

KASPERSKY LAB

---

Kaspersky<sup>®</sup> Anti-Virus for Windows  
Workstations 6.0

MANUALE  
DELL'UTENTE

**KASPERSKY ANTI-VIRUS FOR WINDOWS  
WORKSTATIONS 6.0**

---

# Manuale dell'utente

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

Data revisione: Luglio 2007

# Sommario

|   |    |
|---|----|
| CAPITOLO 1. LE MINACCE ALLA SICUREZZA DEL COMPUTER.....                           | 11 |
| 1.1. Le minacce potenziali.....   | 11 |
| 1.2. La diffusione delle minacce.....   | 12 |
| 1.3. Tipi di minacce.....   | 14 |
| 1.4. Segnali di infezione.....  | 17 |
| 1.5. Come comportarsi se si sospetta un'infezione.....                            | 19 |
| 1.6. Prevenzione delle infezioni.....   | 19 |
| <br>  |    |
| CAPITOLO 2. KASPERSKY ANTI-VIRUS FOR WINDOWS WORKSTATIONS                         |    |
| 6.0.....  | 22 |
| 2.1. Novità di Kaspersky Anti-Virus for Windows Workstations 6.0.....             | 22 |
| 2.2. I componenti di difesa di Kaspersky Anti-Virus for Windows Workstations..... | 25 |
| 2.2.1. Componenti di protezione.....  | 26 |
| 2.2.2. Attività di scansione antivirus.....                                       | 28 |
| 2.2.3. Strumenti del programma.....   | 28 |
| 2.3. Requisiti di sistema hardware e software.....                                | 30 |
| 2.4. Pacchetti software.....  | 31 |
| 2.5. Assistenza per gli utenti registrati.....                                    | 32 |
| <br>  |    |
| CAPITOLO 3. INSTALLARE KASPERSKY ANTI-VIRUS FOR WINDOWS                           |    |
| WORKSTATIONS 6.0.....   | 33 |
| 3.1. Installazione tramite la procedura guidata.....                              | 34 |
| 3.2. Impostazione guidata.....  | 38 |
| 3.2.1. Uso di oggetti salvati con la versione 5.0.....                            | 39 |
| 3.2.2. Attivazione del programma.....   | 39 |
| 3.2.2.1. Scelta di un metodo di attivazione del programma.....                    | 39 |
| 3.2.2.2. Inserimento del codice di attivazione.....                               | 40 |
| 3.2.2.3. Come procurarsi un file chiave di licenza.....                           | 41 |
| 3.2.2.4. Selezione di un file chiave di licenza.....                              | 41 |
| 3.2.2.5. Completamento dell'attivazione del programma.....                        | 41 |
| 3.2.3. Selezione di una modalità di sicurezza.....                                | 42 |
| 3.2.4. Configurazione delle impostazioni di aggiornamento.....                    | 43 |
| 3.2.5. Pianificazione delle scansioni antivirus.....                              | 43 |

|   |           |
|---|-----------|
| 3.2.6. Restrizioni di accesso al programma .....                                      | 44        |
| 3.2.7. Configurazione delle impostazioni di Anti-Hacker .....                         | 45        |
| 3.2.7.1. Determinare lo stato di una zona di sicurezza .....                          | 45        |
| 3.2.7.2. Creazione di un elenco di applicazioni di rete .....                         | 47        |
| 3.2.8. Completamento della procedura di configurazione guidata .....                  | 48        |
| 3.3. Installazione del programma da riga di comando .....                             | 48        |
| 3.4. Procedura per installare l'Oggetto delle Regole di Gruppo .....                  | 49        |
| 3.4.1. Installazione del programma .....  | 49        |
| 3.4.2. Upgrade del programma .....  | 50        |
| 3.4.3. Disinstallazione del programma .....   | 50        |
| 3.5. Upgrade dalla versione 5.0 alla versione 6.0 .....                               | 51        |
| <b>CAPITOLO 4. INTERFACCIA DEL PROGRAMMA .....</b>                                    | <b>52</b> |
| 4.1. L'icona dell'area di notifica .....  | 52        |
| 4.2. Il menu di scelta rapida .....   | 53        |
| 4.3. La finestra principale del programma .....                                       | 55        |
| 4.4. Finestra delle impostazioni del programma .....                                  | 57        |
| <b>CAPITOLO 5. GUIDA INTRODUTTIVA .....</b>   | <b>59</b> |
| 5.1. Qual'è lo stato di protezione del computer? .....                                | 60        |
| 5.1.1. Indicatori della protezione .....  | 60        |
| 5.1.2. Stato dei componenti di Kaspersky Anti-Virus for Windows<br>Workstations ..... | 63        |
| 5.1.3. Statistiche sulle prestazioni del programma .....                              | 65        |
| 5.2. Come eseguire la scansione antivirus del computer .....                          | 65        |
| 5.3. Come eseguire la scansione di aree critiche del computer .....                   | 66        |
| 5.4. Come eseguire la scansione antivirus di un file, una cartella o un disco .....   | 67        |
| 5.5. Come istruire Anti-Spam .....  | 68        |
| 5.6. Come aggiornare il programma .....   | 69        |
| 5.7. Come comportarsi in caso di protezione non funzionante .....                     | 70        |
| <b>CAPITOLO 6. SISTEMA DI GESTIONE DELLA PROTEZIONE .....</b>                         | <b>72</b> |
| 6.1. Interruzione e ripristino della protezione del computer .....                    | 72        |
| 6.1.1. Sospensione della protezione .....   | 73        |
| 6.1.2. Interruzione della protezione .....  | 74        |
| 6.1.3. Sospensione/interruzione dei componenti di protezione e delle attività .....   | 75        |
| 6.1.4. Ripristino della protezione del computer .....                                 | 76        |
| 6.1.5. Chiusura del programma .....   | 76        |

---

|   |            |
|---|------------|
| 6.2. Tipi di programmi nocivi da monitorare.....                                      | 77         |
| 6.3. Creazione di una zona attendibile.....   | 78         |
| 6.3.1. Regole di esclusione .....   | 79         |
| 6.3.2. Applicazioni attendibili.....  | 84         |
| 6.4. Avvio di attività con un altro profilo.....                                      | 88         |
| 6.5. Configurazione delle attività pianificate e delle notifiche .....                | 89         |
| 6.6. Opzioni di alimentazione .....   | 91         |
| 6.7. Tecnologia avanzata di disinfezione.....   | 92         |
| <b>CAPITOLO 7. FILE ANTI-VIRUS .....</b>  | <b>93</b>  |
| 7.1. Selezione di un livello di sicurezza dei file .....                              | 94         |
| 7.2. Configurazione di File Anti-Virus.....   | 95         |
| 7.2.1. Definizione dei tipi di file da esaminare.....                                 | 96         |
| 7.2.2. Definizione dell'ambito della protezione.....                                  | 98         |
| 7.2.3. Configurazione delle impostazioni avanzate .....                               | 100        |
| 7.2.4. Ripristino delle impostazioni di File Anti-Virus .....                         | 103        |
| 7.2.5. Selezione delle azioni da applicare agli oggetti.....                          | 104        |
| 7.3. Riparazione posticipata .....  | 106        |
| <b>CAPITOLO 8. ANTI-VIRUS POSTA .....</b>   | <b>107</b> |
| 8.1. Selezione del livello di protezione della posta elettronica .....                | 108        |
| 8.2. Configurazione di Anti-Virus posta.....  | 110        |
| 8.2.1. Selezione di un gruppo di messaggi di posta elettronica protetti.....          | 110        |
| 8.2.2. Configurazione dell'elaborazione della posta in Microsoft Office Outlook ..... | 112        |
| 8.2.3. Configurazione della scansione della posta in The Bat! .....                   | 114        |
| 8.2.4. Ripristino delle impostazioni predefinite di Anti-Virus posta.....             | 116        |
| 8.2.5. Selezione di un'azione per gli oggetti di posta pericolosi .....               | 116        |
| <b>CAPITOLO 9. WEB ANTI-VIRUS .....</b>   | <b>119</b> |
| 9.1. Selezione del livello di protezione web .....                                    | 120        |
| 9.2. Configurazione di Web Anti-Virus.....  | 122        |
| 9.2.1. Impostazione di un metodo di scansione .....                                   | 122        |
| 9.2.2. Creazione di un elenco di indirizzi attendibili .....                          | 124        |
| 9.2.3. Ripristino delle impostazioni di Web Anti-Virus .....                          | 125        |
| 9.2.4. Selezione delle reazioni agli oggetti pericolosi .....                         | 125        |
| <b>CAPITOLO 10. DIFESA PROATTIVA .....</b>  | <b>127</b> |
| 10.1. Impostazioni di Difesa proattiva .....  | 129        |

|   |            |
|---|------------|
| 10.1.1. Regole di controllo delle attività.....   | 131        |
| 10.1.2. Office Guard.....   | 135        |
| 10.1.3. Registry Guard.....   | 136        |
| 10.1.3.1. Selezione delle chiavi di registro per creare una regola.....                 | 138        |
| 10.1.3.2. Creazione di una regola per Registry Guard.....                               | 139        |
| <b>CAPITOLO 11. ANTI-SPY.....</b>   | <b>142</b> |
| 11.1. Configurazione di Anti-Spy.....   | 144        |
| 11.1.1. Creazione di elenchi di indirizzi attendibili per Popup Blocker.....            | 144        |
| 11.1.2. Elenco di blocco dei banner pubblicitari.....                                   | 146        |
| 11.1.2.1. Configurazione dell'elenco di blocco dei banner pubblicitari<br>standard..... | 147        |
| 11.1.2.2. Liste bianche dei banner pubblicitari.....                                    | 148        |
| 11.1.2.3. Liste nere dei banner pubblicitari.....                                       | 149        |
| 11.1.3. Creazione di una lista dei numeri attendibili con Anti-Dialer.....              | 149        |
| <b>CAPITOLO 12. PROTEZIONE CONTRO GLI ATTACCHI DI RETE.....</b>                         | <b>151</b> |
| 12.1. Selezione di un livello di protezione di Anti-Hacker.....                         | 153        |
| 12.2. Regole delle applicazioni.....  | 154        |
| 12.2.1. Creazione manuale delle regole.....   | 156        |
| 12.2.2. Creazione di regole da un modello.....  | 157        |
| 12.3. Regole di filtraggio pacchetti.....   | 158        |
| 12.4. Aggiustamento delle regole per applicazioni e filtro pacchetti.....               | 160        |
| 12.5. Assegnazione della priorità alle regole.....                                      | 164        |
| 12.6. Regole per zone di sicurezza.....   | 165        |
| 12.7. Modalità Firewall.....  | 167        |
| 12.8. Configurazione del Sistema di rilevamento intrusioni.....                         | 169        |
| 12.9. Elenco degli attacchi di rete intercettati.....                                   | 170        |
| 12.10. Blocco e autorizzazione di attività di rete.....                                 | 173        |
| <b>CAPITOLO 13. PROTEZIONE DALLA POSTA INDESIDERATA.....</b>                            | <b>176</b> |
| 13.1. Selezione di un livello di sensibilità per Anti-Spam.....                         | 178        |
| 13.2. Addestramento di Anti-Spam.....   | 179        |
| 13.2.1. Procedura di apprendimento guidato.....   | 180        |
| 13.2.2. Addestramento con i messaggi in uscita.....                                     | 181        |
| 13.2.3. Training mediante il client di posta.....                                       | 181        |
| 13.2.4. Training sui rapporti di Anti-Spam.....   | 182        |
| 13.3. Configurazione di Anti-Spam.....  | 183        |

|  |            |
|--|------------|
| 13.3.1. Configurazione delle impostazioni di scansione.....                                | 184        |
| 13.3.2. Selezione delle tecnologie di filtraggio antispam.....                             | 185        |
| 13.3.3. Definizione dei fattori di spam e probabile spam.....                              | 186        |
| 13.3.4. Creazione manuale di liste bianche e liste nere.....                               | 187        |
| 13.3.4.1. Liste bianche di indirizzi e frasi.....  | 188        |
| 13.3.4.2. Liste nere di indirizzi e frasi.....   | 190        |
| 13.3.5. Ulteriori funzioni di filtraggio antispam.....                                     | 192        |
| 13.3.6. Recapito posta.....  | 193        |
| 13.3.7. Azioni da eseguire sui messaggi di spam.....                                       | 194        |
| 13.3.8. Configurazione dell'elaborazione della spam in Microsoft Office Outlook.....       | 195        |
| 13.3.9. Configurazione dell'elaborazione dello spam in Outlook Express (Windows Mail)..... | 198        |
| 13.3.10. Configurazione dell'elaborazione della spam in The Bat!.....                      | 199        |
| <b>CAPITOLO 14. SCANSIONE ANTI-VIRUS DEL COMPUTER.....</b>                                 | <b>202</b> |
| 14.1. Gestione delle attività di scansione antivirus.....                                  | 203        |
| 14.2. Creazione di un elenco di oggetti da esaminare.....                                  | 204        |
| 14.3. Creazione di attività di scansione antivirus.....                                    | 205        |
| 14.4. Configurazione delle attività di scansione antivirus.....                            | 206        |
| 14.4.1. Selezione di un livello di sicurezza.....  | 207        |
| 14.4.2. Definizione dei tipi di oggetti da sottoporre a scansione.....                     | 208        |
| 14.4.3. Ripristino delle impostazioni di scansione predefinite.....                        | 212        |
| 14.4.4. Selezione delle azioni da applicare agli oggetti.....                              | 212        |
| 14.4.5. Ulteriori impostazioni di scansione antivirus.....                                 | 214        |
| 14.4.6. Configurazione delle impostazioni di scansione globali per tutte le attività.....  | 216        |
| <b>CAPITOLO 15. TESTARE LE FUNZIONI DI KASPERSKY ANTI-VIRUS.....</b>                       | <b>217</b> |
| 15.1. Test del virus EICAR e delle sue varianti.....                                       | 217        |
| 15.2. Testare File Anti-Virus.....   | 219        |
| 15.3. Testare le attività di scansione anti-virus.....                                     | 220        |
| <b>CAPITOLO 16. AGGIORNAMENTI DEL PROGRAMMA.....</b>                                       | <b>222</b> |
| 16.1. Avvio della procedura di aggiornamento.....  | 224        |
| 16.2. Ripristino dell'aggiornamento precedente.....  | 224        |
| 16.3. Creazione delle attività di aggiornamento.....                                       | 225        |
| 16.4. Configurazione delle impostazioni di aggiornamento.....                              | 226        |

|   |            |
|---|------------|
| 16.4.1. Selezione di un'origine per l'aggiornamento.....                            | 227        |
| 16.4.2. Selezione di un metodo di aggiornamento e degli oggetti da aggiornare ..... | 229        |
| 16.4.3. Configurazione delle impostazioni di connessione .....                      | 231        |
| 16.4.4. Aggiornamento della cartella di distribuzione .....                         | 233        |
| 16.4.5. Azioni successive all'aggiornamento del programma .....                     | 234        |
| <b>CAPITOLO 17. OPZIONI AVANZATE.....</b>   | <b>236</b> |
| 17.1. Quarantena per gli oggetti potenzialmente infetti.....                        | 237        |
| 17.1.1. Azioni da eseguire sugli oggetti in Quarantena .....                        | 238        |
| 17.1.2. Configurazione della Quarantena .....                                       | 240        |
| 17.2. Copie di backup di oggetti pericolosi .....                                   | 241        |
| 17.2.1. Azioni da eseguire sulle copie di backup.....                               | 241        |
| 17.2.2. Configurazione delle impostazioni del Backup.....                           | 243        |
| 17.3. Rapporti .....  | 243        |
| 17.3.1. Configurazione delle impostazioni dei rapporti.....                         | 246        |
| 17.3.2. La scheda <i>Rilevati</i> .....   | 247        |
| 17.3.3. La scheda <i>Eventi</i> .....   | 248        |
| 17.3.4. La scheda <i>Statistiche</i> .....  | 249        |
| 17.3.5. La scheda <i>Impostazioni</i> .....   | 250        |
| 17.3.6. La scheda <i>Macro</i> .....  | 251        |
| 17.3.7. La scheda <i>Registro</i> .....   | 252        |
| 17.3.8. La scheda <i>Phishing</i> .....   | 253        |
| 17.3.9. La scheda <i>Popup</i> .....  | 253        |
| 17.3.10. La scheda <i>Banner</i> .....  | 254        |
| 17.3.11. La scheda <i>Composizioni automatiche numeri nascoste</i> .....            | 255        |
| 17.3.12. La scheda <i>Attacchi provenienti dalla rete</i> .....                     | 255        |
| 17.3.13. La scheda <i>Computer esclusi</i> .....                                    | 256        |
| 17.3.14. La scheda <i>Attività applicazione</i> .....                               | 257        |
| 17.3.15. La scheda <i>Filtri pacchetti</i> .....                                    | 257        |
| 17.3.16. La scheda <i>Connessioni stabilite</i> .....                               | 258        |
| 17.3.17. La scheda <i>Porte aperte</i> .....  | 259        |
| 17.3.18. La scheda <i>Traffico</i> .....  | 259        |
| 17.4. Informazioni generali sul programma .....                                     | 260        |
| 17.5. Gestione delle licenze .....  | 261        |
| 17.6. Supporto tecnico.....   | 263        |
| 17.7. Creazione di un elenco delle porte monitorate.....                            | 264        |



---

|   |            |
|---|------------|
| 17.8. Controllo delle connessioni crittografate.....  | 266        |
| 17.9. Configurazione dell'interfaccia di Kaspersky Anti-Virus for Windows Workstations .....                  | 268        |
| 17.10. Disco di emergenza .....   | 270        |
| 17.10.1. Creazione di un disco di emergenza .....   | 271        |
| 17.10.2. Uso del disco di emergenza.....  | 273        |
| 17.11. Utilizzo di servizi supplementari .....  | 274        |
| 17.11.1. Notifica eventi di Kaspersky Anti-Virus for Windows Workstations .....                               | 275        |
| 17.11.1.1. Tipi di eventi e metodo di notifica .....  | 275        |
| 17.11.1.2. Configurazione delle notifiche via posta elettronica .....   | 277        |
| 17.11.1.3. Configurazione delle impostazioni del registro eventi .....  | 278        |
| 17.11.2. Protezione automatica e limitazioni d'accesso.....   | 279        |
| 17.11.3. Risoluzione dei conflitti con altre applicazioni.....  | 281        |
| 17.12. Importazione ed esportazione delle impostazioni di Kaspersky Anti-Virus for Windows Workstations ..... | 282        |
| 17.13. Ripristino delle impostazioni predefinite .....  | 283        |
| <b>CAPITOLO 18. USO DEL PROGRAMMA DA RIGA DI COMANDO .....</b>  | <b>284</b> |
| 18.1. Attivazione dell'applicazione .....   | 286        |
| 18.2. Gestione dei componenti e delle attività del programma.....   | 286        |
| 18.3. Scansioni antivirus.....  | 290        |
| 18.4. Aggiornamenti del programma .....   | 294        |
| 18.5. Impostazioni di rollback .....  | 295        |
| 18.6. Esportazione delle impostazioni .....   | 296        |
| 18.7. Importazione delle impostazioni.....  | 297        |
| 18.8. Avvio del programma .....   | 298        |
| 18.9. Arresto del programma .....   | 298        |
| 18.10. Ottenere un file traccia .....   | 299        |
| 18.11. Visualizzazione della Guida .....  | 299        |
| 18.12. Codici restituiti dall'interfaccia a riga di comando.....  | 300        |
| <b>CAPITOLO 19. MODIFICA, RIPARAZIONE E DISINSTALLAZIONE DEL PROGRAMMA .....</b>                              | <b>301</b> |
| 19.1. Modifica, riparazione e rimozione del programma tramite la procedura guidata d'installazione.....       | 301        |
| 19.2. Disinstallazione del programma da riga di comando .....   | 304        |
| <b>CAPITOLO 20. GESTIONE DELL'APPLICAZIONE PER MEZZO DI KASPERSKY ADMINISTRATION KIT .....</b>                | <b>305</b> |

|  |     |
|--|-----|
| 20.1. Amministrazione dell'applicazione .....                            | 308 |
| 20.1.1. Avvio/arresto dell'applicazione .....                            | 309 |
| 20.1.2. Configurazione delle impostazioni dell'applicazione .....        | 310 |
| 20.1.3. Configurazione delle impostazioni specifiche .....               | 312 |
| 20.2. Gestione delle attività .....                                      | 313 |
| 20.2.1. Avvio e arresto delle attività .....                             | 315 |
| 20.2.2. Creazione delle attività .....                                   | 315 |
| 20.2.2.1. Creazione delle attività locali .....                          | 316 |
| 20.2.2.2. Creazione delle attività di gruppo .....                       | 318 |
| 20.2.2.3. Creazione delle attività globali .....                         | 318 |
| 20.2.3. Configurazione di impostazioni specifiche dell'attività .....    | 319 |
| 20.3. Gestione delle regole .....  | 320 |
| 20.3.1. Creazione di regole .....  | 320 |
| 20.3.2. Visualizzazione e modifica delle impostazioni delle regole ..... | 323 |
| CAPITOLO 21. DOMANDE FREQUENTI .....                                     | 325 |
| APPENDICE A. INFORMAZIONI DI RIFERIMENTO .....                           | 327 |
| A.1. Elenco dei file esaminati in base all'estensione .....              | 327 |
| A.2. Maschere di esclusione file possibili .....                         | 329 |
| A.3. Maschere di esclusione minacce possibili .....                      | 331 |
| A.4. Panoramica delle impostazioni in <i>setup.ini</i> .....             | 331 |
| APPENDICE B. KASPERSKY LAB .....   | 333 |
| B.1. Altri prodotti Kaspersky Lab .....                                  | 334 |
| B.2. Recapiti .....  | 345 |
| APPENDICE C. CONTRATTO DI LICENZA .....                                  | 346 |

---

# CAPITOLO 1. LE MINACCE ALLA SICUREZZA DEL COMPUTER

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

I criminali informatici hanno mostrato grande interesse per le attività delle strutture statali e delle imprese commerciali. Essi cercano di impadronirsi di e divulgare informazioni riservate, che danneggia la reputazione delle imprese, interrompe la continuità delle attività commerciali e può pregiudicare le risorse informatiche delle organizzazioni. Questi atti possono recare gravi danni a beni materiali e immateriali.

