI RAGIONEVOLE DILIGENZA, PER NEGLIGENZA, PER PERDITA ECONOMICA E PER QUALSIASI ALTRA PERDITA PECUNIARIA O ALTRA PERDITA DI SORTA) DERIVANTE DA O IN QUALSIASI MODO COLLEGATO ALL'USO O ALL'IMPOSSIBILITÀ DI USARE IL SOFTWARE, ALLA FORNITURA O MANCATA FORNITURA DEL SERVIZIO DI SUPPORTO O DI ALTRI SERVIZI, INFORMAZIONI, SOFTWARE E RELATIVI CONTENUTI ATTRAVERSO IL SOFTWARE O COMUNQUE DERIVANTI DALL'USO DEL SOFTWARE O COMUNQUE AI SENSI O IN RELAZIONE A QUALSIASI DISPOSIZIONE DEL PRESENTE CONTRATTO, O DERIVANTI DA UNA VIOLAZIONE DEL PRESENTE CONTRATTO O DA QUALSIVOGLIA ILLECITO (IVI COMPRESA LA NEGLIGENZA, LA FALSA TESTIMONIANZA, QUALSIASI OBBLIGO O DOVERE RELATIVI ALLA RESPONSABILITÀ) O DA UNA VIOLAZIONE DI UN OBBLIGO DI LEGGE O DA UNA VIOLAZIONE DELLA GARANZIA DA PARTE DEL TITOLARE O DI UNO DEI SUOI PARTNER, ANCHE QUALORA IL TITOLARE O UNO DEI SUOI PARTNER SIA STATO INFORMATO DELLA POSSIBILITÀ DI TALI DANNI.

LEI ACCETTA CHE NEL CASO IN CUI IL TITOLARE E/O SUOI PARTNER VENISSERO TROVATI RESPONSABILI, LA RESPONSABILITÀ DEL TITOLARE E/O DEI SUOI PARTNER SI LIMITERÀ AL COSTO DEL SOFTWARE. IN NESSUN CASO LA RESPONSABILITÀ DEL TITOLARE E/O DEI SUOI PARTNER POTRÀ SUPERARE LE SOMME VERSATE PER IL SOFTWARE AL TITOLARE O AL PARTNER (SECONDO QUANTO APPLICABILE).

NULLA IN QUESTO CONTRATTO ESCLUDE O LIMITA LA QUALSIVOGLIA RICHIESTA DI DANNI IN CASO DI MORTE E LESIONI PERSONALI. INOLTRE IN CASO IN CUI UNA MANLEVA, ESCLUSIONE O LIMITAZIONE CONTEMPLATE DAL PRESENTE CONTRATTO NON POSSA ESSERE ESCLUSA O LIMITATA AI SENSI DEL DIRITTO APPLICABILE, QUELLA MANLEVA, ESCLUSIONE O LIMITAZIONE NON SARÀ VALIDA NEI SUOI CONFRONTI E LEI DOVRÀ CONTINUARE A OSSERVARE TUTTE LE RESTANTI MANLEVE, ESCLUSIONI E LIMITAZIONI.

9. GNU e altre licenze di Terzi

Il Software può comprendere alcuni programmi software sottoposti a licenza (o a sublicenza) dell'utente ai sensi della GNU Licenza Pubblica Generica (General Public License, GPL) o ad altra licenza software di analoga natura che, tra gli altri, concede all'utente il diritto di copiare, modificare e ridistribuire certi programmi o porzioni di essi e di avere accesso al codice source ("Software Open Source"). Se tali licenze prevedono che per un software distribuito in formato binario eseguibile anche il codice source venga reso disponibile ai suoi utenti, il codice source deve essere reso accessibile inviando la richiesta all'indirizzo source@kaspersky.com, altrimenti il codice source verrà fornito insieme al Software. Se le licenze dei Software Open Source prevedono che il Titolare fornisca diritti d'uso, di copia e modifica del programma Software Open Source più ampi dei diritti concessi in virtù del presente Contratto, tali diritti avranno la priorità sui diritti e sulle restrizioni contemplati da questo documento.