Non sono solo le grandi società ad essere a rischio, anche i singoli utenti possono essere attaccati. I criminali riescono ad accedere ai dati personali (numero di conto corrente e carta di credito, password, ecc.), provocando anomalie di funzionamento del computer. Alcuni tipi di attacchi consentono agli hacker di avere accesso totale ad un computer, che può quindi essere utilizzato come elemento di una rete "zombie", cioè una rete di computer infetti usati dagli hacker per attaccare server, inviare spam, impadronirsi di informazioni riservate e diffondere nuovi virus e trojan.

Oggiogni chiunque riconosce il valore delle informazioni ed è consapevole della necessità di proteggere i dati. Al tempo stesso le informazioni deve essere facilmente accessibili a chi ne ha legittimamente bisogno (per esempio dipendenti, clienti e partner di un'impresa). Ecco quindi la necessità di creare un sistema di sicurezza completo per le informazioni, che deve tenere conto di tutte le possibili minacce, siano esse umane, prodotte dall'uomo o conseguenze di catastrofi naturali, e applicare una serie completa di misure protettive a livello fisico, amministrativo e di software.

## 1.1. Le minacce potenziali

Singole persone, gruppi di persone o addirittura fenomeni non legati ad attività umane rappresentano potenziali minacce per la sicurezza dei dati. Partendo da questo presupposto, tutte le fonti di pericolo possono essere suddivise in tre gruppi:

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

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

## 1.2. La diffusione delle minacce

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

### Internet

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

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

Gli hacker diffondono virus e altri programmi nocivi sui siti Internet, mascherandoli come utili programmi gratuiti. Inoltre gli script eseguiti automaticamente all'apertura di alcune pagine Web sono in grado di eseguire azioni pericolose sul computer, fra cui la modifica del registro di sistema, il furto di dati personali e l'installazione di software nocivi.

Grazie alle tecnologie di rete, gli hacker possono attaccare PC e server aziendali remoti. Questi attacchi possono provocare il malfunzionamento di parti del sistema, oppure dare agli hacker l'accesso completo al

sistema stesso e alle informazioni in esso memorizzate. Il sistema può essere utilizzato anche come elemento di una rete “zombie”.

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

### **Intranet**

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

### **Posta elettronica**

Poiché quasi tutti i computer hanno un client di posta elettronica installato e i programmi nocivi sfruttano i contenuti delle rubriche elettroniche, la diffusione di programmi nocivi può contare su condizioni ottimali. L'utente di un computer infetto, può inconsapevolmente inviare messaggi di posta elettronica infetti ad amici o colleghi che a loro volta inviano ulteriori messaggi infetti. Ad esempio, succede spesso che i file infetti passino inosservati e vengano inviati unitamente a informazioni aziendali nel sistema di posta elettronica interna di una grande società. Quando ciò avviene, sono molti gli utenti che vengono infettati. Potrebbe trattarsi di centinaia o migliaia di dipendenti dell'azienda, oltre alle eventuali decine di migliaia di abbonati.

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

Gli hacker, inoltre, hanno iniziato a fare uso di programmi di mass mailing e di tecniche di social engineering per convincere gli utenti ad aprire messaggi e-mail o a fare clic su un collegamento ad un determinato sito web. Di conseguenza, la capacità di filtrare la spam è utile per diversi motivi: per fermare la posta indesiderata; per reagire ai nuovi tipi di truffe on-line, come il phishing; infine, per arrestare la diffusione di programmi nocivi.

### **Supporti di archiviazione esterni**

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

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

## 1.3. Tipi di minacce

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

### **Worm**

Questa categoria di programmi nocivi si diffonde principalmente sfruttando le vulnerabilità dei sistemi operativi. Essi devono il loro nome (in italiano, "verme") alla capacità di strisciare da un computer all'altro attraverso le reti e la posta elettronica. Questa caratteristica consente ai worm di diffondersi molto rapidamente.

Quando un worm penetra in un computer, ricerca l'indirizzo di rete degli altri computer accessibili a livello locale e invia molteplici copie di sé stesso a questi indirizzi. Inoltre, i worm utilizzano spesso i dati prelevati dalle rubriche dei clienti di posta elettronica. Alcuni di questi programmi nocivi talvolta creano file funzionanti sui dischi di sistema, ma possono eseguirsi anche senza alcuna risorsa di sistema tranne la RAM.

### **Virus**

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

### **Trojan**

Sono programmi che eseguono azioni non autorizzate sui computer, per esempio la cancellazione di dati sui drive provocando il blocco del sistema, il furto di informazioni riservate, ecc. Questa categoria di programmi nocivi non può essere definita virus nel senso tradizionale del termine in quanto non infetta altri computer o dati. I trojan non possono irrompere autonomamente nei computer. Vengono diffusi dagli hacker, che li camuffano da software regolare. Il danno che provocano può essere molto maggiore di quello inferto dai virus tradizionali.

Ultimamente, la categoria più diffusa di programmi nocivi che danneggiano i dati sui computer è stata quella dei worm, seguita da virus e trojan. Alcuni programmi nocivi combinano le caratteristiche di due o addirittura tre di queste categorie.

## Adware

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

## Spyware

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

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

## Riskware

Le applicazioni a rischio comprendono i software che non hanno funzioni nocive vere e proprie, ma che potrebbero far parte dell'ambiente di sviluppo per programmi pericolosi o essere utilizzati dai pirati informatici come componenti ausiliari per programmi pericolosi. Questa categoria di programmi include i programmi con backdoor e vulnerabilità, come anche alcune utilità di amministrazione remota, commutatori di tastiera, client IRC, server FTP e utilità multifunzione per interrompere processi o per nascondere il funzionamento.

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

## Joke

Si tratta di software che non reca alcun danno diretto ma visualizza messaggi secondo i quali il danno è già stato provocato o lo sarà in circostanze particolari. Questi programmi spesso comunicano all'utente la presenza di rischi inesistenti, per esempio relativi alla formattazione del

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

### **Rootkit**

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

### **Altri programmi pericolosi**

Si tratta di programmi creati, ad esempio, per lanciare attacchi DoS (Denial of Service) su server remoti e penetrare in altri computer; essi fanno parte dell'ambiente di sviluppo dei programmi nocivi. Essi includono hack tool, virus builder, scanner di vulnerabilità, programmi di individuazione di password, e altri tipi di programma per penetrare in un sistema o utilizzare risorse di rete.

### **Attacchi di pirateria informatica**

Gli attacchi degli hacker possono essere lanciati sia dagli hacker che da programmi nocivi. Essi hanno lo scopo di sottrarre informazioni da un computer remoto provocando il malfunzionamento del sistema, oppure di ottenere il controllo completo delle risorse del computer. Per una descrizione dettagliata dei tipi di attacchi che Kaspersky Anti-Virus for Windows Workstations è in grado di bloccare, consultare la sezione 12.9 a pag. 170.

### **Alcuni tipi di truffe online**

Il **Phishing** è una truffa online che utilizza i messaggi di posta elettronica di massa per sottrarre informazioni riservate all'utente, generalmente di natura finanziaria. I messaggi inviati a tal fine sono concepiti in modo da indurre a credere per quanto possibile che si tratti di e-mail informative da parte di istituti di credito e note aziende. Tali messaggi di posta elettronica contengono collegamenti a siti web falsi creati dagli hacker ad imitazione dell'organizzazione legittima. Su questo sito, l'utente viene invitato ad immettere, per esempio, il proprio numero di carta di credito e altre informazioni riservate.

**Dialer a siti web a pagamento** – è un tipo di truffa online che utilizza senza autorizzazione servizi a pagamento su Internet, che sono di solito siti web di natura pornografica. I dialer installati dagli hacker stabiliscono il contatto via modem tra il computer colpito e il numero telefonico del servizio a pagamento. Questi numeri telefonici hanno spesso tariffe altissime e l'utente è costretto a pagare bollette telefoniche salatissime.



## Messaggi pubblicitari importuni

Ne fanno parte le finestre a comparsa (popup) e i banner pubblicitari che si aprono durante la navigazione. Le informazioni contenute in queste finestre sono generalmente inutili. I popup e i banner distraggono l'utente dall'occupazione che stava svolgendo e consumano larghezza di banda.

## Spam

La posta spam consiste in messaggi anonimi non desiderati e comprende diversi tipi di contenuti: pubblicità; messaggi politici; richieste di assistenza; messaggi che invitano a investire grandi somme di denaro o a farsi coinvolgere in strutture piramidali, i messaggi volti a sottrarre password e numeri di carte di credito e quelli per i quali si chiede l'inoltro a tutte le persone conosciute (catene di S. Antonio).

La spam aumenta significativamente il carico sui server di posta e il rischio di perdere dati importanti.

Kaspersky Anti-Virus for Windows Workstations utilizza due metodi per rilevare e bloccare questi tipi di minacce:

- *Reattivo* – questo metodo ricerca i file nocivi utilizzando un database dell'elenco dei virus regolarmente aggiornato. L'implementazione di questo metodo richiede almeno un'infezione - per aggiungere la minaccia ai database e distribuire un aggiornamento al database stesso.
- *Proattivo* – contrariamente alla protezione reattiva, questo metodo non si basa sull'analisi del codice dell'oggetto ma sull'analisi del suo comportamento nel sistema. Questo metodo è volto a rilevare nuovi virus non ancora identificati.

Impiegando entrambi i metodi, Kaspersky Anti-Virus for Windows Workstations fornisce una protezione completa al computer da virus sia noti che sconosciuti.

### Attenzione:

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

## 1.4. Segnali di infezione

Numerosi segni indicano che un computer è infetto. I seguenti eventi sono buoni indicatori della probabile infezione del computer da parte di un virus:

- Il video visualizza messaggi o immagini impreviste, oppure il computer emette suoni anomali;

- Il lettore CD/DVD-ROM si apre e si chiude inaspettatamente;
- Il computer apre arbitrariamente un programma non richiesto dall'utente;
- Il video visualizza sullo schermo messaggi pop-up che comunicano che un determinato programma sta cercando di accedere a Internet, anche se tale azione non è stata richiesta dall'utente.

Anche l'infezione tramite posta elettronica presenta numerosi tratti caratteristici:

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

Occorre specificare che questi segnali possono anche essere dipendere da altre cause, diverse dai virus. Per esempio, nel caso di un messaggio di posta elettronica, i messaggi infetti possono essere inviati con l'indirizzo del mittente, ma non dal proprio computer.

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

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

Nel 90% dei casi, questi sistemi indiretti sono causati da malfunzionamento a livello hardware o software. Benché questi sintomi indichino raramente che il computer è infetto, si raccomanda, non appena li si rileva, di eseguire una scansione completa del computer (vedere 5.2 a pag. 65).

## 1.5. Come comportarsi se si sospetta un'infezione

*Se il computer ha un comportamento sospetto...*

1. Evitare il panico! Questa regola d'oro può scongiurare la perdita di dati importanti.
2. Scollegare il computer da Internet o da un'eventuale rete locale.
3. Se il computer non riesce a partire dal disco fisso (il computer visualizza un messaggio d'errore all'accensione), provare ad avviare la macchina in modalità provvisoria o dal dischetto di emergenza del sistema operativo creato durante la sua installazione.
4. Prima di eseguire qualsiasi operazione, effettuare una copia di backup del lavoro su un supporto esterno (floppy, CD/DVD, unità flash, ecc.).
5. Installare Kaspersky Anti-Virus for Windows Workstations, se non si è già provveduto.
6. Aggiornare gli elenchi delle minacce del programma e i moduli dell'applicazione (vedere 5.6 a pag. 69). Se possibile, scaricare gli aggiornamenti accedendo a Internet da un altro computer non infetto, per esempio quello di un amico, in un Internet point o in ufficio. È consigliabile utilizzare un computer diverso, poiché connettendosi a Internet da un computer infetto è probabile che il virus invii informazioni importanti agli hacker o si diffonda agli indirizzi presenti nella rubrica. Per questa ragione, se si sospetta di avere un virus, la cosa migliore da fare è scollegarsi immediatamente da Internet. È possibile procurarsi gli aggiornamenti degli elenchi delle minacce anche su un dischetto floppy da Kaspersky Lab o dai suoi distributori e aggiornare l'elenco dei virus dal dischetto.
7. Selezionare il livello di sicurezza raccomandato dagli esperti di Kaspersky Lab.
8. Avviare una scansione completa del computer (vedere 5.2 a pag. 65).

## 1.6. Prevenzione delle infezioni

Neanche le misure più affidabili e dirette possono garantire una protezione al 100% dai virus e dai trojan, ma tenendo presente alcune regole si può significativamente ridurre la probabilità di attacchi di virus e il conseguente danno potenziale.

Uno dei metodi base per combattere i virus è, come nella medicina, la *prevenzione* tempestiva. La profilassi del computer comporta poche regole che, se rispettate, possono ridurre in maniera considerevole la probabilità di incorrere in un virus e perdere dati.

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

**Regola n. 1:** *Utilizzare un software antivirus e programmi di sicurezza quando si naviga su Internet. Per fare ciò:*

- Installare Kaspersky Anti-Virus for Windows Workstations appena possibile.
- Aggiornare regolarmente gli elenchi delle minacce del programma (vedere 5.6 a pag. 69). L'elenco deve essere aggiornato più volte al giorno durante le epidemie. In queste situazioni, l'elenco delle minacce sui server di aggiornamento di Kaspersky Lab viene immediatamente aggiornato.
- Selezionare le impostazioni di sicurezza raccomandate da Kaspersky Lab per il computer. In questo modo il computer sarà protetto costantemente dal momento dell'accensione e per i virus sarà più difficile infettare il computer.
- Selezionare le impostazioni di scansione completa raccomandate da Kaspersky Lab e pianificare le scansioni almeno una volta la settimana. Se non si è installato Anti-Hacker, si raccomanda di provvedere in modo da proteggere il computer durante la navigazione.

**Regola n. 2:** *Prestare attenzione quando si copiano nuovi dati sul computer.*

- Esaminare tutte le unità di memoria rimovibili, quali i floppy, i CD/DVD e le unità flash, per individuare eventuali virus prima di utilizzarle (vedere 5.4 a pag. 67).
- Trattare i messaggi di posta elettronica con cautela. Evitare di aprire qualsiasi file allegato ai messaggi, a meno che non si sia certi che si tratti di un invio legittimo, anche se il mittente è una persona conosciuta.
- Trattare con prudenza qualsiasi informazione ottenuta tramite Internet. Se un sito web suggerisce di installare un nuovo programma, verificare che esso abbia un certificato di sicurezza.
- Se si sta copiando un file eseguibile da Internet o dalla rete locale, verificare di analizzarlo mediante Kaspersky Anti-Virus for Windows Workstations.
- Visitare i siti web con prudenza. Molti siti sono infetti da script pericolosi o worm di Internet.

**Regola nr. 3:** *Prestare molta attenzione alle informazioni ricevute da Kaspersky Lab.*

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

**Regola n. 4:** *Non fidarsi delle burle sui virus*, come programmi e messaggi di posta elettronica riguardanti le minacce di infezione.

**Regola n. 5:** *Utilizzare il tool Windows Update* e installare regolarmente gli aggiornamenti del sistema operativo Windows.

**Regola n. 6:** *Acquistare copie legittime del software dai distributori ufficiali.*

**Regola n. 7:** *Limitare il numero di persone autorizzate ad utilizzare il proprio computer.*

**Regola n. 8:** *Diminuire il rischio di conseguenze spiacevoli di una potenziale infezione:*

- Eseguire regolarmente una copia di backup dei dati. Se si perdono i dati, il sistema sarà in grado di ripristinarli piuttosto rapidamente se si dispone di copie di backup. Conservare in un luogo sicuro i dischetti floppy, i CD, le unità flash e altri supporti di archiviazione contenenti software e informazioni importanti.
- Creare un disco di emergenza (vedere 17.10 a pag. 270) con il quale avviare il computer, utilizzando un sistema operativo pulito.

**Regola n. 9:** *Ispezionare regolarmente l'elenco dei programmi installati sul computer.* A tal fine, aprire **Installazione applicazioni** nel **Pannello di controllo** oppure aprire la directory **Programmi**. Qui è possibile scoprire che è stato installato del software a insaputa dell'utente, per esempio, mentre si stava navigando in Internet o durante l'installazione di un altro programma. I programmi come questi sono molto spesso potenzialmente pericolosi.

---

# CAPITOLO 2. KASPERSKY ANTI-VIRUS FOR WINDOWS WORKSTATIONS 6.0

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

Ciò che realmente distingue Kaspersky Anti-Virus for Windows Workstations 6.0 da altri software, anche da altri prodotti Kaspersky Lab, è l'approccio multifaccettato alla sicurezza dei dati.

## 2.1. Novità di Kaspersky Anti-Virus for Windows Workstations 6.0

Kaspersky Anti-Virus for Windows Workstations 6.0 ha un approccio nuovo alla sicurezza dei dati. La caratteristica principale del programma è la combinazione in un'unica soluzione delle funzioni esistenti di tutti i prodotti dell'azienda, in versione potenziata. Il programma offre protezione contro gli attacchi dei virus, della posta spam, degli hacker, nonché dalle minacce sconosciute, dal phishing e dai rootkit.

In altre parole, garantisce una sicurezza globale del computer senza la necessità di installare numerosi prodotti. Solo questo è un valido motivo per installare Kaspersky for Windows Workstations 6.0.

La protezione completa difende tutti i canali dati in entrata ed in uscita. Tutti i componenti del programma offrono impostazioni flessibili che consentono di adattare Kaspersky Anti-Virus for Windows Workstations alle necessità di qualunque utente. La configurazione del programma può essere effettuata da una singola posizione.

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

### *Nuove funzionalità di protezione*

- Kaspersky Anti-Virus for Windows Workstations protegge il computer sia dai programmi nocivi noti che da quelli ancora ignoti. La difesa proattiva (vedere Capitolo 10 a pag. 127) è il vantaggio principale del programma. Esso analizza il comportamento delle applicazioni installate sul computer,

monitorare le modifiche al registro di sistema, individuare le macro e combattere le minacce nascoste. Il componente si avvale di un analizzatore euristico per rilevare e registrare diversi tipi di attività nociva, per poter quindi annullare le azioni eseguite dai programmi nocivi e ripristinare il sistema allo stato precedente l'attività nociva.

- Il programma protegge il computer da rootkit e dialer, blocca i banner pubblicitari, le finestre popup e gli script nocivi scaricati dalle pagine web, e individua i siti di phishing.
- La tecnologia File Anti-Virus è stata migliorata per ridurre il carico sulla CPU e aumentare la rapidità delle scansioni antivirus sui file. Così facendo, il programma esclude la possibilità di esaminare due volte lo stesso file.
- Il processo di scansione si svolge ora come attività in background, consentendo all'utente di continuare ad usare il computer. Se più programmi si disputano le risorse di sistema, la scansione anti-virus entra in pausa finché l'utente non ha terminato la propria attività, per poi riprendere da dove era stata interrotta.
- Alle aree critiche del computer, dove le infezioni potrebbero danneggiare gravemente la qualità o la sicurezza dei dati, vengono assegnate attività distinte. È possibile configurare quest'attività in modo che venga eseguita automaticamente ad ogni avvio del sistema.
- La protezione dei sistemi di posta elettronica contro i programmi nocivi e lo spam è stata considerevolmente migliorata. Il programma esamina questi protocolli alla ricerca di messaggi contenenti virus o classificabili come spam:
  - IMAP, SMTP, POP3, indipendentemente dal client di posta utilizzato
  - NNTP (solo scansione anti-virus), indipendentemente dal client di posta
  - Indipendentemente dal protocollo (sia MAPI che HTTP) se si utilizzano i plug-in per MS Outlook e The Bat!
- Sono disponibili plug-in specifici per i client di posta più comuni come Outlook, Microsoft Outlook Express (Windows Mail) e The Bat! Questi offrono la protezione della posta sia contro i virus che la spam, direttamente dal client di posta.
- Anti-Spam dispone ora di una modalità di addestramento basata sull'algoritmo iBayes, che apprende monitorando come l'utente gestisce la posta elettronica. Garantisce inoltre la massima flessibilità nella configurazione della posta spam – ad esempio, è possibile compilare liste

bianche e liste nere di indirizzi di mittenti e di espressioni ricorrenti nei messaggi identificati come spam.

Anti-Spam si avvale di un database di phishing in grado di escludere tutte le e-mail studiate per procurare informazioni confidenziali di natura finanziaria.

- Il programma filtra la posta in arrivo e quella in uscita, individua e blocca le minacce da attacchi di rete comuni e consente di utilizzare Internet in modalità invisibile.
- Quando si utilizza una combinazione di reti, è possibile inoltre specificare le reti completamente attendibili e quelle da monitorare con estrema attenzione.
- La funzione di notifica dell'utente (vedere 17.11.1 a pag. 275) è stata ampliata includendo determinati eventi che si verificano durante il funzionamento del programma. Il metodo di notifica può essere selezionato autonomamente per ciascuno di questi tipi di eventi: e-mail, notifiche sonore, messaggi pop-up.
- È stata aggiunta la scansione per i dati trasmessi su connessioni SSL protette.
- Il programma dispone ora di funzioni di auto-difesa, tra cui la protezione contro gli strumenti di amministrazione remota non autorizzati e la protezione delle impostazioni del programma tramite password. Queste funzioni impediscono ai programmi nocivi, agli hacker e agli utenti non autorizzati di disabilitare la protezione.
- È inoltre possibile creare un disco di emergenza, col quale è possibile riavviare il sistema operativo dopo un'epidemia di virus ed esaminare il computer alla ricerca di codici nocivi.
- Il sistema di protezione offre ora la funzione di amministrazione remota centralizzata, tramite un'interfaccia di amministrazione aggiunta sotto Kaspersky Administration Kit.

#### *Nuove funzioni dell'interfaccia del programma*

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



### *Nuove funzioni di aggiornamento del programma*

- Questa versione del programma introduce una nuova e più potente procedura di aggiornamento: Kaspersky Anti-Virus verifica automaticamente la sorgente degli aggiornamenti per nuovi aggiornamenti. Se trova nuovi aggiornamenti, il programma li scarica e li installa sul computer.
- Il programma scarica gli aggiornamenti in maniera incrementale, ignorando i file già scaricati. Questo riduce il traffico di download degli aggiornamenti di anche 10 volte.
- Gli aggiornamenti vengono scaricati dalla sorgente più efficiente.
- Oggi è possibile scegliere di non utilizzare un server proxy, scaricando gli aggiornamenti del programma da un'origine locale. Ciò riduce considerevolmente il carico sul server proxy.
- Il programma è dotato di una funzione di rollback che consente di ripristinare la precedente versione dell'elenco dei virus se quello installato risulta danneggiato o si è verificato un errore durante la copia.
- La funzione di aggiornamento comprende ora uno strumento che rende gli aggiornamenti accessibili agli altri computer della rete copiandoli in una cartella locale. Ciò riduce il traffico Internet.

## 2.2. I componenti di difesa di Kaspersky Anti-Virus for Windows Workstations

Kaspersky Anti-Virus for Windows Workstations è stato studiato tenendo conto delle provenienze delle minacce. In altre parole, ogni tipo di minaccia è gestito da un componente distinto del programma, che lo monitora e lo affronta con le misure necessarie a impedirne gli effetti nocivi sui dati dell'utente. Questa struttura rende flessibile la Security Suite, offrendo opzioni di facile utilizzo per tutti i componenti in modo da soddisfare le esigenze di utenti specifici o aziende nella loro globalità.

Kaspersky Anti-Virus for Windows Workstations include:

- Componenti di protezione (vedere 2.2.1 a pag. 26) che difendono complessivamente tutti i canali di trasmissione e scambio dati sul computer in tempo reale.

- Attività di scansione anti-virus (vedere 2.2.2 a pag. 28) che esaminano la memoria ed il file system del computer come anche singoli file, cartelle, dischi o aree alla ricerca di virus.
- Strumenti di supporto (vedere 2.2.3 a pag. 28) che offrono assistenza sul programma e ne estendono le funzionalità.

## 2.2.1. Componenti di protezione

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

### File Anti-Virus

Un file system può contenere virus e altri programmi pericolosi. I programmi nocivi possono restare inattivi nel file system per anni dopo esservi stati introdotti attraverso un dischetto floppy o da Internet, senza mostrare affatto la propria presenza. Ma è sufficiente accedere al file infetto per attivare istantaneamente il virus.

*File Anti-Virus* è il componente che controlla il file system del computer. Esamina tutti i file che vengono aperti, eseguiti o salvati sul computer e tutte le unità disco collegate. Kaspersky Anti-Virus intercetta ogni tentativo di accedere ad un file e lo esamina alla ricerca di virus noti. Se per qualsiasi motivo non è possibile disinfettare un file, esso viene eliminato dopo averne salvata una copia nella cartella Backup (vedere 17.2 a pag. 241), o trasferito in Quarantena (vedere 17.1 a pag. 237).

### Anti-Virus posta

La posta elettronica è molto utilizzata dagli hacker per diffondere programmi nocivi e rappresenta uno dei canali più comuni per la diffusione di worm. Pertanto, è importantissimo controllare tutti i messaggi di posta elettronica

Il componente *Anti-Virus posta* analizza tutte le e-mail in entrata e in uscita sul computer. Analizza la posta elettronica alla ricerca di programmi nocivi, consentendo al destinatario di aprire il messaggio solo se privo di oggetti pericolosi.

### Web Anti-Virus

Quando si accede ai diversi siti Web su Internet, si rischia di infettare il computer con i virus che vengono installati tramite gli script memorizzati sulle pagine web. Si rischia inoltre di scaricare un file pericoloso sul computer.

*Web Anti-Virus* è progettato appositamente per combattere tali rischi, intercettando e bloccando gli script sui siti Web se questi costituiscono una minaccia, e monitorando tutto il traffico HTTP.

### **Difesa proattiva**

Ogni giorno compaiono nuovi programmi nocivi in quantità crescente. Essi diventano sempre più complessi combinando più tipi di minaccia, e i metodi utilizzati per diffondersi cambiano diventando sempre più difficili da rilevare.

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

### **Anti-Spy**

I programmi che visualizzano messaggi pubblicitari indesiderati (ad esempio, i banner pubblicitari e le finestre popup), i programmi che si collegano a numeri telefonici per servizi Internet a pagamento senza l'autorizzazione dell'utente, gli strumenti di amministrazione e monitoraggio in remoto, i programmi joke, ecc., sono sempre più diffusi.

*Anti-Spy* registra queste azioni sul computer e le blocca. Per esempio, blocca i banner pubblicitari e le finestre popup, blocca i programmi che cercano di collegarsi a numeri di telefono, e analizza le pagine web per escludere la presenza di contenuti di phishing.

### **Anti-Hacker**

Gli hacker sfruttano ogni potenziale falla del sistema per invadere i computer, sia che si tratti di una porta aperta o di trasmissioni dati tra computer, ecc.

Il componente *Anti-Hacker* protegge il computer mentre si utilizza Internet o altre reti. Controlla le connessioni in entrata e in uscita e esamina le porte e i pacchetti di dati.

### **Anti-Spam**

Anche se non rappresenta una minaccia diretta per il computer, lo spam incrementa il carico sui server di posta elettronica, riempie la casella di posta e fa perdere tempo, provocando danni finanziari.

Il componente *Anti-Spam* si inserisce nel client di posta installato sul computer e ne esamina tutta la posta in entrata verificando la presenza di spam. Il componente contrassegna tutta la posta spam con una speciale

intestazione. Anti-Spam può essere configurato per elaborare lo spam nel modo desiderato (eliminazione automatica, spostamento in una data cartella, ecc.).

## 2.2.2. Attività di scansione antivirus

Oltre a monitorare costantemente i potenziali accessi di programmi nocivi, è estremamente importante eseguire periodicamente la scansione antivirus del computer. Ciò è necessario al fine di rilevare i programmi nocivi non ancora rilevati dal programma, ad esempio a causa della protezione impostata su un livello insufficiente.

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

### **Aree critiche**

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

### **Risorse del computer**

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

### **Oggetti di avvio**

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

È possibile inoltre creare altre attività di scansione anti-virus e pianificarne l'esecuzione. Per esempio, si può creare un'attività di scansione del database di posta per ricercare eventuali virus una volta alla settimana, oppure creare una scansione antivirus per la cartella **Documenti**.

## 2.2.3. Strumenti del programma

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

### **Aggiornamento**

Per poter essere sempre pronto per un attacco di un hacker o per eliminare un virus o altri programmi pericolosi, Kaspersky Anti-Virus for

Windows Workstations deve essere mantenuto aggiornato. Il componente di *aggiornamento* è progettato esattamente per questo. È responsabile dell'aggiornamento dell'elenco dei virus e dei moduli del programma di Kaspersky Anti-Virus for Windows Workstations.

La funzione di distribuzione degli aggiornamenti consente di salvare gli aggiornamenti all'elenco dei virus ed ai moduli dell'applicazione recuperati dai server di aggiornamento di Kaspersky Lab in una cartella locale. Gli altri computer della rete possono quindi accedere ad essi per risparmiare larghezza di banda Internet.

## File di dati

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

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

L'area di *Backup* contiene le copie dei file ripuliti o eliminati dal programma. Queste copie vengono create per l'eventualità in cui si renda necessario ripristinare file o ottenere informazioni sull'infezione. Tali copie di backup sono anch'esse memorizzate in forma criptata per impedire ulteriori infezioni.

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

## Disco di emergenza

Kaspersky Anti-Virus for Windows Workstations può creare un disco di ripristino, che offre un piano di backup in caso di danneggiamento dei file di sistema da parte di un'infezione che renda impossibile avviare il sistema operativo. In tal caso, il disco di emergenza consente di riavviare il computer e ripristinare il sistema nella configurazione in cui si trovava prima dell'infezione.

## Supporto

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

Tramite questi collegamenti, è possibile accedere ad un forum degli utenti di Kaspersky Lab e consultare le domande più frequenti che potrebbero favorire la risoluzione del problema. Inoltre, compilando il modulo sul sito, è possibile inviare all'assistenza tecnica un messaggio relativo all'errore o al problema di funzionamento dell'applicazione.

Ma è possibile anche accedere all'Assistenza tecnica online, e, naturalmente, i nostri dipendenti saranno sempre lieti di aiutarvi telefonicamente per risolvere qualsiasi problema legato all'uso di Kaspersky Anti-Virus.

## 2.3. Requisiti di sistema hardware e software

Per garantire il corretto funzionamento di Kaspersky Anti-Virus for Windows Workstations 6.0, il computer deve possedere i seguenti requisiti minimi:

*Requisiti di carattere generale:*

- 50 MB di spazio disponibile sul disco fisso
- CD-ROM (per installare Kaspersky Anti-Virus for Windows Workstations 6.0 dal CD di installazione)
- Microsoft Internet Explorer 5.5 o successivo (per aggiornare gli elenchi delle minacce e i moduli del programma attraverso Internet)
- Microsoft Windows Installer 2.0

*Microsoft Windows 98, Microsoft Windows Me, Microsoft Windows NT Workstation 4.0 (Service Pack 6a):*

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

*Microsoft Windows 2000 Professional (Service Pack 3 o successiva), Microsoft Windows XP Home Edition, Microsoft Windows XP Professional (Service Pack 1 o successiva), Microsoft Windows XP Professional x64 Edition:*

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

*Microsoft Windows Vista, Microsoft Windows Vista x64:*

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

## 2.4. Pacchetti software

Kaspersky Anti-Virus for Windows Workstations può essere acquistato presso i nostri rivenditori, nella versione in scatola, oppure via Internet, ad esempio su [www.kaspersky.com](http://www.kaspersky.com), nella sezione **eStore**.

La versione in scatola include:

- Una busta sigillata con CD di installazione contenente i file del programma
- Una chiave di licenza, inclusa col pacchetto d'installazione o su uno speciale dischetto, oppure un codice di attivazione dell'applicazione su CD
- Un manuale d'uso
- Il contratto di licenza con l'utente finale (EULA)

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

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

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

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

Leggere attentamente l'EULA.

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

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

## 2.5. Assistenza per gli utenti registrati

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

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

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

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



---

# CAPITOLO 3. INSTALLARE KASPERSKY ANTI-VIRUS FOR WINDOWS WORKSTATIONS 6.0

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

- Installazione locale: installa l'applicazione su un solo host. È necessario l'accesso diretto all'host in questione per eseguire e portare a termine l'installazione. L'installazione locale può essere eseguita in uno dei due seguenti modi:
  - installazione interattiva tramite la Procedura guidata dell'applicazione (vedere 3.1 a pag. 34); questa modalità richiede l'input dell'utente per procedere nell'installazione;
  - un'installazione non interattiva lanciata da riga di comando che non richiede alcun intervento da parte dell'utente per procedere (vedere 3.3 a pag. 48).
- Installazione remota: installa l'applicazione in remoto nei computer in rete da una workstation di amministrazione, utilizzando:
  - la suite software Kaspersky Administration Kit (vedere la Guida di distribuzione di Kaspersky Administration Kit);
  - le regole di dominio di gruppo di Microsoft Windows Server 2000/2003 (vedere 3.4, pag. 49).

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

Nel caso Kaspersky Anti-Virus 5.0 sia già installato, verrà disinstallato ed aggiornato a Kaspersky Anti-Virus 6.0 quando si esegue la procedura di installazione (vedere 3.5 a pag. 51 per ulteriori dettagli). Gli aggiornamenti alle build più recenti (versioni minori) di Kaspersky Anti-Virus 6.0 sono trasparenti.

## 3.1. Installazione tramite la procedura guidata

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

### Nota:

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

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

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

Osserviamo in dettaglio le fasi della procedura di installazione.

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

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


In assenza di uno qualsiasi dei requisiti necessari, il programma visualizza un messaggio informando l'utente del problema. Prima di installare Kaspersky Anti-Virus for Windows Workstations si consiglia di installare i service pack necessari attraverso **Windows Update** ed eventuali altri programmi.

### Passaggio 2. Finestra di avvio dell'installazione

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

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

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

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

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

### Passaggio 4. Scelta di una cartella di installazione

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

- <drive> → Programmi → **Kaspersky Lab** → **Kaspersky Anti-Virus 6.0 for Windows Workstations** – per sistemi a 32 bit.
- <drive> → Programmi (x86) → **Kaspersky Lab** → **Kaspersky Anti-Virus 6.0 for Windows Workstations** – per sistemi a 64 bit.

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

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

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

### Passaggio 5. Utilizzo delle impostazioni di installazione salvate

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

Esaminiamo in dettaglio le opzioni sopra descritte.

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

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

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

Si consiglia inoltre di usare il database di Anti-Spam eventualmente salvato al momento di disinstallare la versione precedente del programma. In tal modo non sarà necessario istruire nuovamente Anti-Spam. Per utilizzare il database già creato in precedenza, selezionare  **Usa database Anti-Spam salvato in precedenza.**

## Passaggio 6. Scelta di un tipo di installazione

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

**Completa.** Selezionando questa opzione, si installano tutti i componenti di Kaspersky Anti-Virus for Windows Workstations. L'installazione riparte con Passaggio 8.

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

**Funzionalità Anti-Virus.** Questa opzione installa solo i componenti che proteggono il computer dai virus. Anti-Hacker, Anti-Spam e Anti-Spy non saranno installati.

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

## Passaggio 7. Scelta dei componenti da installare

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

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

Per selezionare i componenti desiderati, fare clic sull'icona a fianco del nome di un componente e selezionare **Sarà installata sul disco fisso rigido locale** dal menu apertosi. Ulteriori informazioni sul tipo di protezione offerto da un

determinato componente e sulla quantità di spazio su disco necessario per l'installazione sono disponibili nella parte inferiore della finestra del programma di installazione.

Se non si desidera installare un componente, selezionare **L'intera funzionalità non sarà disponibile** dal menu di scelta rapida. Si tenga presente che, scegliendo di non installare un componente, ci si priva di un elemento di protezione da una vasta gamma di programmi pericolosi.


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

## Passaggio 8. Disabilitazione del firewall di Microsoft Windows

Questo passo verrà intrapreso solo se si sta installando il componente Anti-Hacker di Kaspersky Anti-Virus for Windows Workstations su un computer con il firewall incorporato abilitato.

In questo passaggio, Kaspersky Anti-Virus for Windows Workstations chiede se si desidera disabilitare Windows Firewall, poiché il componente Anti-Hacker di Kaspersky Anti-Virus for Windows Workstations garantisce una protezione firewall completa.

Se si desidera utilizzare Anti-Hacker come firewall predefinito, fare clic su **Avanti**. Il firewall di Windows viene disabilitato automaticamente.

Se invece si desidera utilizzare il firewall di Windows, selezionare  **Non disabilitare Windows Firewall**. Se si seleziona questa opzione, Anti-Hacker sarà installato ma disabilitato per evitare conflitti tra programmi.

## Passaggio 9. Ricerca di altri programmi antivirus

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

Il programma di installazione visualizza sullo schermo un elenco di tali programmi, se rilevati. Il programma chiede se si desidera disinstallarli prima di proseguire l'installazione.

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

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

## Passaggio 10. Completamento dell'installazione

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

È sconsigliabile deselezionare l'opzione  **Abilita Auto-difesa prima dell'installazione** alla prima installazione di Kaspersky Anti-Virus 6.0. Se i moduli di protezione sono abilitati, l'installazione potrà essere annullata correttamente in caso di errori durante l'installazione dell'applicazione. Se si sta cercando di installare nuovamente l'applicazione, si consiglia invece di deselezionare questa casella di controllo.

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

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

### Attenzione!

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

## Passaggio 11. Completamento della procedura di installazione

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

Per avviare la procedura guidata, fare clic sul pulsante **Avanti** (vedere 3.2, pag. 38).

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

## 3.2. Impostazione guidata

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

Questa interfaccia è concepita come una procedura guidata standard di Windows ed è costituita da una serie di passaggi tra i quali è possibile navigare

utilizzando i pulsanti **Indietro** e **Avanti**; per completare la procedura, fare clic sul pulsante **Fine**. Per uscire dalla procedura in qualsiasi momento, fare clic su **Annulla**.

È possibile omettere questa fase iniziale di impostazione durante l'installazione del programma chiudendo la finestra della procedura guidata. Sarà possibile eseguirla di nuovo in seguito dall'interfaccia del programma se si ripristinano le impostazioni predefinite di Kaspersky Anti-Virus for Windows Workstations (vedere 17.13 a pag. 283).

### 3.2.1. Uso di oggetti salvati con la versione 5.0

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

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

### 3.2.2. Attivazione del programma

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

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

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

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

#### 3.2.2.1. Scelta di un metodo di attivazione del programma

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

- ④ **Attiva mediante codice di attivazione.** Selezionare questa opzione di attivazione se è stata acquistata la versione completa del programma con codice di attivazione in dotazione. Questo codice di attivazione consente di ottenere un file chiave che garantisce l'accesso alla funzionalità completa del programma fino alla scadenza della licenza.
- ④ **Attiva versione di valutazione (30 giorni).** Selezionare questa opzione di attivazione se si desidera installare la versione di prova del programma prima di decidere se acquistare la versione commerciale. Si riceverà una chiave gratuita valida per il periodo descritto nell'accordo di licenza per la versione di prova.
- ④ **Applica chiave di licenza.** Il programma viene attivato utilizzando un file chiave di licenza per Kaspersky Anti-Virus 6.0.
- ④ **Attiva successivamente.** Selezionando questa opzione si omette la fase di attivazione. Kaspersky Anti-Virus for Windows Servers 6.0 viene installato sul computer e si potrà accedere a tutte le funzioni del programma ad eccezione degli aggiornamenti (è possibile aggiornare gli elenchi delle minacce solo dopo l'installazione del programma).

Le prime due opzioni di attivazione utilizzano un server web di Kaspersky Lab, che richiede una connessione a Internet. Prima di attivare, modificare le impostazioni di rete (vedere 16.4.3 a pag. 231) nella finestra che si apre facendo clic su **Impostazioni LAN** (se è il caso). Per informazioni più approfondite sulla configurazione delle impostazioni di rete, consultare l'amministratore di sistema o l'ISP.

Se non si dispone di connessione a Internet quando si installa il programma, si può attivare l'applicazione successivamente (vedere 17.5 a pag. 261) tramite la sua interfaccia, oppure si può utilizzare l'accesso a Internet di un altro computer per registrarsi presso il sito web Assistenza tecnica di Kaspersky Lab e ottenere la chiave di licenza utilizzando il codice di attivazione.

### 3.2.2.2. Inserimento del codice di attivazione

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

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

Immettere i dati di contatto nella parte inferiore della finestra: Nome completo, indirizzo e-mail, Paese e città di residenza. Queste informazioni possono essere richieste per identificare un utente registrato se, per esempio, la chiave viene



persa o rubata. In tal caso, le informazioni di contatto immesse consentiranno di ottenere una nuova chiave di licenza.

### 3.2.2.3. Come procurarsi un file chiave di licenza

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

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

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

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

### 3.2.2.4. Selezione di un file chiave di licenza

Se si dispone di un file contenente la chiave di licenza di Kaspersky Anti-Virus for Windows Workstations 6.0, la finestra della procedura guidata chiederà di installarlo. Se sì, servirsi del pulsante **Sfoglia** per selezionare il percorso del file della chiave di licenza, riconoscibile dall'estensione *.key*, nella finestra di selezione.

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

### 3.2.2.5. Completamento dell'attivazione del programma

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

### 3.2.3. Selezione di una modalità di sicurezza

In questa finestra, la procedura guidata chiede di selezionare la modalità di sicurezza da applicare al programma:

**Protezione di base.** È l'impostazione predefinita, studiata per utenti dotati di scarsa esperienza con il computer o con l'uso di software antivirus. Imposta tutti i componenti del programma ai relativi livelli di sicurezza raccomandati e informa l'utente solo in caso di eventi pericolosi, come il rilevamento di un codice nocivo o l'esecuzione di azioni pericolose.