10. Proprietà Intellettuale

10.1 Lei accetta che il Software e il fatto di esserne autori, i sistemi, le idee e i metodi operativi, la documentazione e altre informazioni contenute nel Software, sono proprietà intellettuale esclusiva e/o preziosi segreti commerciali del Titolare o dei suoi partner e che il Titolare e i suoi partner, secondo quanto applicabile, sono protetti dal diritto civile e penale e dalla legge sul copyright, sul segreto commerciale, sul marchio di fabbrica e sui brevetti della Federazione Russa, dell'Unione Europea e degli Stati Uniti e da altri trattati internazionali o di altri paesi. Il presente Contratto non Le concede alcun diritto di proprietà intellettuale né alcun diritto sui marchi o sui marchi di servizio del Titolare e/o dei suoi partner ("Marchi di fabbrica"). Lei ha la facoltà di usare i marchi di fabbrica solo nella misura in cui essi permettono di identificare le stampe prodotte dal Software in conformità con la pratica sui marchi generalmente accettata, ivi compresa l'identificazione del nome del proprietario del Marchio di fabbrica. Tale uso di un Marchio di fabbrica non Le conferisce alcun diritto di proprietà sul Marchio stesso. Il Titolare e/o i relativi partner possiedono e conservano ogni diritto, titolo e interesse relativo e collegato al Software, ivi comprese, senza alcuna limitazione, le correzioni d'errore, i perfezionamenti, gli Aggiornamenti o altre modifiche del Software, sia apportate dal Titolare che da Terzi nonché tutti i diritti d'autore, i brevetti, i diritti su segreti commerciali, i marchi di fabbrica e qualsiasi altro diritto di proprietà intellettuale ivi contemplato. Il possesso, l'installazione o l'uso del Software da parte Sua non Le trasferisce alcun titolo nella proprietà intellettuale del Software e Lei non acquisirà alcun diritto sul Software, salvo nella misura espressamente indicata nel presente Contratto. Tutte le copie del Software eseguite ai sensi del presente documento devono contenere le stesse avvertenze proprietarie che compaiono sul e nel Software. Fatto salvo quanto disposto in questo documento, il presente Contratto non Le conferisce alcun diritto di proprietà intellettuale sul Software e Lei riconosce che la Licenza, secondo la definizione data in seguito, concessa ai sensi del presente Contratto Le conferisce soltanto il diritto di uso limitato ai termini e alle condizioni del presente Contratto. Il Titolare si riserva tutti i diritti che non Le sono espressamente concessi ai sensi del presente Contratto.

10.2 Lei riconosce che il codice source, il codice di attivazione e/o il file di codice di licenza per il Software sono proprietari del Titolare e che essi costituiscono segreto commerciale del Titolare. Lei accetta di non modificare, adattare, reingegnerizzare, decompilare, disassemblare, né comunque tentare di scoprire il codice source del Software.

10.3 Lei accetta di non modificare, né alterare in alcun modo il Software. Lei non ha la facoltà di rimuovere, né di alterare alcuna delle avvertenze in materia di diritti d'autore o altre avvertenze proprietarie sulle copie del Software.

11. Diritto applicabile; Arbitrato

Il presente Contratto sarà regolamentato dalle leggi della Federazione Russa e interpretato conformemente a esse, senza riferimento a conflitti fra stato di diritto e principi. Il presente Contratto non sarà regolamentato dalla Convenzione delle Nazioni Unite sui Contratti per la Vendita Internazionale di Merci, la cui applicazione è espressamente esclusa. Qualsiasi vertenza derivante dall'interpretazione o dall'applicazione dei termini del presente Contratto o dalla sua violazione dovrà essere regolata tramite trattativa diretta oppure dal Tribunale dell'Arbitrato Commerciale Internazionale avente sede presso la Camera di Commercio e dell'Industria della Federazione Russa di Mosca, Federazione Russa. Qualsiasi lodo arbitrale emesso dall'arbitro sarà definitivo e vincolante per le parti e qualsiasi giudizio su tale lodo può essere fatto valere in ogni foro competente. Nulla nel presente Paragrafo 11 può impedire a una delle Parti di ricercare e ottenere equo indennizzo presso un foro competente, sia prima, durante sia dopo il processo d'arbitrato.

12. Periodo di validità per la presentazione di azioni legali

A prescindere dalla forma, nessuna azione derivante dalle transazioni commerciali eseguite ai sensi del presente Contratto può essere presentata dalle due parti contrattuali a più di un (1) anno dal momento in cui è accaduto o si è scoperto che è accaduto l'evento su cui si basa l'azione, tranne in caso di azioni per violazione dei diritti di proprietà intellettuale, che possono essere presentate entro il periodo massimo applicabile secondo i termini di legge.

13. Totalità del Contratto; Clausola salvatoria; Assenza di deroga.

Il presente Contratto costituisce l'intero contratto tra Lei e il Titolare e sostituisce ogni altro accordo, proposta, comunicato o comunicato commerciale precedente, sia verbale che scritto, relativo al Software o relativo al presente Contratto. Lei riconosce di aver letto il presente Contratto, lo comprende e accetta di essere vincolato ai suoi termini e condizioni. Se un foro competente giudica una qualsiasi disposizione del presente Contratto non valida, nulla o per qualsiasi motivo non applicabile, *in toto* o in parte, tale disposizione sarà riformulata più precisamente per renderla legittima e applicabile; ciò tuttavia non inficerà il Contratto e le rimanenti disposizioni del Contratto resteranno pienamente valide e in vigore nella massima misura consentita dalla legge diritto o dall'equity, conservando quanto più possibile il loro intento originale. Non varrà alcuna deroga a disposizioni o a condizioni del presente Contratto, a meno che la deroga non sia presentata per iscritto e firmata da Lei e da rappresentante autorizzato del Titolare, purché nessuna deroga a una violazione di una disposizione del presente Contratto valga come una deroga a qualsiasi violazione precedente, concorrente o successiva. La mancata insistenza da parte del Titolare nel richiedere la stretta applicazione di qualsiasi disposizione del presente Contratto o nel far valere un diritto non potrà essere interpretata quale deroga a tale disposizione o rinuncia a tale diritto.

14. Informazioni di contatto.

Per qualsiasi domanda relativa al presente Contratto, o se si desidera consultare per qualsiasi motivo il Titolare, si prega di contattare il nostro Servizio Clienti presso:

Kaspersky Lab ZAO, 10 edificio 1 1st Volokolamsky Proezd
Mosca, 123060
Federazione Russa

Tel: +7-495-797-8700
Fax: +7-495-645-7939

E-mail: info@kaspersky.com

Sito Web: www.kaspersky.com

© 1997-2010 Kaspersky Lab ZAO. Tutti i diritti riservati. Il Software e la documentazione d'accompagnamento sono soggetti a diritto d'autore e sono protetti dalle leggi sul copyright e dai trattati internazionali sul copyright nonché da altre leggi e trattati in materia di proprietà intellettuale.

INDICE

A

Abilita / disabilita la protezione in tempo reale ... 152

Addestramento di Anti-Spam
- con Addestramento guidato ... 110
- con i messaggi in uscita ... 111
- tramite i rapporti ... 113
- tramite il client di posta ... 111

Aggiornamenti
- impostazioni internazionali ... 147
- rollback dell'ultimo aggiornamento ... 146
- sorgente dell'aggiornamento ... 146
- utilizzo di un server proxy ... 147

Aggiornamenti manuali ... 145

Aggiornamenti pianificati ... 149

Aggiornamento da una cartella locale ... 148

Aggiornamento dell'applicazione ... 144

Algoritmo di funzionamento
- Anti-Spam ... 108
- Anti-Virus File ... 53
- Anti-Virus IM ... 76
- Anti-Virus Posta ... 63
- Anti-Virus Web ... 70
- Controllo Applicazioni ... 81

Ambito di protezione
- Anti-Virus File ... 55
- Anti-Virus IM ... 77
- Anti-Virus Posta ... 65
- Anti-Virus Web ... 71
- Controllo Applicazioni ... 83

Analisi euristica
- Anti-Banner ... 127
- Anti-Virus File ... 56
- Anti-Virus IM ... 79
- Anti-Virus Posta ... 67
- Anti-Virus Web ... 74