**Protezione interattiva.** Questa modalità offre una protezione dei dati del computer più personalizzata rispetto alla modalità Base. Essa è in grado di intercettare tentativi di modifica delle impostazioni di sistema, attività sospette a livello di sistema e attività non autorizzate a livello di rete.

Ciascuna di queste attività potrebbe essere indice di programmi nocivi, oppure essere un'attività standard di qualche programma utilizzato sul computer. Spetta all'utente stabilire per ogni singolo caso se consentire o bloccare tali attività.

Se si sceglie questa modalità, specificare il contesto in cui applicarla:

**Abilita modalità Apprendimento Anti-Hacker** – richiede l'intervento dell'utente quando i programmi installati sul computer tentano di connettersi a determinate risorse di rete. L'utente può autorizzare o bloccare quella connessione, nonché configurare una regola di Anti-Hacker per quel programma. Se si disabilita la modalità di training, Anti-Hacker funziona con un livello di protezione minimo, vale a dire che consente a tutte le applicazioni di accedere alle risorse di rete.

**Abilita Registry Guard** – richiede l'intervento dell'utente quando vengono rilevati tentativi di modifica delle chiavi del registro di sistema.

Se l'applicazione è installata su un computer che esegue Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista o Microsoft Windows Vista x64, le impostazioni elencate di seguito per l'interattività non saranno disponibili.

**Abilita Difesa proattiva estesa** – analizza tutte le attività sospette delle applicazioni nel sistema, inclusa l'apertura del browser mediante impostazioni da riga di comando, l'inserimento nei processi applicativi, e gli intercettatori degli hook delle finestre (questa opzione è disabilitata per impostazione predefinita).

### 3.2.4. Configurazione delle impostazioni di aggiornamento

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

- ④ **Automaticamente.** Kaspersky Anti-Virus verifica ad intervalli specificati la disponibilità di nuovi aggiornamenti presso la relativa sorgente. Durante le epidemie, la frequenza di verifica può aumentare, diminuendo al loro scemare. Se trova nuovi aggiornamenti, il programma li scarica e li installa sul computer. È la modalità predefinita.
- ④ **Come pianificato.** Gli aggiornamenti vengono eseguiti automaticamente in base a quanto pianificato. Per configurare la programmazione fare clic su **Cambia**.
- ④ **Manualmente.** Questa opzione consente di eseguire manualmente gli aggiornamenti.

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

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

### 3.2.5. Pianificazione delle scansioni antivirus

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

Al momento dell'installazione di Kaspersky Anti-Virus for Windows Workstations, vengono create tre attività di scansione antivirus predefinite. In questa finestra, viene richiesto di scegliere un'impostazione iniziale per l'attività di scansione:

### Scansione oggetti ad esecuzione automatica

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

### Scansione aree critiche

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

Per impostazione predefinita, questa scansione automatica è disabilitata.

### Scansione completa del computer

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

L'impostazione predefinita per l'esecuzione pianificata di questa scansione automatica è disabilitata. Tuttavia, si raccomanda di eseguire una scansione antivirus completa del computer subito dopo l'installazione del programma.

## 3.2.6. Restrizioni di accesso al programma

Kaspersky Anti-Virus dà la possibilità di proteggere il programma con una password, poiché diverse persone potrebbero utilizzare lo stesso computer e diversi programmi pericolosi potrebbero disabilitare la protezione. L'uso di una password è utile per proteggere il programma da tentativi non autorizzati di disabilitare la protezione o modificare le impostazioni.

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

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

- Tutte le operazioni (ad eccezione delle notifiche di eventi pericolosi).**  
Richiede la password se l'utente tenta di effettuare qualsiasi azione con il programma tranne rispondere agli avvisi nel momento in cui vengono rilevati oggetti pericolosi.

### Operazioni selezionate:

- Salvataggio impostazioni programma** – richiede la password quando un utente cerca di salvare le modifiche alle impostazioni del programma.
- Uscita dal programma in esecuzione** – richiede la password se un utente cerca di uscire dal programma.
- Arresto / sospensione componenti di protezione o attività di ricerca virus** – richiede la password se l'utente cerca di sospendere o di disabilitare completamente qualsiasi componente di protezione o attività di scansione anti-virus.

## 3.2.7. Configurazione delle impostazioni di Anti-Hacker

Anti-Hacker è il componente di Kaspersky Anti-Virus for Windows Workstations che protegge il computer sulle reti locali e su Internet. In questa fase, la procedura di configurazione guidata chiede di creare un elenco di regole per guidare Anti-Hacker durante l'analisi dell'attività di rete del computer.

### 3.2.7.1. Determinare lo stato di una zona di sicurezza

In questa fase, la procedura guidata analizza l'ambiente di rete del computer. In base a questa analisi, l'intero spazio di rete viene suddiviso in zone:

*Internet* – la rete a livello mondiale. In questa zona, Kaspersky Anti-Virus for Windows Workstations opera come personal firewall. Così facendo, le regole predefinite di filtraggio pacchetti e delle applicazioni regolano l'intera attività di rete per garantire la massima sicurezza. Durante una sessione di lavoro in questa zona non è possibile modificare le impostazioni di protezione ma solo abilitare la modalità invisibile per una maggiore sicurezza del computer.

*Aree di protezione* – alcune zone che più corrispondono alle sottoreti in cui è incluso il computer (potrebbero essere sottoreti locali domestiche o al lavoro). Per impostazione predefinita, queste zone sono definite a medio rischio. È possibile modificare lo stato di queste zone in base a quanto si ritiene affidabile una determinata sottorete, e configurare regole per il filtraggio pacchetti e le applicazioni.

Tutte le zone individuate vengono visualizzate in un elenco. Ciascuna di esse è accompagnata da una descrizione, dall'indirizzo e dalla subnet mask, e dallo

grado col quale qualsiasi attività di rete sarà autorizzata o bloccata da Anti-Hacker.

- **Internet.** Questo è lo stato predefinito assegnato a Internet, poiché, su Internet, il computer è soggetto potenzialmente a tutti i tipi di minacce. Questo stato è raccomandato anche per reti che non sono protette da nessun programma antivirus, firewall, filtro, ecc. Selezionando questo stato, il programma garantisce la massima sicurezza all'interno di questa zona, in particolare:
  - blocco di qualsiasi attività di rete NetBios all'interno della sottorete
  - blocco delle regole delle applicazioni e di filtraggio dei pacchetti che consentono un'attività NetBios all'interno della sottorete

Anche se è stata creata una cartella condivisa, le informazioni nella stessa non saranno disponibili ad utenti appartenenti a sottoreti con questo stato. Inoltre, se questo stato è selezionato per una certa sottorete, non sarà possibile accedere ai file ed alle stampanti di questa sottorete.

- **Rete locale.** Il programma assegna questo stato alla maggior parte delle aree di protezione rilevate durante l'analisi dell'ambiente di rete del computer, con l'eccezione delle zone Internet. Si raccomanda di applicare questo status alle zone caratterizzate da un fattore di rischio medio (per esempio LAN aziendali). Selezionando questo stato, il programma consente:
  - qualsiasi attività di rete NetBios all'interno della sottorete
  - regole per applicazioni e filtraggio pacchetti che consentono un'attività NetBios all'interno della sottorete

Selezionare questo stato se si desidera garantire l'accesso a determinate cartelle o stampanti del computer, bloccando al tempo stesso qualsiasi altra attività esterna.

- **Attendibile.** Questo stato è assegnato solo alle zone ritenute assolutamente sicure, in cui il computer non è esposto ad attacchi o tentativi di accesso ai dati in esso custoditi. In questo caso, ogni attività di rete è consentita. Anche se in precedenza si è selezionato il massimo livello di protezione creando regole di blocco, questi sistemi di sicurezza non vengono applicati per i computer remoti provenienti da una rete affidabile.

È possibile utilizzare la *Modalità Mascheramento* per maggiore sicurezza quando si usano reti classificate come **Internet**. Questa funzione consente solo le attività di rete avviate dal computer in uso, il che significa in realtà che il computer si

rende invisibile all'ambiente circostante. Questa modalità non pregiudica le prestazioni del computer su Internet.

Si sconsiglia l'uso della Modalità Mascheramento se il computer viene utilizzato come server (per esempio, un server di posta o un server HTTP), in quanto in questa modalità i computer che si connettono al server non lo vedranno come collegato.

Per modificare lo stato di una zona o per abilitare/disabilitare la Modalità Mascheramento, selezionare la zona dalla lista e utilizzare i collegamenti appropriati nel riquadro **Descrizione regola** sotto la lista. È possibile eseguire attività simili e modificare indirizzi e subnet mask nella finestra **Impostazioni rete** che si apre facendo clic su **Modifica**.

È possibile aggiungere una nuova zona all'elenco durante la visualizzazione. A tal fine, fare clic su **Aggiorna**. Anti-Hacker cerca le zone disponibili e, se ne rileva, chiede di selezionare uno stato da assegnare loro. È possibile inoltre aggiungere manualmente nuove zone all'elenco (per esempio se si connette il laptop a una nuova rete). A tal fine, fare clic su **Aggiungi** e compilare i dati necessari nella finestra **Impostazioni rete**.

Per eliminare la rete dalla lista, fare clic sul pulsante **Elimina**.

### 3.2.7.2. Creazione di un elenco di applicazioni di rete

La procedura di configurazione guidata analizza il software installato sul computer e crea un elenco di applicazioni che usano una connessione di rete.

Anti-Hacker crea una regola volta a controllare l'attività di rete per ciascuna di queste applicazioni. Le regole vengono applicate in base a modelli per le applicazioni di rete più comuni, creati da Kaspersky Lab e in dotazione con il software.

È possibile visualizzare un elenco delle applicazioni di rete e delle relative regole nella finestra delle impostazioni di Anti-Hacker, che si apre facendo clic su **Applicazioni**.

Per una maggiore sicurezza, si consiglia di disabilitare la funzione di cache DNS durante l'uso di risorse Internet. Questa funzione riduce drasticamente il tempo di connessione del computer a questa valida risorsa Internet; al tempo stesso rappresenta però una pericolosa vulnerabilità, sfruttando la quale gli hacker possono creare perdite di dati non individuabili per mezzo del firewall. Per aumentare il grado di sicurezza del computer, si consiglia quindi di disabilitare la cache DNS.

### 3.2.8. Completamento della procedura di configurazione guidata

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

Alcuni componenti del programma potrebbero non funzionare finché il computer non viene riavviato.

## 3.3. Installazione del programma da riga di comando

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

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

Parte l'installazione guidata (vedere 3.1 a pag. 34). Una volta installato il programma, è necessario riavviare il computer.

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

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

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

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

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

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

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

```
KLUNINSTPASSWD=*****, durante l'esecuzione di un'installazione interattiva;
```

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



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

Se si installa Kaspersky Anti-Virus in modalità non interattiva, è possibile accedere al file *setup.ini*, che contiene le impostazioni generali per l'installazione dell'applicazione (vedere A.4 a pag. 331), al file di configurazione *install.cfg* (vedere 18.8 a pag. 298), nonché al file chiave di licenza. Si noti che questi file devono essere ubicati nella stessa cartella nella quale si trova il pacchetto di installazione di Kaspersky Anti-Virus.

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

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

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

### 3.4.1. Installazione del programma

Per installare Kaspersky Anti-Virus:

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

È inoltre possibile copiare nella stessa posizione il file *setup.ini*, che contiene le impostazioni generali per l'installazione dell'applicazione (vedere A.4 a pag. 331), il file di configurazione *install.cfg* (vedere 18.7 a pag. 297), nonché il file chiave di licenza.

2. Aprire l'**Editor oggetti Criteri di gruppo** tramite la MMC (per maggiori informazioni sull'utilizzo dell'oggetto Criteri di gruppo, consultare la guida di Microsoft Windows Server).
3. Creare un nuovo pacchetto. Per fare ciò, selezionare dall'albero della console **Oggetto criteri di gruppo/ Configurazione computer/ Impostazioni del software/ Installazione software** ed utilizzare il comando **Nuovo/ Pacchetto** dal menù contestuale.

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

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

### 3.4.2. Upgrade del programma

*Per effettuare l'upgrade di Kaspersky Anti-Virus:*

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

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

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

### 3.4.3. Disinstallazione del programma

*Per disinstallare Kaspersky Anti-Virus*

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

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

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

## 3.5. Upgrade dalla versione 5.0 alla versione 6.0

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

Una volta avviato il programma d'installazione per Kaspersky Anti-Virus 6.0, sarà possibile scegliere se prima disinstallare la versione 5.0. Una volta completato il processo di disinstallazione, è necessario riavviare il computer, dopodiché verrà eseguita l'installazione della versione 6.0.

### Attenzione!

Quando si fa l'upgrade da Kaspersky Anti-Virus 5.0 a 6.0 da una cartella di rete protetta da password, la versione 5.0 verrà disinstallata ed il computer verrà riavviato senza poi installare la versione 6.0 dell'applicazione. Ciò succede perché il programma d'installazione non dispone di diritti d'accesso alla cartella di rete. Per risolvere il problema, eseguire il programma d'installazione esclusivamente da una cartella locale.

---

# CAPITOLO 4. INTERFACCIA DEL PROGRAMMA

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

- Icona dell'area di notifica (vedere 4.1 a pag. 52)
- Il menù contestuale (vedere 4.2 a pag. 53)
- Finestra principale (vedere 4.3 a pag. 55)
- Finestra delle impostazioni del programma (vedere 4.4 a pag. 57)

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



- Microsoft Office Outlook – scansioni antivirus (vedere 8.2.2 a pag. 112) e scansioni antispam (vedere 13.3.8 a pag. 195)
- Microsoft Outlook Express (Windows Mail) (vedere 13.3.9 a pag. 198)
- The Bat! – scansioni antivirus (vedere 8.2.3 a pag. 114) e scansioni antispam (vedere 13.3.10 a pag. 199)
- Microsoft Internet Explorer (vedere Capitolo 11 a pag. 142)
- Microsoft Windows Explorer (vedere 14.2 a pag. 204)

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






## 4.1. L'icona dell'area di notifica

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

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

Se l'icona è attiva  (colorata), il computer è protetto. Se l'icona non è attiva  (bianco e nero), tutti i componenti di protezione (vedere 2.2.1 a pag. 26) sono disattivati.

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

|   |  |
|---|--|
|  | Si stanno esaminando i messaggi di posta elettronica.  |
|  | Si stanno esaminando gli script.   |
|  | Scansione in corso di un file in fase di apertura, salvataggio o esecuzione da parte dell'utente o di un programma.                |
|  | Gli elenchi delle minacce di Kaspersky Anti-Virus for Windows Workstations e i moduli del programma sono in fase di aggiornamento. |
|  | Si è verificato un errore in qualche componente di Kaspersky Anti-Virus.   |

L'icona consente inoltre di accedere alle funzioni di base dell'interfaccia del programma: il menu di scelta rapida (vedere 4.2 a pag. 53) e la finestra principale (vedere 4.3 a pag. 55).

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

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

## 4.2. Il menu di scelta rapida

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

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

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

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

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

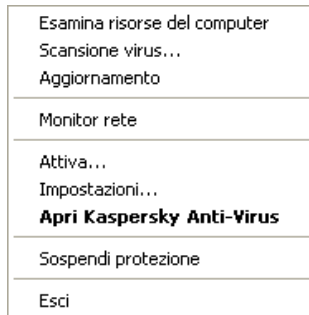


Figura 1. Il menu di scelta rapida

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

**Monitor rete** – visualizza l'elenco delle connessioni di rete stabilite, le porte aperte e il traffico.

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

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

**Apri Kaspersky Anti-Virus** – apre la finestra principale del programma (vedere 4.3 a pag. 55).

**Sospendi protezione / Riprendi protezione** – disabilita o abilita temporaneamente i componenti di protezione (vedere 2.2.1 a pag. 26). Questa voce di menu non influisce sugli aggiornamenti del programma o sulle attività di scansione antivirus.

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

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

## 4.3. La finestra principale del programma

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

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

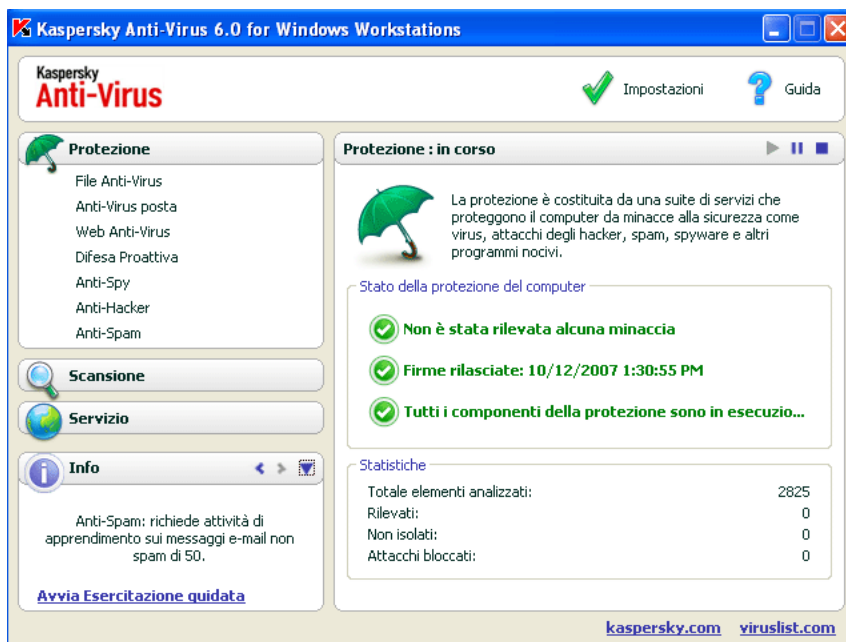

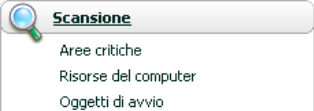



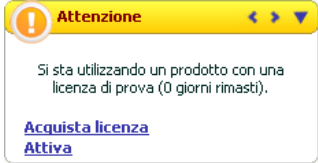
Figura 2. Finestra principale di Kaspersky Anti-Virus for Windows Workstations

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

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

| Sezione della finestra principale  | Scopo   |
|--|---|
| <p>Questa finestra fornisce principalmente informazioni sullo stato di protezione del computer. La sezione <b>Protezione</b> ha proprio questa funzione.</p>  | <p>Per visualizzare informazioni generali sul funzionamento di Kaspersky Anti-Virus, esaminare le statistiche generali di funzionamento del programma e verificare che tutti i componenti operino correttamente, selezionare la sezione <b>Protezione</b> nell'area di navigazione.</p> <p>Da qui è possibile inoltre abilitare/disabilitare i componenti di protezione. Per visualizzare le statistiche e le impostazioni relative a un particolare componente di protezione, selezionare il nome del componente sul quale si desidera avere informazioni nella sezione <b>Protezione</b>.</p> |
| <p>Per esaminare il computer e rilevare eventuali file o programmi nocivi, utilizzare la speciale sezione <b>Scansione</b> nella finestra principale.</p>   | <p>Questa sezione contiene un elenco di oggetti che è possibile sottoporre alla scansione anti-virus.</p> <p>Le attività più importanti e più comuni sono incluse in questa sezione. Tra queste vi sono le attività di scansione antivirus delle aree critiche, dei programmi di avvio e le scansioni complete del computer.</p>  |
| <p>La sezione <b>Servizio</b> include funzioni supplementari di Kaspersky Anti-Virus for Windows Workstations.</p>    | <p>In questa sezione è possibile aggiornare il programma, visualizzare rapporti sulle prestazioni di qualsiasi componente o attività di Kaspersky Anti-Virus for Windows Workstations, lavorare con gli oggetti in quarantena e le copie di backup, consultare le informazioni relative all'assistenza tecnica, creare un disco di ripristino e gestire le chiavi di licenza.</p>   |



| Sezione della finestra principale   | Scopo   |
|---|---|
| <p>La sezione <b>Commenti e suggerimenti</b> accompagna l'utente durante l'uso del programma.</p>  | <p>Questa sezione offre suggerimenti su come incrementare il livello di sicurezza del computer. Vi si trovano inoltre commenti sulle prestazioni correnti dell'applicazione e sulle sue impostazioni. I link di questa sezione consentono di eseguire le azioni raccomandate per una sezione particolare o visualizzare informazioni più dettagliate.</p> |

Ogni elemento del pannello di navigazione è accompagnato da uno speciale menu di scelta rapida. Esso contiene punti per i componenti di protezione e strumenti che agevolano l'utente nella configurazione e gestione dei componenti e nella visualizzazione dei rapporti. È inoltre disponibile un'ulteriore voce di menù per le scansioni antivirus e le attività di aggiornamento che consente di creare un'attività personalizzata modificando la copia di un'attività esistente.

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

## 4.4. Finestra delle impostazioni del programma

La finestra delle impostazioni di Kaspersky Anti-Virus for Windows Workstations (vedere 4.3 a pag. 55) può essere aperta dalla finestra principale. A tal fine, fare clic su Impostazioni nella parte superiore della stessa.

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

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

Quando si seleziona qualsiasi sezione, componente o attività nella parte sinistra della finestra delle impostazioni, la parte destra ne visualizza le impostazioni di

base. Per configurare le impostazioni avanzate, è possibile aprire le finestre delle impostazioni di secondo e terzo livello. Per una descrizione dettagliata delle impostazioni del programma, vedere le sezioni corrispondenti della Guida.

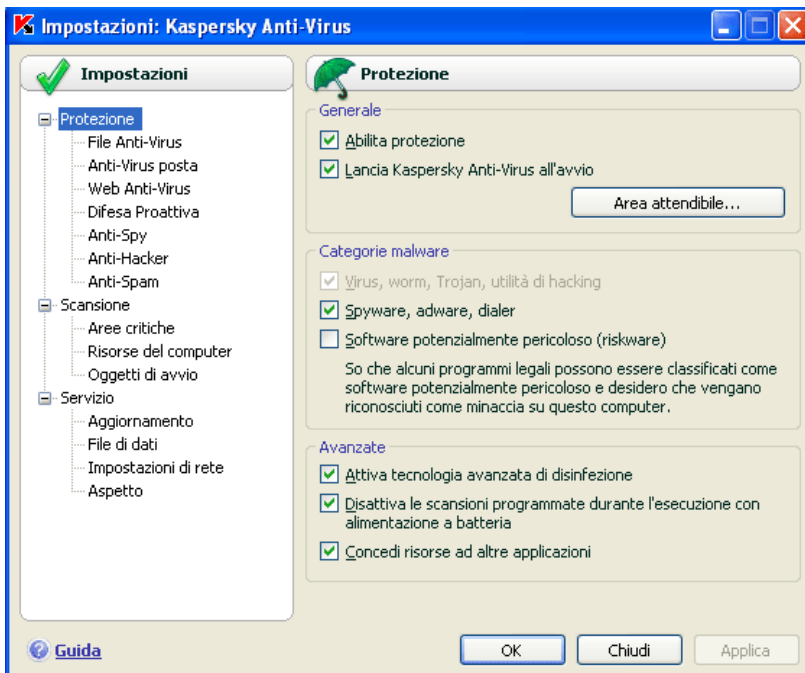


Figura 3. Finestra delle impostazioni di Kaspersky Anti-Virus for Windows Workstations

---

# CAPITOLO 5. GUIDA INTRODUTTIVA

Uno dei principali obiettivi di Kaspersky Lab nell'elaborazione di Kaspersky Anti-Virus for Windows Workstations era quello di fornire la configurazione ottimale per ciascuna opzione del programma. Ciò consente agli utenti a qualsiasi livello di conoscenza del computer di proteggere rapidamente il computer subito dopo l'installazione.

È possibile tuttavia che il computer o il tipo di lavoro per il quale lo si utilizza richiedano delle configurazioni specifiche. Per questa ragione, si raccomanda di eseguire una configurazione preliminare per ottenere una protezione più flessibile e personalizzata per il computer.

Per facilitare al massimo la messa in funzione del programma, abbiamo combinato tutte le fasi di configurazione preliminare in una procedura di configurazione guidata (vedere 3.2 a pag. 38) che si avvia al termine dell'installazione del programma. Seguendo le istruzioni della procedura guidata è possibile attivare il programma, configurare le impostazioni degli aggiornamenti e delle scansioni antivirus, proteggere l'accesso al programma tramite password e configurare Anti-Hacker in modo da soddisfare i requisiti della rete.

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

- Controllare lo stato corrente della protezione (vedere 5.1 a pag. 60) per garantire che Kaspersky Anti-Virus for Windows Workstations funzioni al livello appropriato.
- Addestramento di Anti-Spam (vedere 5.5 a pag. 68) utilizzando i propri messaggi.
- Aggiornare il programma (vedere 5.6 a pag. 69) se la procedura guidata non ha provveduto automaticamente dopo l'installazione del programma.
- Eseguire la scansione antivirus del computer (vedere 5.2 a pag. 65).

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

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

**Stato della protezione del computer** visualizza lo stato corrente di protezione del computer per mezzo di speciali indicatori (vedere 5.1.1 a pag. 60). Le Statistiche (vedere 5.1.2 a pag. 63) analizzano la sessione corrente del programma.

### 5.1.1. Indicatori della protezione

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

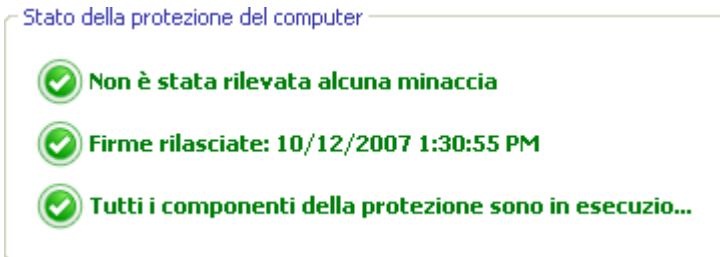


Figura 4. Gli indicatori che riflettono lo stato della protezione del computer

Ciascun indicatore ha tre possibili aspetti:



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



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



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


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

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


|  |   |
|--|---|
|  | <p><i>Non è stata rilevata alcuna minaccia</i></p> <p>Kaspersky Anti-Virus for Windows Workstations non ha rilevato alcun file o programma pericoloso sul computer.</p>   |
|  | <p><i>Tutte le minacce sono state isolate</i></p> <p>Kaspersky Anti-Virus for Windows Workstations ha trattato tutti i file e i programmi infetti da virus ed ha eliminato quelli che non era possibile trattare.</p>   |
|  | <p><i>Le minacce sono state rilevate</i></p> <p>Il computer è a rischio di infezione. Kaspersky Anti-Virus for Windows Workstations ha rilevato programmi nocivi (virus, trojan, worm, ecc.) che devono essere neutralizzati. A tal fine, usare il collegamento <u>Isola tutto</u>. Fare clic su <u>Dettagli</u> per ulteriori dettagli sugli oggetti nocivi.</p> |



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

|  |  |
|--|--|
|  | <p><i>Firme rilasciate: (data, ora)</i></p> <p>Sia l'applicazione che l'elenco delle minacce utilizzati da Kaspersky Anti-Virus for Windows Workstations sono le versioni più recenti.</p>   |
|  | <p><i>Le firme non sono aggiornate</i></p> <p>I moduli del programma e il database di Kaspersky Anti-Virus for Windows Workstations non sono stati aggiornati da diversi giorni. L'utente corre il rischio di infettare il computer con nuovi programmi nocivi apparsi dopo l'ultimo aggiornamento del programma. Si consiglia di aggiornare Kaspersky Anti-Virus for Windows Workstations. A tal fine, usare il collegamento <u>Aggiorna</u>.</p> |

|   |  |
|---|--|
|   | <p><i>Gli elenchi dei virus sono parzialmente corrotti</i></p> <p>Gli elenchi delle minacce sono parzialmente corrotti. In tal caso, è consigliabile eseguire nuovamente l'aggiornamento del programma. Se si ripresenta lo stesso messaggio d'errore, rivolgersi al servizio di assistenza tecnica Kaspersky Lab.</p> |
|   | <p><i>Riavviare il computer</i></p> <p>Per garantire il corretto funzionamento del programma è necessario riavviare il sistema. Salvare e chiudere tutti i file su cui si sta lavorando e fare clic sul collegamento <u>Riavviare il computer</u>.</p>   |
|   | <p><i>Gli aggiornamenti al programma sono disabilitati</i></p> <p>Il servizio di aggiornamento all'elenco delle minacce ed ai moduli del programma è disabilitato. Per mantenere la protezione in tempo reale, si consiglia di abilitare gli aggiornamenti.</p>  |
|  | <p><i>L'elenco dei virus è obsoleto</i></p> <p>Kaspersky Anti-Virus for Windows Workstations non è stato aggiornato per diverso tempo. I dati sul computer sono in grande pericolo. Aggiornare il programma al più presto. A tal fine, usare il collegamento <u>Aggiorna ora</u>.</p>                                  |
|   | <p><i>Gli elenchi dei virus sono corrotti</i></p> <p>Gli elenchi delle minacce sono completamente corrotti. In tal caso, è consigliabile eseguire nuovamente l'aggiornamento del programma. Se si ripresenta lo stesso messaggio d'errore, rivolgersi al servizio di assistenza tecnica Kaspersky Lab.</p>             |

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

|   |   |
|---|---|
|  | <p><i>Tutti i componenti della protezione sono in esecuzione</i></p> <p>Kaspersky Anti-Virus for Windows Workstations sta proteggendo il computer su tutti i canali attraverso i quali potrebbero infiltrarsi i programmi nocivi. Tutti i componenti della protezione sono abilitati.</p> |
|---|---|

|   |  |
|---|--|
|   | <p><i>Protezione non installata</i></p> <p>Al momento dell'installazione di Kaspersky Anti-Virus for Windows Workstations non è stato installato nessuno dei componenti di monitoraggio. Questo significa che è possibile solo eseguire la scansione antivirus. Per la massima sicurezza è necessario installare i componenti di protezione sul computer.</p>              |
|  | <p><i>Tutti i componenti della protezione sono sospesi</i></p> <p>Tutti i componenti di protezione sono stati sospesi. Per ripristinare i componenti, selezionare <b>Riprendi protezione</b> dal menu di scelta rapida facendo clic sull'icona dell'area di notifica.</p>  |
|   | <p><i>Alcuni componenti della protezione sono disabilitati</i></p> <p>Uno o più componenti di protezione sono stati interrotti. Ciò potrebbe portare all'infezione del computer ed alla perdita di dati. Si consiglia fortemente di abilitare la protezione. A tal fine, selezionare un componente inattivo dall'elenco e fare clic su ►.</p>                              |
|   | <p><i>Tutti i componenti della protezione sono disabilitati</i></p> <p>La protezione è completamente disabilitata. Nessun componente è in funzione. Per ripristinare i componenti, selezionare <b>Ripristina protezione</b> dal menu di scelta rapida facendo clic sull'icona dell'area di notifica.</p>   |
|  | <p><i>Si è verificato un errore in alcuni componenti di protezione</i></p> <p>Si è verificato un errore interno in uno o più componenti di Kaspersky Anti-Virus for Windows Workstations. Si raccomanda in questo caso di abilitare il componente o di riavviare il computer (è possibile che i driver del componente debbano essere registrati dopo l'aggiornamento).</p> |

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

Per determinare in che modo Kaspersky Anti-Virus for Windows Workstations stia proteggendo file system, e-mail, traffico HTTP o altre aree dove i programmi pericolosi potrebbero penetrare nel computer, o per visualizzare l'avanzamento delle attività di scansione antivirus o dell'aggiornamento dell'elenco dei virus, è

sufficiente aprire la sezione corrispondente della finestra principale del programma.

Per esempio, per visualizzare lo stato corrente di File Anti-Virus, selezionare **File Anti-Virus** dalla parte sinistra del pannello principale, oppure, per vedere se il computer è protetto dai nuovi virus, selezionare **Difesa Proattiva**. Il riquadro destro visualizzerà un riassunto delle informazioni relative al funzionamento del componente.

Per i componenti di protezione, il pannello destro contiene la **barra di stato**, il riquadro di **Stato** ed il riquadro delle **Statistiche**.

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



- *File Anti-Virus: in corso* – la protezione dei file è attiva al livello selezionato (vedere 7.1 a pag. 94).
- *File Anti-Virus: in sospeso* – File Anti-Virus è disabilitato per un determinato intervallo di tempo. Il componente riprenderà a funzionare automaticamente alla scadenza del periodo stabilito o dopo aver riavviato il programma. La protezione dei file può anche essere ripristinata manualmente facendo clic sul pulsante ► ubicato sulla barra di stato.
- *File Anti-Virus: Disattivato* – il componente è stato arrestato dall'utente. La protezione dei file può essere ripristinata manualmente facendo clic sul pulsante ► ubicato sulla barra di stato.
- *File Anti-Virus: non in funzione* – la protezione dei file non è disponibile per qualche ragione.
- *File Anti-Virus: disabilitato (errore)* – il componente ha provocato un errore.

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

Se il componente contiene più moduli, la sezione **Stato** conterrà informazioni sullo stato di ciascuno di essi. Per i componenti non composti da moduli singoli, vengono visualizzati lo stato, il livello di sicurezza e, per alcuni, la risposta ai programmi pericolosi.

La casella **Stato** non è disponibile per le attività di scansione antivirus e di aggiornamento. Il livello di sicurezza, l'azione applicata ai programmi pericolosi

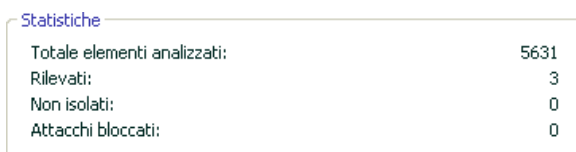


per le attività di scansione antivirus, e la modalità di esecuzione per gli aggiornamenti sono elencati nel riquadro **Impostazioni**.

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

### 5.1.3. Statistiche sulle prestazioni del programma

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



The image shows a screenshot of a software window titled "Statistiche". Inside the window, there is a table with four rows of statistics. The first row shows "Totale elementi analizzati:" with the value "5631". The second row shows "Rilevati:" with the value "3". The third row shows "Non isolati:" with the value "0". The fourth row shows "Attacchi bloccati:" with the value "0".

| Statistiche                 |      |
|-----------------------------|------|
| Totale elementi analizzati: | 5631 |
| Rilevati:                   | 3    |
| Non isolati:                | 0    |
| Attacchi bloccati:          | 0    |

Figura 5. Il riquadro statistiche generali del programma

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

- Informazioni sugli oggetti analizzati (vedere 17.3.2 a pag. 247) e sullo stato assegnato a ciascuno
- Registro degli eventi (vedere 17.3.3 a pag. 248)
- Statistiche generali sulla scansione (vedere 17.3.4 a pag. 249) per il computer in uso
- Statistiche sulle prestazioni del programma (vedere 17.3.5 a pag. 250)

## 5.2. Come eseguire la scansione antivirus del computer

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

Kaspersky Anti-Virus for Windows Workstations include un'attività per una scansione antivirus del computer, ubicata nella sezione **Scansione** della finestra principale del programma.

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

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

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

Fare clic sul pulsante **Scansione**. Il programma avvia la scansione del computer visualizzando i dettagli in una finestra apposita. Facendo clic sul pulsante **Chiudi**, la finestra di avanzamento verrà nascosta, ma la scansione continua.

## 5.3. Come eseguire la scansione di aree critiche del computer

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

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

Una volta selezionata l'attività denominata **Aree critiche**, il pannello a destra della finestra principale visualizzerà quanto segue: le statistiche relative alla scansione più recente di queste aree; il livello di sicurezza selezionato, e quali azioni vengono applicate alle minacce alla sicurezza. Qui è anche possibile selezionare quali aree critiche si desidera esaminare, ed esaminarle immediatamente.

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

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

Fare clic sul pulsante **Scansione**. Il programma avvia la scansione delle aree selezionate visualizzando i dettagli in una finestra apposita. Facendo clic sul pulsante **Chiudi**, la finestra di avanzamento verrà nascosta, ma la scansione continua.

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

In determinate situazioni, occorre sottoporre alla scansione anti-virus singoli oggetti ma non l'intero computer. Per esempio, uno dei dischi fissi sui quali si trovano programmi e giochi, database di posta copiati dal lavoro con tanto di file allegati, ecc. È possibile selezionare un oggetto da esaminare con gli strumenti standard del sistema operativo Microsoft Windows (per esempio dalla finestra **Esplora risorse** o dal **Desktop**, ecc.).

*Per esaminare un oggetto,*

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

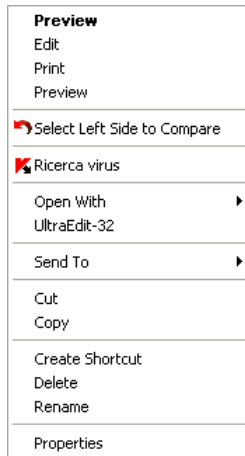


Figura 6. Scansione di un oggetto selezionato utilizzando il menù contestuale standard di Windows

Il programma avvia quindi la scansione dell'oggetto selezionato visualizzando i dettagli in una finestra apposita. Facendo clic sul pulsante **Chiudi**, la finestra di avanzamento verrà nascosta, ma la scansione continua.

## 5.5. Come istruire Anti-Spam

Per iniziare, il primo passo è addestrare Anti-Spam a lavorare con la posta elettronica eliminando la posta indesiderata. Per spam si intende la posta indesiderata, anche se è molto difficile stabilire cosa sia effettivamente lo spam per ogni singolo utente. Nonostante ci siano categorie di posta che possono essere generalmente definite spam con un elevato grado di precisione (per esempio i messaggi di massa, le pubblicità), tali messaggi potrebbero appartenere legittimamente alla casella della posta in arrivo di qualche utente.

Pertanto, l'utente è invitato a determinare autonomamente quali messaggi di posta considerare come spam. Dopo l'installazione, Kaspersky Anti-Virus for Windows Workstations chiede di lanciare il training Anti-Spam per distinguere lo spam dalla posta accettata. Ciò è possibile per mezzo degli appositi pulsanti che vengono integrati nel client di posta (Microsoft Outlook, Outlook Express (Windows Mail), The Bat!) oppure servendosi della procedura guidata di addestramento.

**Attenzione!**

Questa versione di Kaspersky Anti-Virus non offre plug-in Anti-Spam per Microsoft Office Outlook in esecuzione su Microsoft Windows 98.

*Per addestrare Anti-Spam utilizzando il pulsante del plug-in nel client di posta,*

1. Aprire il client di posta predefinito del computer (es. Microsoft Office Outlook). Nella barra degli strumenti sono comparsi due pulsanti: **Spam** e **Non spam**.
2. Selezionare una o più messaggi di posta contenenti messaggi validi e fare clic su **Non spam**. Da questo momento, i messaggi di posta provenienti dagli indirizzi selezionati non saranno mai trattate come spam.
3. Selezionare un messaggio di posta, un gruppo di messaggi o una cartella contenente i messaggi considerati come spam e fare clic su **Spam**. Anti-Spam analizza il contenuto di questi messaggi e in futuro considererà tutti i messaggi con contenuto simile come spam.

*Per istruire Anti-Spam con la procedura guidata,*

1. Aprire la finestra delle impostazioni dell'applicazione, selezionare il componente Anti-Spam in **Protezione** e fare clic su **Apprendimento guidato**.
2. Seguire le istruzioni della procedura di Apprendimento guidato di Anti-Spam (vedere 13.2.1, pag. 180).

Quando un messaggio di posta arriva nella casella della posta in arrivo, Anti-Spam ne analizza il contenuto e aggiunge la dicitura [Spam] alla riga dell'oggetto dei messaggi spam. È possibile configurare una speciale regola nel client di posta per questi messaggi, che per esempio stabilisca di eliminarli o di spostarli in una determinata cartella.

## 5.6. Come aggiornare il programma

Kaspersky Lab aggiorna gli elenchi delle minacce di Kaspersky Anti-Virus for Windows Workstations e i moduli per mezzo di appositi server di aggiornamento.

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

**Attenzione!**

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

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

*Per aggiornare manualmente Kaspersky Anti-Virus for Windows Workstations,*

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

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

## 5.7. Come comportarsi in caso di protezione non funzionante

Se si verificano problemi o errori di funzionamento di qualsiasi componente di protezione, è bene verificarne lo stato. Se lo stato del componente è *disattivato* o *disabilitato (errore di funzionamento)*, provare a riavviare Kaspersky Anti-Virus.

Se il problema non si risolve riavviando il programma, si consiglia di risolvere eventuali errori utilizzando la funzione di ripristino del programma (vedere Capitolo 19, pag.301).

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

*Per salvare il rapporto su un file:*

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

*Per salvare in una sola volta un rapporto su tutti i componenti di Kaspersky Anti-Virus for Windows Workstations (componenti di protezione, attività di scansione antivirus, funzioni di supporto):*

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

oppure

Fare clic su Tutti i rapporti nella finestra dei rapporti di qualsiasi componente. A questo punto la scheda **Rapporto** elencherà i rapporti di tutti i componenti del programma.

2. Fare clic sul pulsante **Salva con nome** e specificare nella finestra che si apre il nome del file per il rapporto sulle prestazioni del programma.

---

# CAPITOLO 6. SISTEMA DI GESTIONE DELLA PROTEZIONE

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

- Abilitare, disabilitare e sospendere (vedere 6.1 a pag. 72) il programma
- Definire i tipi di programmi pericolosi (vedere 6.2 a pag. 77) dai quali Kaspersky Anti-Virus for Windows Workstations deve proteggere il computer
- Creare un elenco di esclusioni (vedere 6.3 a pag. 78) per la protezione
- Creare attività di scansione antivirus e di aggiornamento personalizzate (vedere 6.4 a pag. 88)
- Pianificare una serie di scansioni antivirus (vedere 6.5 a pag. 89)
- Configurare le impostazioni di produttività (vedere 6.6 a pag. 91) per la protezione antivirus

## 6.1. Interruzione e ripristino della protezione del computer

Per impostazione predefinita, Kaspersky Anti-Virus viene caricato all'avvio del sistema e protegge il computer per tutto il tempo che resta in uso. Le parole *Kaspersky Anti-Virus 6.0* nell'angolo superiore destro dello schermo indicano tutto ciò. Tutti i componenti di protezione (vedere 2.2.1 a pag. 25) sono attivi.

La protezione fornita da Kaspersky Anti-Virus for Windows Workstations può essere disabilitata completamente o in parte.