Anti-Banner
- analisi euristica ... 127
- elenco consentiti ... 128
- elenco di indirizzi di banner bloccati ... 129
- elenco di indirizzi di banner consentiti ... 128

Anti-Spam
- addestramento ... 109
- algoritmo di funzionamento ... 108
- database degli indirizzi di phishing ... 114
- elenco di frasi bloccate ... 117
- elenco di frasi consentite ... 118
- elenco di mittenti bloccati ... 115
- elenco di mittenti consentiti ... 117
- estensione per Microsoft Office Outlook ... 123
- estensione per Microsoft Outlook Express ... 125
- estensione per The Bat! ... 125
- estensione per Thunderbird ... 126
- fattore di probabile spam ... 108, 120
- fattore di spam ... 108, 120
- filtraggio dei messaggi di posta sul server ... 122
- funzioni avanzate di filtraggio ... 121
- importazione dell'elenco di mittenti consentiti ... 119

livello di sensibilità ... 114
messaggi di Microsoft Exchange Server ... 122
ripristino delle impostazioni predefinite ... 126

Anti-Virus File
algoritmo di funzionamento ... 53
ambito di protezione ... 55
analisi euristica ... 56
livello di protezione ... 54
modalità di scansione ... 58
ottimizzazione della scansione ... 56
reazione alle minacce ... 54
ripristino delle impostazioni predefinite ... 61
scansione dei file compositi ... 57
sospensione in corso ... 59, 60
tecnologia di scansione ... 58

Anti-Virus IM
algoritmo di funzionamento ... 76
ambito di protezione ... 77
analisi euristica ... 79
database degli indirizzi di phishing ... 77

Anti-Virus Posta
algoritmo di funzionamento ... 63
ambito di protezione ... 65
analisi euristica ... 67
filtraggio degli allegati ... 67
livello di protezione ... 63
reazione alle minacce ... 64
ripristino delle impostazioni predefinite ... 68
scansione dei file compositi ... 67

Anti-Virus Web
algoritmo di funzionamento ... 70
ambito di protezione ... 71
analisi euristica ... 74
Barra degli strumenti di Kaspersky ... 73
database degli indirizzi di phishing ... 72
livello di protezione ... 71
ottimizzazione della scansione ... 74
reazione alle minacce ... 71

Area attendibile
applicazioni attendibili ... 163
regole di esclusione ... 164

B

Backup
cancellazione di un archivio ... 180
Connessione di un archivio ... 180
creare un archivio ... 179
creazione di un'attività di backup ... 181
esecuzione di un'attività di backup ... 182
ricerca di copie di backup ... 182
rimozione di un archivio ... 181
ripristino dei dati ... 184
visualizzazione dei dati sulle copie di backup ... 183
visualizzazione del rapporto sugli eventi ... 184

Barra degli strumenti di Kaspersky
Anti-Virus Web ... 73

C

Cartella Condivisa
Modalità Protetta ... 92

Categorie di minacce rilevabili ... 162

Centro di controllo
aggiornamenti ... 243

analisi della protezione della rete ... 241
Backup ... 244
configurazione della gestione remota ... 240
Gestione dei componenti di protezione ... 242
gestione delle licenze ... 242
gestione di Parental Control ... 242
scansione remota di virus e vulnerabilità ... 243
Classificazione della pericolosità
Controllo Applicazioni ... 82
Controllo Applicazioni
algoritmo di funzionamento ... 81
ambito di protezione ... 83
classificazione della pericolosità ... 82
esclusioni ... 88
gruppi di applicazioni ... 82
modifica di una regola di applicazione ... 87
privilegi di eredità ... 81
regole di Controllo Applicazioni ... 85
sequenza di avvio dell'applicazione ... 83
Creazione di un collegamento
Modalità Protetta ... 90
Crittografia dei dati
aggiunta di file nel contenitore ... 207
configurazione del contenitore ... 207
connessione e disconnessione del contenitore ... 206
creazione di un contenitore ... 205

D

Database degli indirizzi di phishing
Anti-Spam ... 114
Anti-Virus IM ... 77
Anti-Virus Web ... 72
Difesa Proattiva
controllo degli account di sistema ... 104
elenco di attività pericolose ... 101
gruppo di applicazioni attendibili ... 103
regole per il monitoraggio delle attività pericolose ... 102

E

Eliminare i dati
Modalità Protetta ... 93
Esclusioni
Controllo Applicazioni ... 88

F

Fattore di probabile spam ... 120
Fattore di spam
Anti-Spam ... 108, 120
Firewall
Creazione guidata regole ... 98
estensione dell'intervallo degli indirizzi di rete ... 95
impostazioni della connessione di rete ... 99
modifica della categoria della rete ... 94
regola di applicazione ... 98
regola Firewall ... 96
regola per pacchetti ... 97
selezione delle azioni eseguite dalla regola ... 99
selezione dell'intervallo di indirizzi ... 100

G

Gestione delle password
Accesso al database delle password ... 213

account ... 215
avvio veloce delle funzioni dell'applicazione ... 228
dati personali ... 221
Generatore di password ... 238
gruppi di account ... 220
identità ... 219
importazione ed esportazione di password ... 222
metodo di crittografia ... 231
modifica della password master ... 234
nome utente. ... 219
pulsante Titolo ... 237
puntatore ... 239
ricerca di password ... 222

Gestore della posta
Anti-Spam ... 122

Gruppi di applicazioni
Controllo Applicazioni ... 82

L

Livello di protezione
Anti-Virus File ... 54
Anti-Virus Posta ... 63
Anti-Virus Web ... 71

M

Memoria di backup ... 170

Modalità Protetta
Cartella Condivisa ... 92
creazione di un collegamento ... 90
eliminare i dati ... 93
selezione della modalità ... 91, 92

Modifica di una regola di applicazione
Controllo Applicazioni ... 87

N

Network
porte monitorate ... 166

O

Ottimizzazione del sistema
configurazione del browser ... 196
Disco di Ripristino ... 198
Eliminazione definitiva dei dati ... 200
Eliminazione dei dati inutilizzati ... 201
Pulizia guidata dei dati riservati ... 202
ripristino dopo un'infezione ... 197

P

Parental Control
accesso a siti Web ... 188
attivazione e configurazione ... 186
download di file da Internet ... 188
esecuzione di applicazioni e giochi ... 193
esportazione e importazione delle impostazioni di Parental Control ... 194
invio di dati personali ... 191
limitazione del tempo di accesso a Internet ... 187
limitazione del tempo di utilizzo del computer ... 193
messaggistica immediata ... 190
modalità di ricerca sicura ... 189
ricerca per parole chiave ... 192

Pianifica
scansione anti-virus ... 138

Prevenzione Intrusioni
durata del blocco ... 105
sbloccare ... 105
tipi di attacchi di rete rilevati ... 105
Privilegi di eredità
Controllo Applicazioni ... 81

Q

Quarantena ... 169
Quarantena e Backup ... 169

R

Rapporti ... 172
filtraggio ... 177
ricerca eventi ... 177
salvataggio in un file ... 176
selezione di un componente o di un'attività ... 172
tipo di evento ... 174
Reazione alle minacce
Anti-Virus File ... 54
Anti-Virus Posta ... 64
Anti-Virus Web ... 71
scansione anti-virus ... 134
Regola di applicazione
Firewall ... 98
Regola Firewall
Firewall ... 96
Regola per pacchetti
Firewall ... 97
Regole di Controllo Applicazioni
Controllo Applicazioni ... 85
Rete
connessioni crittografate ... 167
Ripristino delle impostazioni predefinite
Anti-Spam ... 126
Anti-Virus File ... 61
Anti-Virus Posta ... 68

S

Scansione
account utente ... 139
avvio automatico delle attività ignorate ... 138
azione da eseguire sugli oggetti rilevati ... 134
l'avvio delle attività ... 131
livello di protezione ... 134
ottimizzazione della scansione ... 135
pianifica ... 138
scansione dei file compositi ... 136
scansione Vulnerabilità ... 140
tecnologie di scansione ... 137
tipo di oggetti da esaminare ... 135
Scansione Vulnerabilità
account utente ... 143
elenco di oggetti da esaminare ... 142
pianifica ... 142
Selezione della modalità
Modalità Protetta ... 91, 92
Sequenza di avvio dell'applicazione
Controllo Applicazioni ... 83