### Attenzione!

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

Si noti che in questo caso la protezione è descritta nel contesto dei componenti di protezione. Disabilitare o sospendere i componenti di protezione non



pregiudica le prestazioni delle attività di scansione antivirus o aggiornamento del programma.

## 6.1.1. Sospensione della protezione

Sospendere la protezione significa disabilitare temporaneamente tutti i componenti che monitorano i file sul computer, la posta in entrata e in uscita, gli script eseguibili e il comportamento dell'applicazione.

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

1. Selezionare **Sospendi protezione** nel menu di scelta rapida del programma (vedere 4.2 a pag. 53).
2. Nella finestra Interrompi protezione che si apre (vedere Figura 7), specificare quando si desidera ripristinare la protezione:
  - **Tra <intervallo di tempo>** – la protezione sarà ripristinata dopo il periodo indicato. Utilizzare il menu a discesa per selezionare l'intervallo di tempo.
  - **Al prossimo riavvio del programma** – la protezione sarà abilitata se si apre il programma dal menu Start o dopo aver riavviato il computer (se il programma è impostato per l'avvio automatico all'accensione del computer (vedere 6.1.5 a pag. 76)).
  - **Solo su richiesta dell'utente** – la protezione verrà abilitata solo se avviata manualmente. Per abilitare la protezione, selezionare **Riprendi protezione** dal menù di scelta rapida del programma.

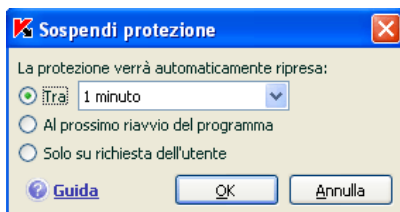



Figura 7. Finestra di sospensione della protezione

**Suggerimento:**

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

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

Se si sospende la protezione, si sospendono tutti i componenti. Questo stato è indicato da quanto segue:

- I nomi dei componenti della sezione **Protezione** della finestra principale sono inattivi (in grigio).
- L'icona nell'area di notifica è inattiva (grigia).
- Il terzo indicatore di protezione (vedere 5.1.1 a pag. 60) del computer segnala che  **Tutti i componenti della protezione sono sospesi.**

## 6.1.2. Interruzione della protezione

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


Se la protezione è interrotta, essa può essere ripristinata esclusivamente dall'utente: i componenti di protezione non si riattiveranno automaticamente dopo il riavvio del sistema o del programma. Si tenga presente che se Kaspersky Anti-Virus for Windows Workstations è in conflitto con altri programmi installati sul computer, è possibile sospendere i singoli componenti o creare un'elenco di esclusioni (vedere 6.3 a pag. 78).

*Per arrestare completamente la protezione:*

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

Dopo aver disabilitato la protezione, tutti i componenti di protezione si arrestano. Questo stato è indicato da quanto segue:


- Nomi inattivi (di colore grigio) dei componenti disabilitati nella sezione Protezione della finestra principale.
- L'icona nell'area di notifica è inattiva (grigia).


- Il terzo indicatore di protezione (vedere 5.1.1 a pag. 60) del computer, che segnala che  **Tutti i componenti della protezione sono disabilitati.**

### 6.1.3. Sospensione/interruzione dei componenti di protezione e delle attività

Esistono molti modi per interrompere un componente di protezione, una scansione antivirus o un aggiornamento. Prima di fare ciò, si consiglia caldamente di stabilire perché è necessario l'arresto. È probabile infatti che esista una soluzione diversa al problema, per esempio modificare il livello di sicurezza. Se, per esempio, si lavora con un database che sicuramente non contiene virus, è sufficiente aggiungerne i file tra le esclusioni (vedere 6.3 a pag. 78).


*Per sospendere componenti della protezione, scansioni antivirus e attività di aggiornamento:*


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

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

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

*Per interrompere componenti della protezione, scansioni antivirus e attività di aggiornamento:*

Fare clic sul pulsante  nella barra di stato. È possibile interrompere i componenti della protezione anche dalla finestra delle impostazioni del programma deselegzionando  **Attiva <nome componente>** nella sezione **Generale** relativa al componente.

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


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

## 6.1.4. Ripristino della protezione del computer

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

- *Dal menu di scelta rapida.*  
A tal fine, selezionare **Riprendi protezione**.
- *Dalla finestra principale del programma.*  
A tal fine, fare clic sul pulsante ► sulla barra di stato nella sezione **Protezione** della finestra principale.

Lo stato della protezione passa immediatamente a **in corso**. L'icona dell'area di notifica diventa attiva (colorata). Anche il terzo indicatore della protezione

(vedere 5.1.1 a pag. 60) informa l'utente che  **Tutti i componenti della protezione sono in esecuzione.**

## 6.1.5. Chiusura del programma


Per chiudere Kaspersky Anti-Virus for Windows Workstations, selezionare **Esci** dal menu di scelta rapida del programma (vedere 4.2 a pag. 53). Il programma si chiude lasciando il computer privo di protezione.

Se le connessioni di rete monitorate dal programma sono attive sul computer nel momento in cui il programma viene chiuso, viene visualizzato un messaggio che informa che queste connessioni saranno interrotte. Ciò è necessario per consentire al programma di chiudersi correttamente. Le connessioni vengono interrotte automaticamente dopo dieci secondi oppure facendo clic su **Si**. La maggior parte delle connessioni sarà ripristinata automaticamente dopo qualche tempo.

Si noti che se è in corso il download di un file senza un download manager, nel momento in cui si interrompe la connessione, il trasferimento del file sarà perso. Sarà necessario scaricare nuovamente il file.

Si può scegliere di non interrompere le connessioni facendo clic sul pulsante **No** nella finestra dell'avviso. In tal caso, il programma resta in esecuzione.

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




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

## 6.2. Tipi di programmi nocivi da monitorare

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

Per specificare da quali programmi nocivi Kaspersky Anti-Virus for Windows Workstations proteggerà il computer, selezionare la sezione **Protezione** nella finestra delle impostazioni del programma (vedere 4.4 a pag. 57).

Il riquadro **Categorie malware** contiene i tipi di minaccia (vedere 1.1 a pag. 11):

-  **Virus, worm, trojan, utilità di hacking.** Questo gruppo combina le categorie più comuni e pericolose di programmi nocivi. Questo è il livello di sicurezza minimo ammissibile. Come da raccomandazioni degli esperti di Kaspersky Lab, Kaspersky Anti-Virus controlla sempre questa categoria di programmi nocivi.
-  **Spyware, adware, dialer.** Questo gruppo include il software potenzialmente pericoloso che potrebbe dare problemi all'utente o causare danni gravi.
-  **Software potenzialmente pericoloso (riskware).** Questo gruppo include programmi che non sono nocivi o pericolosi. Tuttavia, in determinate circostanze possono essere utilizzati per causare danni al computer in uso.

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

Se tutti i gruppi sono selezionati, Kaspersky Anti-Virus for Windows Workstations garantisce la massima protezione antivirus del computer. Se il secondo e il terzo gruppo sono disabilitati, il programma protegge solo dai programmi nocivi più comuni. Fra questi non sono compresi i programmi potenzialmente pericolosi

che potrebbero essere installati sul computer e danneggiare i file, provocare perdite finanziarie e rubare tempo.

Kaspersky Lab sconsiglia di disabilitare il monitoraggio del secondo gruppo. Se si verificano situazioni in cui Kaspersky Anti-Virus for Windows Workstations classifica un programma che non viene considerato pericoloso come potenzialmente pericoloso, si consiglia di configurare un'esclusione per esso (vedere 6.3 a pag. 78).

## 6.3. Creazione di una zona attendibile

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

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

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

### Attenzione!

Un oggetto escluso non viene esaminato quando il disco o la cartella che lo contiene vengono sottoposti a scansione. Tuttavia, se l'oggetto viene specificatamente selezionato, la regola di esclusione non verrà applicata.

*Per creare un elenco di esclusioni,*

1. Aprire la finestra delle impostazioni di Kaspersky Anti-Virus for Windows Workstations e selezionare la sezione **Protezione**.
2. Fare clic sul pulsante **Area attendibile** nella sezione **Generale**.
3. Configurare le regole di esclusione per gli oggetti e creare una lista delle applicazioni attendibili nella finestra che si apre (vedere Figura 8).

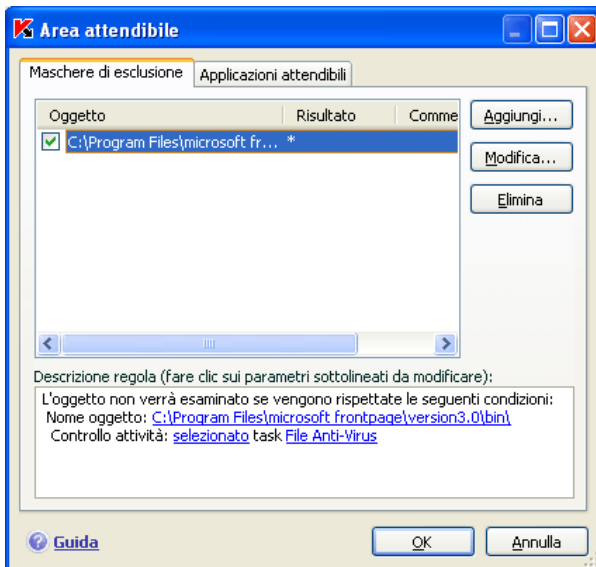


Figura 8. Creazione di una zona attendibile

### 6.3.1. Regole di esclusione

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

È possibile escludere i file dalla scansione in base al formato, usare una maschera, escludere una determinata area, come ad esempio una cartella, un programma, i processi di programmi od oggetti, in base al loro risultato.

Il *risultato* è lo stato che Kaspersky Anti-Virus for Windows Workstations assegna a un oggetto durante la scansione. Il verdetto si basa sulla classificazione dei programmi nocivi e potenzialmente pericolosi presenti nella Virus Encyclopedia di Kaspersky Lab.

Il software potenzialmente pericoloso non svolge una funzione nociva vera e propria ma può essere utilizzato dagli hacker come componente ausiliario di un codice maligno in quanto contiene errori e vulnerabilità. Di questa categoria fanno parte, per esempio, programmi di amministrazione remota, i client IRC, i server FTP, le utilità multifunzione per interrompere o nascondere i processi, i keylogger, le macro per la decodifica di password, gli autodialer, ecc. Questi programmi non sono classificati come virus. Essi possono essere suddivisi in diverse categorie, per esempio adware, joke, riskware, ecc. (per ulteriori

informazioni sui programmi potenzialmente pericolosi individuati da Kaspersky Anti-Virus for Windows Workstations, vedere la Virus Encyclopedia all'indirizzo [www.viruslist.com](http://www.viruslist.com)). Dopo la scansione, questi programmi possono essere bloccati. Poiché molti di loro sono molto comuni, è possibile escluderli dalla scansione. A tal fine, occorre specificare il verdetto assegnato a quel programma come maschera di esclusione.

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

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

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

1. Fare clic sul pulsante **Aggiungi** nella scheda **Maschere di esclusione**.
2. Nella finestra che si apre (vedere Figura 9), fare clic sul tipo di esclusione nella sezione **Proprietà**:
  - Oggetto** – esclusione dalle scansioni di un determinato oggetto, directory o file che corrisponde a una certa maschera.
  - Risultato** – esclusione degli oggetti dalla scansione in base allo stato ad essi assegnato dalla Virus Encyclopedia.



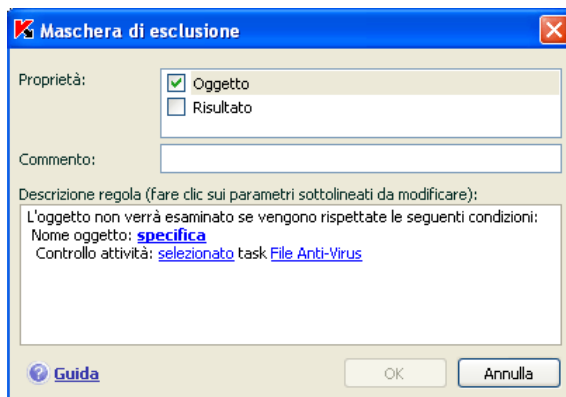


Figura 9. Creazione di una regola di esclusione

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

- Se si specifica un certo file come **Oggetto** e un certo stato nella sezione **Risultato**, il file specificato verrà escluso solo se durante la scansione viene classificato come la minaccia selezionata.
  - Se si seleziona un'area o una cartella come **Oggetto** e lo stato (o maschera di risultato) come **Risultato**, gli oggetti contrassegnati da quello stato saranno esclusi solo dalla scansione in quell'area o cartella.
3. Assegnare valori ai tipi di esclusione selezionati. A tal fine, fare clic nella sezione **Descrizione regola** sul collegamento specifica situato accanto al tipo di esclusione:
- Per il tipo di **Oggetto**, immettere il relativo nome nella finestra che si apre (può essere un file, una cartella particolare o una maschera di file (vedere A.2 a pag. 331). Selezionare  **Includi sottocartelle** per l'oggetto (file, maschera file, cartella) affinché sia ripetutamente escluso dalla scansione. Per esempio se **C:\Programmi\winword.exe** è stato assegnato come esclusione e l'opzione Includi sottocartelle è stata selezionata, il file **winword.exe** sarà escluso dalla scansione se si trova in qualsiasi sottocartella in **C:\Programmi**.
  - Digitare il nome completo della minaccia che si desidera escludere dalle scansioni come indicato nell'enciclopedia dei

virus, oppure utilizzare una maschera (vedere A.3 a pag. 331) per il **Risultato**.

Per alcuni risultati, è possibile assegnare condizioni avanzate per l'applicazione delle regole nel campo **Impostazioni avanzate** (vedere A.3 a pag. 331). Nella maggior parte dei casi, questo campo è compilato automaticamente quando si aggiunge una regola di esclusione da un avviso di Difesa proattiva.

È possibile aggiungere impostazioni avanzate per i seguenti verdetti in particolare:

- *Invader*. Per questa classificazione, è possibile fornire un nome, una maschera o un percorso completo fino all'oggetto incorporato (per esempio, un file .dll) come condizione supplementare di esclusione.
  - *Lancio Internet Browser*. Per questo verdetto è possibile elencare le impostazioni di apertura del browser come impostazioni di esclusione supplementari.  
Per esempio, si è deciso di bloccare i browser dall'apertura con determinate impostazioni nell'analisi dell'attività dell'applicazione Difesa proattiva. Tuttavia, si vuole consentire al browser di aprire il dominio *www.kaspersky.com* con un collegamento da Microsoft Office Outlook come regola di esclusione. A tal fine, selezionare Microsoft Office Outlook come **Oggetto** e *Lancio browser Internet* come **Risultato**, quindi immettere una maschera di dominio ammessa nel campo **Impostazioni avanzate**.
4. È possibile definire quali componenti di Kaspersky Anti-Virus for Windows Workstations utilizzeranno questa regola. Se è selezionata l'opzione qualsiasi, questa regola si applica a tutti i componenti. Per limitare la regola a uno o più componenti, fare clic su qualsiasi, che si modificherà in selezionato. Nella finestra che si apre, selezionare le caselle relative ai componenti ai quali si desidera applicare questa regola di esclusione.

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

1. Utilizzare il collegamento Aggiungi a zona attendibile nella finestra dell'avviso (vedere Figura 10).
2. Nella finestra che si apre, verificare che tutte le impostazioni delle regole di esclusione corrispondano alle proprie esigenze. Il programma inserisce automaticamente il nome dell'oggetto e il tipo di minaccia in

base alle informazioni ottenute dalla notifica. Per creare una regola, fare clic su **OK**.

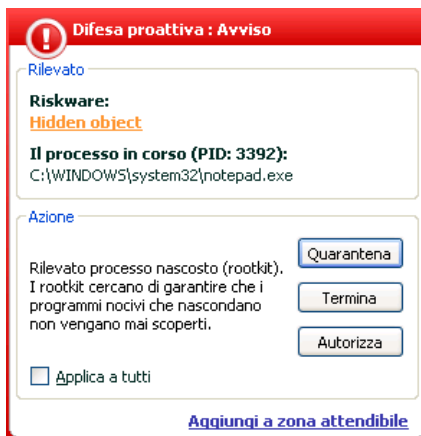


Figura 10. Avviso di intercettazione di oggetto pericoloso

*Per creare una regola di esclusione dalla finestra dei rapporti:*

1. Selezionare nel rapporto l'oggetto che si desidera aggiungere alle esclusioni.
2. Aprire il menu di scelta rapida e selezionare **Aggiungi a zona attendibile** (vedere Figura 11).

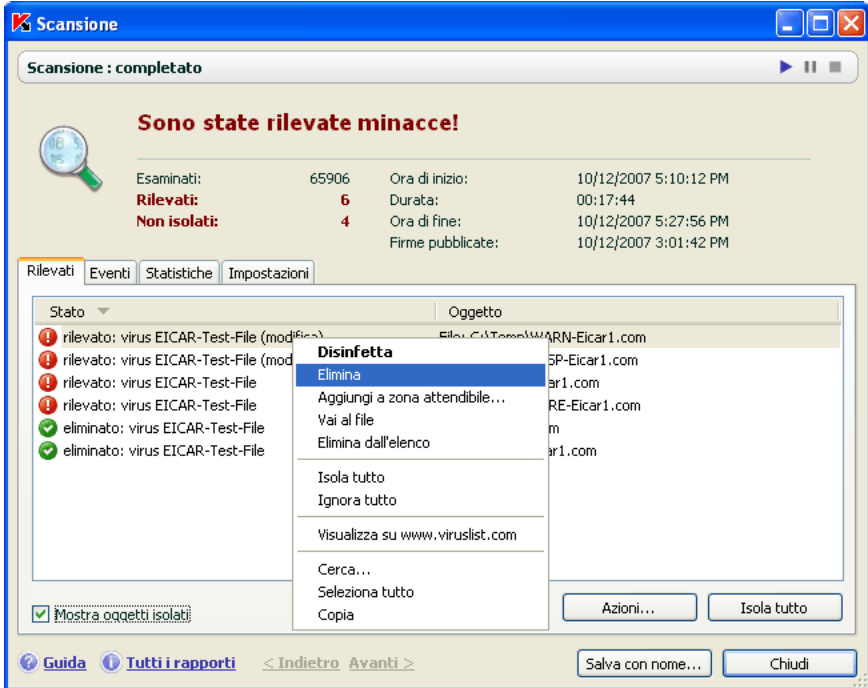


Figura 11. Creazione di una regola di esclusione da un rapporto

3. Si apre quindi la finestra delle impostazioni delle esclusioni. Verificare che tutte le impostazioni delle regole di esclusione corrispondano alle proprie esigenze. Il programma inserisce automaticamente il nome dell'oggetto e il tipo di minaccia in base alle informazioni ottenute dal rapporto. Per creare una regola, fare clic su **OK**.

### 6.3.2. Applicazioni attendibili

È possibile escludere esclusivamente le applicazioni attendibili dalla scansione antivirus di Kaspersky Anti-Virus, se è installato su un computer che esegue Microsoft Windows NT 4.0/2000/XP/Vista.

Kaspersky Anti-Virus consente di creare una lista delle applicazioni attendibili le cui attività, sospette o meno, nonché l'accesso ai file, alla rete ed al registro di sistema, non vengono monitorate.

Per esempio, si può ritenere che gli oggetti e i processi utilizzati dal **Blocco note** di Windows siano sicuri e non necessitino di scansione. Per escludere gli oggetti utilizzati da questo processo dalla scansione, aggiungere **Blocco note** alla lista delle applicazioni attendibili. Tuttavia, il file eseguibile e il processo dell'applicazione affidabile saranno sottoposti a scansione antivirus come in precedenza. Per escludere completamente l'applicazione dalla scansione, è necessario utilizzare le regole di esclusione (vedere 6.3.1 a pag. 79).

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

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

Come impostazione predefinita, Kaspersky Anti-Virus for Windows Workstations scansiona gli oggetti aperti, in esecuzione, o salvati da qualsiasi processo di programma e monitora l'attività di tutti i programmi e il traffico di rete che creano.

È possibile creare un'elenco delle applicazioni attendibili sull'apposita scheda **Applicazioni attendibili** (vedere Figura 12). Per impostazione predefinita, tale elenco contiene le applicazioni che non saranno monitorate sulla base delle raccomandazioni di Kaspersky Lab quando s'installa Kaspersky Anti-Virus. Se non si ritiene affidabile una applicazione dell'elenco, deselezionare la relativa casella di controllo. Per modificare l'elenco, utilizzare i pulsanti **Aggiungi**, **Modifica** ed **Elimina** sulla destra.

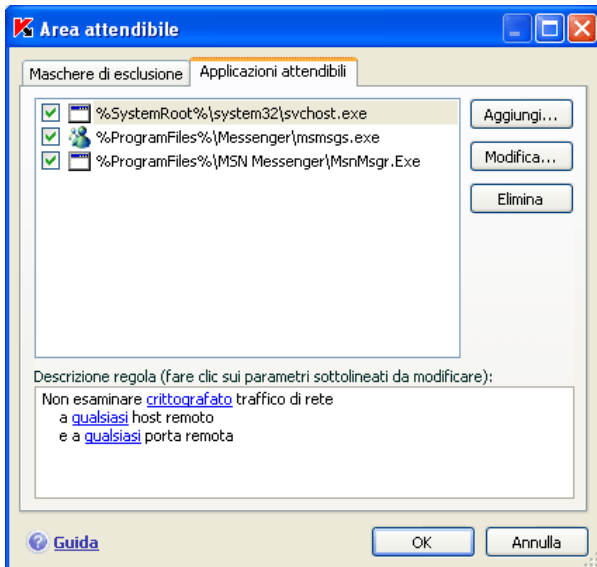


Figura 12. Elenco delle applicazioni attendibili

*Per aggiungere un programma all'elenco delle applicazioni attendibili:*

1. Fare clic sul pulsante **Aggiungi** sulla parte destra della scheda **Applicazioni attendibili**.
2. Nella finestra Applicazioni attendibili (Figura 13) che si apre, selezionare l'applicazione utilizzando il pulsante **Sfoggia**. Si apre un menu di scelta rapida dal quale, facendo clic su **Sfoggia**, si va alla finestra di selezione file, dove è possibile selezionare il percorso al file eseguibile, oppure, facendo clic su **Applicazioni** si va a un elenco di applicazioni attualmente in funzione, che possono essere eventualmente selezionate.

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

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

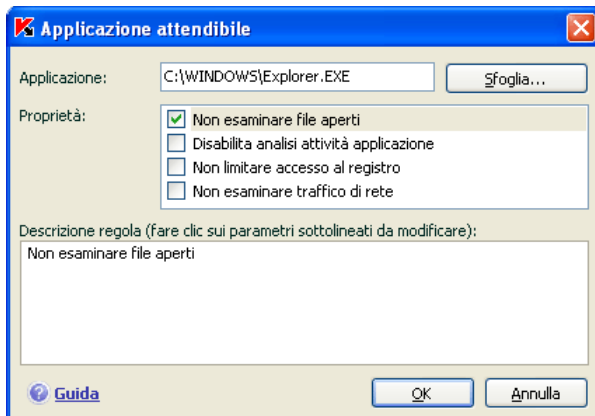


Figura 13. Aggiunta di un'applicazione all'elenco delle applicazioni attendibili

3. Specificare quali azioni eseguite da questo processo non saranno monitorate:

- Non esaminare file aperti** – esclude dalla scansione tutti i file aperti dal processo dell'applicazione attendibile.
- Disabilita analisi attività applicazione** – esclude dal monitoraggio di Difesa proattiva qualsiasi attività, sospetta o meno, eseguita dall'applicazione attendibile.
- Non limitare accesso al registro** – esclude i tentativi di accesso al registro di sistema dalla scansione quando sono lanciati da applicazioni attendibili.
- Non esaminare traffico di rete** – esclude dalla scansione anti-virus e anti-spam il traffico di rete lanciato dalle applicazioni attendibili. È possibile escludere dalla scansione il traffico di rete o quello protetto (SSL) generato da tali applicazioni. A tal fine, usare il collegamento Tutto. Questo sarà modificato in crittografato. È inoltre possibile limitare l'esclusione assegnando una porta remota o un host remoto. Per creare una limitazione, fare clic su tutti, che diventeranno selezionati, e digitare un valore per la porta/host remoto.

Si noti che se è selezionata l'opzione  **Non esaminare traffico di rete**, il traffico per quell'applicazione sarà sottoposto solo alla scansione anti-virus e anti-spam. Questo tuttavia non influisce sulla scansione del traffico da parte di Anti-Hacker. Le impostazioni di Anti-Hacker gestiscono l'analisi dell'attività di rete per quell'applicazione.

## 6.4. Avvio di attività con un altro profilo

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

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

Si noti che questa funzione non è disponibile in Microsoft Windows 98/ME.

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

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

1. Selezionare il nome dell'attività nelle sezioni **Scansione** (per le attività di scansione antivirus) o **Servizio** (per attività di aggiornamento) della finestra principale ed utilizzare il collegamento Impostazioni per aprire la finestra delle impostazioni delle attività.
2. Fare clic sul pulsante **Personalizza** nella finestra delle impostazioni dell'attività e andare alla scheda **Avanzate** nella finestra che si apre (vedere Figura 14).

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

Si noti che se l'attività non viene eseguita da un utente che disponga dei privilegi necessari, l'aggiornamento pianificato verrà eseguito con i privilegi dell'account utente corrente. Se non ci sono utenti attualmente collegati al computer, l'esecuzione degli aggiornamenti con un altro account utente non è stata configurata, e gli aggiornamenti vengono eseguiti automaticamente, essi verranno eseguiti con i privilegi SYSTEM.



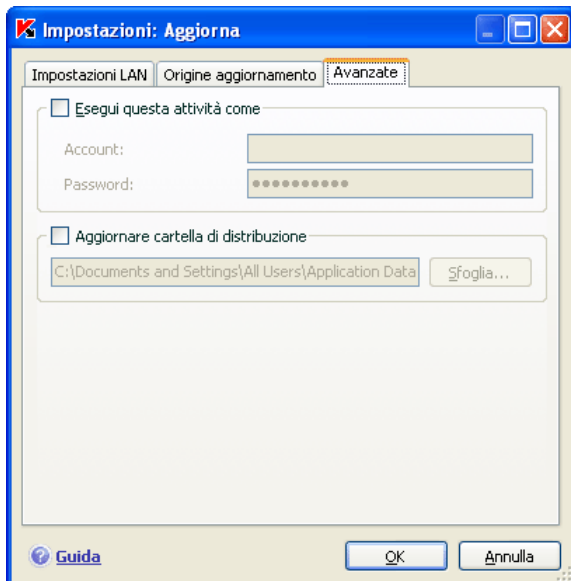


Figura 14. Configurazione di un'attività di aggiornamento da un altro profilo

## 6.5. Configurazione delle attività pianificate e delle notifiche

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

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

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

Per fare avviare le attività in base a una pianificazione, selezionare la casella dell'avvio automatico delle attività nella sezione **Modalità esecuzione**. L'orario di avvio dell'attività di scansione può essere modificato nella finestra **Pianificazione** (vedere Figura 15), che si apre facendo clic su **Cambia**.



Figura 15. Pianificazione delle attività

L'impostazione primaria da definire è la frequenza di un evento (esecuzione o notifica di un'attività). Selezionare l'opzione desiderata in **Frequenza** (vedere Figura 15). Quindi, le impostazioni per l'opzione selezionata devono essere specificate in Impostazioni di pianificazione. Sono disponibili diverse opzioni:

- Ogni minuto.** L'intervallo di tempo tra le scansioni è di parecchi minuti. Specificare l'intervallo di tempo in minuti nelle impostazioni di pianificazione. Non deve essere superiore a 59 minuti.
- Ogni ora.** L'intervallo tra le scansioni o le notifiche è di diverse ore. Se questa opzione viene selezionata, specificare l'intervallo temporale nelle impostazioni di pianificazione: **Ogni N ora/e** e specificare *N*. Per esempio, immettere **Ogni 1 ora/e** se si intende eseguire l'operazione a cadenza oraria.
- Ogni giorno.** L'attività viene avviata o la notifica viene inviata ad intervalli di diversi giorni. Specificare l'intervallo nelle impostazioni di pianificazione:

  - Selezionare **Ogni N giorno(i)** ed immettere un valore per *N* se si desidera mantenere un intervallo di diversi giorni.
  - Selezionare **Ogni giorno feriale** per eseguire l'attività quotidianamente, dal lunedì al venerdì.
  - Selezionare **Ogni fine settimana** per eseguire l'attività o inviare la notifica solo di sabato e domenica.

Utilizzare il campo **Ora** per specificare a che ora del giorno verrà eseguita l'attività di scansione.

- **Ogni settimana.** L'attività viene avviata o la notifica inviata in certi giorni della settimana. Se si seleziona questa opzione, apporre i segni di spunta accanto ai giorni della settimana in cui si desidera lanciare l'attività. Inserire l'ora del giorno nel campo **Ora**.
- **Ogni mese.** L'attività viene avviata o la notifica inviata una volta al mese, ad un'ora specificata.
- **A un'ora specificata.** Avvia un'attività o invia una notifica alla data ed all'ora specificate.
- **All'avvio del programma.** Avvia un'attività o invia una notifica ogni volta che Kaspersky Anti-Virus viene avviato. È inoltre possibile specificare un ritardo in relazione all'avvio di un'attività da parte dell'applicazione.
- **Dopo ogni aggiornamento.** L'attività parte dopo ciascun aggiornamento all'elenco delle minacce (quest'opzione si applica solo alle scansioni antivirus).

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

## 6.6. Opzioni di alimentazione

Per preservare la batteria del laptop e ridurre il carico sul processore e sui sottosistemi del disco è possibile posticipare le scansioni antivirus:

- Poiché le scansioni antivirus a gli aggiornamenti del programma richiedono talvolta una discreta quantità di risorse e possono durare diverso tempo, si raccomanda di disabilitare le pianificazioni di queste attività, aiutando a prolungare la durata delle batterie. Se necessario, è possibile aggiornare manualmente il programma (vedere 5.6 a pag. 69) oppure avviare una scansione antivirus (vedere 5.2 a pag. 65). Per utilizzare la funzione di risparmio energetico, selezionare  **Disattiva le scansioni programmate durante l'esecuzione con alimentazione a batteria**.
- Le scansioni antivirus aumentano il carico sul processore centrale e sui sottosistemi del disco, rallentando di conseguenza altri programmi. Per impostazione predefinita, in tali circostanze il programma sospende temporaneamente la scansione antivirus e libera risorse di sistema per le applicazioni dell'utente.

Esistono tuttavia numerosi programmi che possono essere avviati non appena si liberano risorse di sistema e funzionano in modalità secondaria. Affinché le scansioni antivirus non dipendano dal funzionamento di tali programmi, deselezionare  **Concedi risorse ad altre applicazioni**.

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

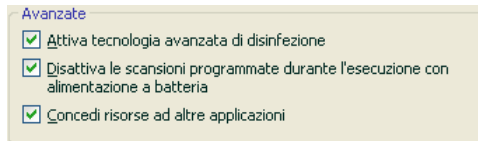


Figura 16. Configurazione delle impostazioni di alimentazione

*Per configurare le impostazioni di alimentazione per le scansioni anti-virus:*

Selezionare la sezione **Protezione** della finestra principale del programma e fare clic su Impostazioni. Configurare le impostazioni di alimentazione nel riquadro **Avanzate** (vedere Figura 16).

## 6.7. Tecnologia avanzata di disinfezione

I programmi nocivi moderni possono invadere i livelli più bassi di un sistema operativo, il che li rende praticamente impossibile da rilevare. Kaspersky Anti-Virus 6.0 chiede se si desidera eseguire la Tecnologia avanzata di disinfezione quando rileva una minaccia attualmente attiva nel sistema. Ciò neutralizza la minaccia eliminandola dal computer.

In seguito a questa procedura, occorre riavviare il computer. Dopo il riavvio del computer, si raccomanda di eseguire una scansione anti-virus completa. Per utilizzare la Tecnologia avanzata di disinfezione, selezionare  **Attiva tecnologia avanzata di disinfezione**.


*Per attivare/disattivare la tecnologia avanzata di disinfezione:*

Selezionare la sezione **Protezione** della finestra principale del programma e fare clic sul collegamento Impostazioni. Configurare le impostazioni di alimentazione nel riquadro **Avanzate** (vedere Figura 16).

---

# CAPITOLO 7. FILE ANTI-VIRUS

Il componente di Kaspersky Anti-Virus for Windows Workstations che protegge i file del computer dalle infezioni è *File Anti-Virus*. Esso viene caricato all'avvio del sistema operativo ed eseguito nella RAM del computer, ed esamina tutti i file aperti, salvati o eseguiti.

L'attività del componente viene indicata dall'icona di Kaspersky Anti-Virus for Windows Workstations nell'area di notifica, che ha il seguente aspetto  ogniqualvolta viene esaminato un file.

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

1. Ogni volta che si verifica l'accesso da parte dell'utente o di un programma, il componente lo intercetta.
2. File Anti-Virus esamina i database di iChecker™ e iSwift™ in cerca di informazioni sul file intercettato. La decisione se esaminare o meno il file viene presa in base alle informazioni recuperate.

Il processo di scansione si svolge come segue:

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

## 7.1. Selezione di un livello di sicurezza dei file

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

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

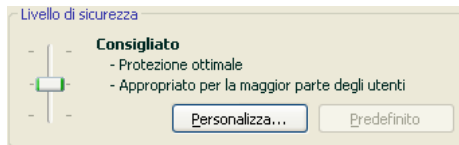


Figura 17. Livello di sicurezza di File Anti-Virus

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

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

*Per modificare il livello di sicurezza:*

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

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

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

Esempio:

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

Suggerimento per la selezione di un livello:

In base ai dati sulla provenienza, si potrebbe concludere che il rischio di infezione da parte di un programma nocivo sia piuttosto elevato. Le dimensioni e il tipo dei file gestiti sono molto eterogenei e l'eventuale esclusione di qualsiasi file dalla scansione comporterebbe un rischio elevato per i dati del computer. L'utente desidera esaminare i file utilizzati in base al contenuto, non in base all'estensione.

Si consiglia di iniziare con il livello di sicurezza **Consigliato** apportando le seguenti modifiche: rimuovere le restrizioni sui file eliminati e ottimizzare il funzionamento di File Anti-Virus esaminando solo i file nuovi e modificati. In tal modo la scansione non influirà eccessivamente sulle risorse di sistema e sarà possibile continuare a usare senza problemi altre applicazioni.

*Per modificare le impostazioni di un livello di sicurezza:*

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

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

## 7.2. Configurazione di File Anti-Virus

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

- Impostazioni che definiscono i tipi di file (vedere 7.2.1 a pag. 96) da sottoporre alla scansione antivirus
- Impostazioni che definiscono l'ambito della protezione (vedere 7.2.2 a pag. 98)

- Impostazioni che definiscono le reazioni del programma agli oggetti pericolosi individuati (vedere 7.2.5 a pag. 104).
- Impostazioni supplementari di File Anti-Virus (vedere 7.2.3 a pag. 100)

La presente sezione prende in esame dettagliatamente questi gruppi.

## 7.2.1. Definizione dei tipi di file da esaminare

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

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

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

- **Esamina tutti i file.** Con questa opzione selezionata tutti gli oggetti del file system che vengono aperti, eseguiti o salvati saranno esaminati senza eccezioni.
- **Esamina programmi e documenti (in base al contenuto).** Selezionando questo gruppo di file, File Anti-Virus esamina solo i file potenzialmente infetti, che potrebbero contenere un virus.

**Nota:**

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

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

Prima dell'analisi anti-virus di un file, viene analizzato il formato della sua intestazione (txt, doc, exe, ecc.). Se dall'analisi risulta che il formato del file non consente infezioni, il file viene escluso dalla scansione e messo immediatamente a disposizione dell'utente. Se il formato file è infettabile, il file viene sottoposto a scansione antivirus.



- Esamina programmi e documenti (in base all'estensione)**. Se è stata selezionata questa opzione, File Anti-Virus esamina solo i file potenzialmente infetti determinandone il formato file in base all'estensione. Per mezzo del collegamento estensione, è possibile consultare un elenco delle estensioni (vedere A.1 a pag. 327) esaminate con questa opzione.

#### Suggerimento:

Ricordare che è possibile inviare virus all'interno di file con estensione (ad esempio, .txt) che sono in realtà file eseguibili rinominati come file di testo. Selezionando l'opzione  **Esamina programmi e documenti (in base all'estensione)**, tale file sarebbe escluso dalla scansione. Selezionando invece l'opzione  **Esamina programmi e documenti (in base al contenuto)**, il programma ignorerà l'estensione del file analizzandone invece l'intestazione, determinandone così la reale natura di file eseguibile. File Anti-Virus esaminerà il file alla ricerca di virus.

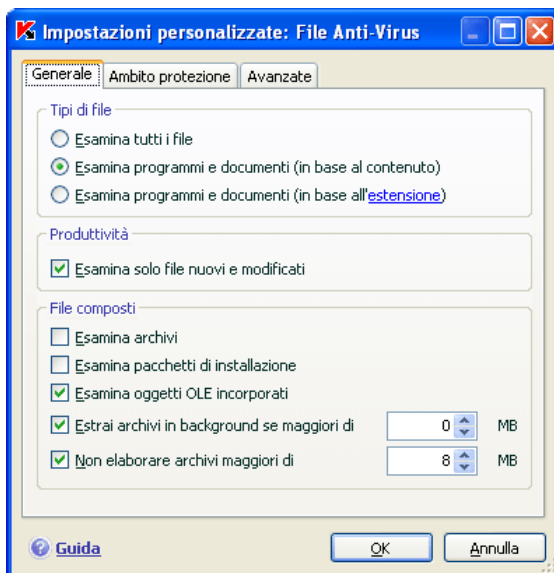


Figura 18. Selezione dei tipi di file sottoposti a scansione antivirus.

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

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

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

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

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

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

## 7.2.2. Definizione dell'ambito della protezione

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

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

1. Selezionare **File Anti-Virus** nella finestra principale e andare alla finestra delle impostazioni del componente facendo clic su Impostazioni.
2. Fare clic sul pulsante **Personalizza** e selezionare la scheda **Ambito protezione** (vedere Figura 19) nella finestra che si apre.

La scheda visualizza un elenco di oggetti che File Anti-Virus analizzerà. La protezione è abilitata per impostazione predefinita per tutti gli oggetti presenti sui dischi fissi, su supporti esterni e su unità di rete connesse al computer. Utilizzare i pulsanti **Aggiungi**, **Modifica** ed **Elimina** per aggiungere elementi della lista e modificarla.

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

- Specificare solo le cartelle, le unità e i file che necessitano di protezione.
- Creare un elenco di oggetti che non necessitano di protezione (vedere 6.3 a pag. 78).
- Combinare i metodi uno e due per creare una protezione il cui ambito esclude una serie di oggetti.

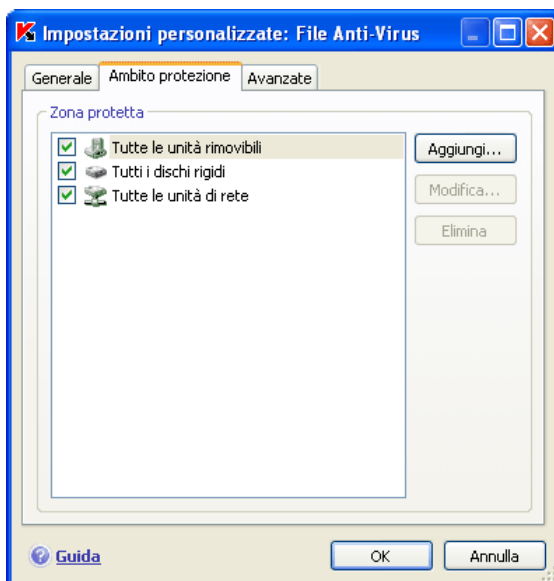


Figura 19. Definizione dell'ambito della protezione

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

- **C:\dir\\*.\*** o **C:\dir\\*** o **C:\dir\** – tutti i file nella cartella **C:\dir\**
- **C:\dir\\*.exe** – tutti i file con estensione \*.exe contenuti nella cartella **C:\dir\**

- **C:\dir\*.ex?** – tutti i file con estensione .ex? nella cartella C:\dir\, dove ? può rappresentare qualsiasi carattere
- **C:\dir\test** – solo il file C:\dir\test

Per eseguire la scansione in modo ripetitivo, selezionare  **Includi sottocartelle**.

#### Attenzione!

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

## 7.2.3. Configurazione delle impostazioni avanzate

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

*Per configurare le impostazioni avanzate di File Anti-Virus:*

1. Selezionare **File Anti-Virus** nella finestra principale e passare alla finestra delle impostazioni del componente facendo clic sul collegamento Impostazioni.
2. Fare clic sul pulsante **Personalizza** e selezionare la scheda **Avanzate** nella finestra che si apre (vedere Figura 20).

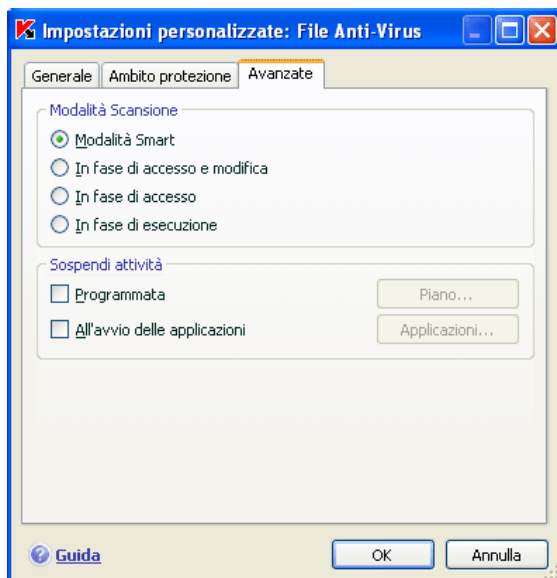


Figura 20. Configurazione delle impostazioni supplementari Anti-Virus file

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

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

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

La modalità Smart è quella predefinita.

- **In fase di accesso e modifica** – Anti-Virus file esamina i file quando vengono aperti o modificati.
- **In fase di accesso** – i file vengono esaminati solo quando si cerca di aprirli.
- **In fase di esecuzione** – i file vengono esaminati solo quando si cerca di eseguirli.

Potrebbe essere necessario sospendere l'attività di Anti-Virus file quando si eseguono attività che richiedano una grande quantità di risorse del sistema. Per diminuire il carico e fare in modo che l'utente riottienga rapidamente l'accesso ai

file, si consiglia di configurare il componente per la disattivazione ad una certa ora o quando vengono utilizzati determinati programmi.

Per sospendere l'attività del componente per un certo tempo, selezionare  **Programmata** e fare clic su **Piano** per assegnare un intervallo per la disattivazione del componente nella finestra che si apre (vedere Figura 21). Per fare ciò, inserire una valore in formato HH:MM nei campi corrispondenti.

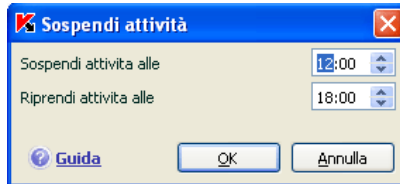


Figura 21. Sospensione dell'attività del componente

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

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

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

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

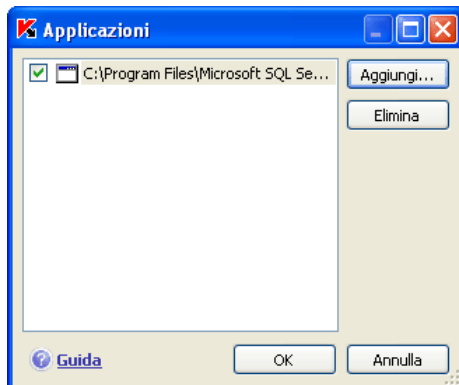


Figura 22. Creazione di un elenco di applicazioni

## 7.2.4. Ripristino delle impostazioni di File Anti-Virus

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

*Per ripristinare le impostazioni predefinite di File Anti-Virus:*

1. Selezionare **File Anti-Virus** nella finestra principale e andare alla finestra delle impostazioni del componente facendo clic su Impostazioni.
2. Fare clic sul pulsante **Predefinito** nella sezione **Livello di sicurezza**.

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

## 7.2.5. Selezione delle azioni da applicare agli oggetti

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

File Anti-Virus applica agli oggetti i seguenti stati:

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

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

*Per modificare un'azione da applicare a un oggetto:*

selezionare **File Anti-Virus** nella finestra principale e andare alla finestra delle impostazioni del componente facendo clic su Impostazioni. Nelle sezioni corrispondenti vengono visualizzate tutte le potenziali azioni (vedere Figura 23).

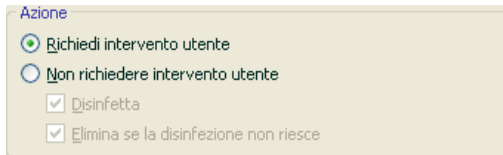


Figura 23. Azioni possibili di File Anti-Virus in caso di oggetti pericolosi


| Se l'azione selezionata è  | Quando viene rilevato un oggetto pericoloso  |
|--|--|
| <input checked="" type="radio"/> <b>Richiedi intervento utente</b> | File Anti-Virus visualizza un avvertimento contenente informazioni sul programma nocivo che ha o potrebbe aver infettato il file e propone una serie di azioni da scegliere. Le azioni possono variare in funzione dello stato dell'oggetto. |



| Se l'azione selezionata è   | Quando viene rilevato un oggetto pericoloso   |
|---|---|
| <input checked="" type="radio"/> <b>Non richiedere intervento utente</b>  | File Anti-Virus blocca l'accesso all'oggetto. Le informazioni relative all'evento vengono registrate nel rapporto (vedere 17.3 a pag. 243). In un secondo tempo sarà possibile tentare di disinfettare l'oggetto.   |
| <input checked="" type="radio"/> <b>Non richiedere intervento utente</b><br><input checked="" type="checkbox"/> <b>Disinfetta</b>   | File Anti-Virus blocca l'accesso all'oggetto e cerca di disinfettarlo. Se la disinfezione ha esito positivo, il file viene ripristinato per l'uso. Se la disinfezione non riesce, il file verrà considerato <i>potenzialmente infetto</i> e spostato in Quarantena (vedere 17.1 a pag. 237). Le informazioni relative all'evento vengono registrate nel rapporto. In un secondo tempo sarà possibile tentare di disinfettare l'oggetto. |
| <input checked="" type="radio"/> <b>Non richiedere intervento utente</b><br><input checked="" type="checkbox"/> <b>Disinfetta</b><br><input checked="" type="checkbox"/> <b>Elimina se la disinfezione non riesce</b> | File Anti-Virus blocca l'accesso all'oggetto e cerca di disinfettarlo. Se la disinfezione ha esito positivo, il file viene ripristinato per l'uso. Se la disinfezione non riesce, l'oggetto viene eliminato. Una copia dell'oggetto viene conservata in backup (vedere 17.2 a pag. 241).  |
| <input checked="" type="radio"/> <b>Non richiedere intervento utente</b><br><input type="checkbox"/> <b>Disinfetta</b><br><input checked="" type="checkbox"/> <b>Elimina</b>  | File Anti-Virus blocca l'accesso all'oggetto e lo elimina.  |

Prima di disinfettare o eliminare l'oggetto, Kaspersky Anti-Virus for Windows Workstations ne crea una copia di backup, qualora l'oggetto dovesse essere ripristinato o si presentasse la possibilità di trattarlo.

## 7.3. Riparazione posticipata

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

Se l'azione selezionata fosse

 **Non richiedere intervento utente**

**Disinfetta**

anche tutti gli oggetti non trattati saranno bloccati.

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

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


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

---

# CAPITOLO 8. ANTI-VIRUS

## POSTA

*Anti-Virus posta* è il componente di Kaspersky Anti-Virus for Windows Workstations dedicato a prevenire che i messaggi di posta elettronica in entrata ed uscita trasferiscano oggetti pericolosi. Esso viene eseguito all'avvio del sistema, rimane attivo nella memoria di sistema ed esamina tutta la posta basata sui protocolli POP3, SMTP, IMAP, MAPI<sup>1</sup> e NNTP, nonché le connessioni crittografate (SSL) per POP3 e IMAP (SSL).

L'attività del componente viene indicata dall'icona di Kaspersky Anti-Virus for Windows Workstations nell'area di notifica, che ha il seguente aspetto  ogniqualvolta viene esaminato un messaggio di posta.

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

1. Anti-Virus posta intercetta ciascun messaggio ricevuto o inviato dall'utente.
2. Il messaggio viene suddiviso nelle parti che lo compongono: intestazioni del messaggio, corpo del messaggio, allegati.
3. Il corpo del messaggio e gli allegati (inclusi gli allegati OLE) vengono esaminati per escludere la presenza di oggetti pericolosi. Gli oggetti nocivi sono rilevati utilizzando *gli elenchi dei virus* inclusi nel programma e con l'algoritmo euristico. Gli elenchi contengono le descrizioni di tutti i programmi nocivi noti e dei metodi per neutralizzarli. L'algoritmo euristico è in grado di rilevare nuovi virus non ancora inseriti negli elenchi.
4. Dopo la scansione antivirus è possibile scegliere tra le seguenti azioni:
  - Se il corpo o gli allegati del messaggio contengono un codice nocivo, Anti-Virus posta blocca il messaggio, memorizza una copia dell'oggetto infetto nella memoria di *back-up*, e cerca di disinfettarlo. Se la pulizia del messaggio riesce, viene di nuovo messa a disposizione dell'utente. In caso contrario, l'oggetto infetto nel messaggio viene eliminato. Dopo la scansione antivirus, nel campo dell'oggetto del messaggio viene inserito

---

<sup>1</sup>I messaggi di posta elettronica inviati con il protocollo MAPI vengono esaminate per mezzo di uno speciale plug-in per Microsoft Office Outlook e The Bat!

un testo che dichiara che il messaggio è stato esaminato da Kaspersky Anti-Virus for Windows Workstations.

- Se nel corpo o nell' allegato viene rilevato codice che sembra essere nocivo ma non in maniera certa, la parte sospetta del messaggio viene inviata nella cartella di *Quarantena*.
- Se all'interno del messaggio non viene individuato alcun codice nocivo, il messaggio viene reso nuovamente disponibile.

Il programma è dotato di uno speciale plug-in (vedere 8.2.2 a pag. 112) per Microsoft Outlook in grado di configurare le scansioni della posta con maggior precisione.

Se si usa il client di posta The Bat!, Kaspersky Anti-Virus for Windows Workstations può essere utilizzato unitamente ad altre applicazioni anti-virus. Le regole di elaborazione del traffico di posta elettronica (vedere 8.2.3 a pag. 114) sono configurate direttamente da The Bat! e sostituiscono le impostazioni di protezione della posta di Kaspersky Anti-Virus for Windows Workstations.

#### Attenzione!

Questa versione di Kaspersky Anti-Virus non offre plug-in Anti-Virus posta per le versioni a 64 bit dei client di posta elettronica.

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

Si noti che i messaggi di posta trasmessi su IMAP non vengono esaminati in Thunderbird se si usano filtri che rimuovono i messaggi dalla **casella della posta in arrivo**.

## 8.1. Selezione del livello di protezione della posta elettronica

Kaspersky Anti-Virus 6.0 for Windows Workstations protegge la posta elettronica a uno dei seguenti livelli (vedere Figura 24):

- Alto** – il livello con il monitoraggio più completo dei messaggi di posta sia in entrata che in uscita. Il programma esamina approfonditamente gli allegati di posta, inclusi gli archivi, indipendentemente dalla durata della scansione.

**Consigliato** – gli esperti di Kaspersky Lab raccomandano questo livello. A questo livello di protezione vengono esaminati gli stessi oggetti del livello **Alto**, con l'eccezione degli allegati o dei messaggi la cui scansione richieda più di 3 minuti.

**Basso** – livello di sicurezza che permette all'utente un agevole impiego di applicazioni che utilizzino intensamente le risorse della macchina, poiché la gamma dei file sottoposti a scansione è ridotta. In base a queste impostazioni, viene esaminata solo la posta in entrata, escludendo però gli archivi e gli oggetti (di posta) allegati la cui scansione richieda più di tre minuti. Questo livello è consigliato se nel computer sono installate altre applicazioni di protezione della posta elettronica.

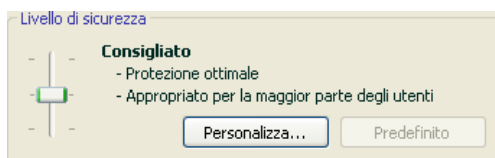


Figura 24. Selezione del livello di protezione della posta elettronica

Come impostazione predefinita, il livello di sicurezza della posta elettronica è impostato su **Consigliato**.

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

*Per modificare il livello di sicurezza:*

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

Se nessuno dei livelli preimpostati risulta soddisfacente, è possibile modificarne le impostazioni. In questo caso il livello diventa **Impostazioni personalizzate**. Ecco un esempio in cui un livello di sicurezza per la posta elettronica definito dall'utente può essere utile.

Esempio:

Il computer si trova all'esterno della LAN e si connette a Internet mediante una connessione di accesso remoto. Il client installato per ricevere e inviare la posta elettronica è Outlook Express e il servizio utilizzato è gratuito. Per svariate ragioni, la posta contiene allegati compressi. Come ottimizzare la protezione del computer dalle infezioni provenienti dalla posta elettronica?

### Suggerimento per la selezione di un livello:

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

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

*Per modificare le impostazioni del livello di sicurezza corrente:*

Fare clic sul pulsante **Personalizza** nella finestra delle impostazioni di iAnti-Virus posta. Modificare le impostazioni di protezione della posta nella finestra che si apre e fare clic su **OK**.

## 8.2. Configurazione di Anti-Virus posta

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

- Impostazioni che definiscono il gruppo di messaggi protetti (vedere 8.2.1 a pag. 110)
- Impostazioni di scansione della posta per Microsoft Outlook (vedere 8.2.2 a pag. 112) e The Bat! (vedere 8.2.3 a pag. 114)
- Impostazioni che definiscono le azioni da eseguire in caso di oggetti di posta pericolosi (vedere 8.2.4 a pag. 116)

Le seguenti sezioni esaminano in dettaglio queste impostazioni.


### 8.2.1. Selezione di un gruppo di messaggi di posta elettronica protetti

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

Per impostazione predefinita, il componente protegge la posta elettronica al livello di sicurezza **Consigliato**, esaminando cioè sia i messaggi in arrivo sia quelli in uscita. Quando si inizia a lavorare con il programma, si consiglia di analizzare la posta in uscita, in quanto è possibile che sul computer si trovino dei

worm che utilizzano la posta come canale per diffondersi. Questo accorgimento eviterà la possibilità che il computer invii inavvertitamente mailing di massa con messaggi infetti.

Se l'utente è certo che i messaggi di posta elettronica che si stanno inviando non contengano oggetti pericolosi, è possibile disabilitare la scansione della posta in uscita. Per fare ciò:

1. Selezionare **Anti-Virus posta** nella finestra principale e andare alla finestra delle impostazioni del componente facendo clic su **Impostazioni**. Fare clic sul pulsante **Personalizza** nella finestra delle impostazioni di Anti-Virus posta.
2. Nella finestra **Impostazioni personalizzate: Anti-Virus posta** (vedere Figura 25), selezionare  **Solo posta in arrivo** nella sezione **Ambito**.

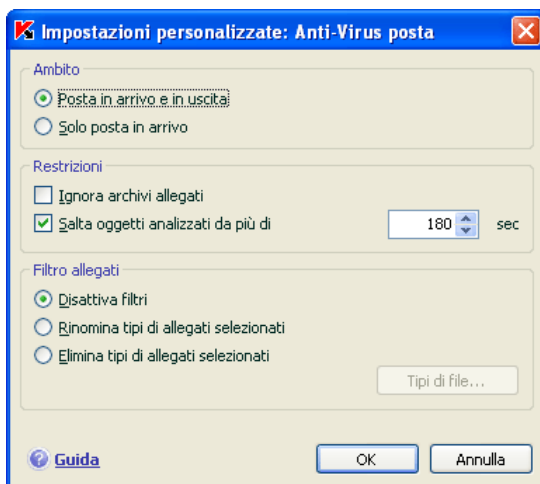


Figura 25. Anti-Virus posta, impostazioni

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

Se il computer non è protetto da alcun software di rete locale e se ci si collega a Internet senza un server proxy o un firewall, si consiglia di **non disabilitare** la scansione degli archivi allegati e di non impostare un tempo limite per la scansione.

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

È possibile configurare le condizioni di filtraggio per gli oggetti collegati a un messaggio di posta nella sezione **Filtro allegati**:

- Disattiva filtri** – Non applica ulteriori filtri per gli allegati.
- Rinomina tipi di allegati selezionati** – filtra un determinato formato di allegato e sostituisce l'ultimo carattere del nome del file con un trattino basso. Per selezionare il tipo di file, fare clic sul pulsante Tipi di file.
- Elimina tipi di allegati selezionati** – filtra ed elimina un determinato formato di allegato. Per selezionare il tipo di file, fare clic sul pulsante Tipi di file.

Per ulteriori informazioni sui tipi di allegati filtrati, consultare la sezione A.1 a pag. 327.

L'uso del filtro accresce ulteriormente la sicurezza per il computer, poiché nella maggior parte dei casi i programmi nocivi si diffondono tramite posta elettronica sotto forma di allegati. Rinominando o eliminando certi tipi di allegati, si protegge il computer dall'apertura automatica di allegati quando si riceve un messaggio.

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

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

Al momento dell'installazione di Kaspersky Anti-Virus for Windows Workstations, viene installato anche uno speciale plug-in per Outlook, in grado di accedere rapidamente alle impostazioni di Anti-Virus posta e di impostare l'ora di avvio della scansione antivirus dei singoli messaggi.

### Attenzione!

Questa versione di Kaspersky Anti-Virus non offre plug-in Anti-Virus posta per la versione a 64 bit di Microsoft Office Outlook.

Il plug-in si presenta sotto forma di una speciale scheda **Mail Anti-Virus** ubicata in **Strumenti** → **Opzioni** (vedere Figura 26).

Selezionare una modalità di scansione della posta:

- Scansione alla ricezione** – analizza ogni messaggio di posta nel momento in cui entra nella cassetta della posta in arrivo.
- Scansione alla lettura** – analizza ciascun messaggio nel momento in cui lo si apre per leggerlo.



- Scansione all'invio** – analizza alla ricerca di virus ogni messaggio di posta nel momento in cui lo si invia.

**Attenzione!**

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

L'azione che verrà intrapresa sugli oggetti di posta pericolosi viene stabilita nelle impostazioni di Anti-Virus posta, che può essere configurato seguendo il collegamento [fare clic qui](#) nella sezione **Stato**.

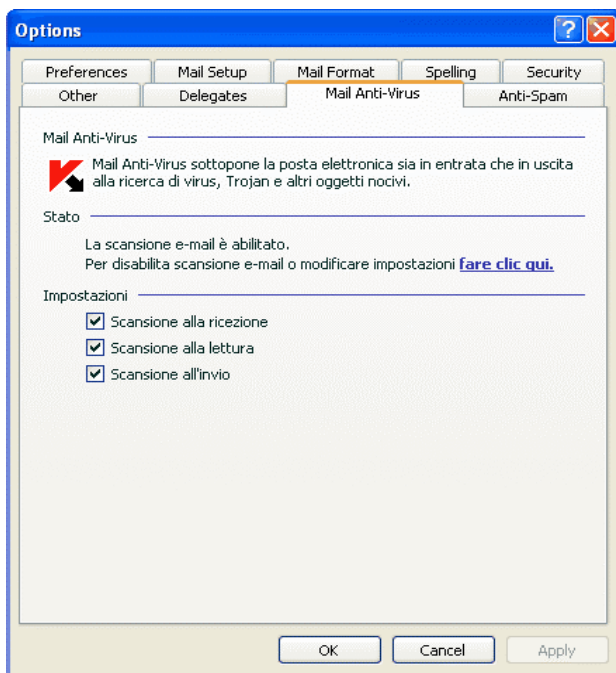


Figura 26. Configurazione delle impostazioni di Anti-Virus posta in Microsoft Outlook

### 8.2.3. Configurazione della scansione della posta in The Bat!

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

#### Attenzione!

Le impostazioni di Anti-Virus posta che determinano se esaminare i messaggi in arrivo e in uscita, nonché le azioni da eseguire sugli oggetti di posta pericolosi e le esclusioni, sono ignorate. Gli unici elementi di cui The Bat! tiene conto sono la scansione degli archivi allegati e le limitazioni temporali della scansione dei messaggi (vedere 8.2.1 a pag. 110).

Questa versione di Kaspersky Anti-Virus non offre plug-in Anti-Virus posta per la versione a 64 bit di The Bat!.

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

1. Selezionare **Settings (Impostazioni)** dal menu **Properties (Proprietà)** del client di posta.
2. Selezionare **Protection - Anti-virus** dalla struttura ad albero delle impostazioni.

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

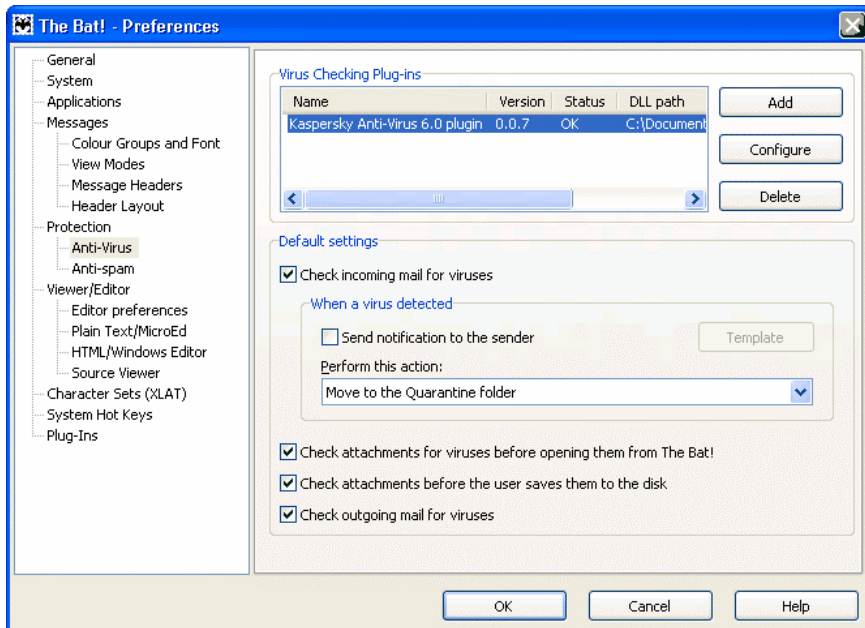


Figura 27. Configurazione della scansione della posta in The Bat!

A questo punto occorre stabilire:

- Quali gruppi di messaggi saranno sottoposti alla scansione antivirus (in arrivo, in uscita)
- In quale momento gli oggetti di posta saranno sottoposti alla scansione antivirus (all'apertura del messaggio o prima di salvarlo sul disco)
- Le azioni intraprese dal client di posta nel momento in cui nella posta sono rilevati oggetti pericolosi. Per esempio, è possibile selezionare:

**Tenta di disinfettare le parti infette** – cerca di trattare l'oggetto di posta infetto; se la disinfezione non riesce, l'oggetto resta nel messaggio. Kaspersky Anti-Virus for Windows Workstations informa sempre l'utente ogni volta che viene individuato un messaggio infetto. Ma anche selezionando **Elimina** nella finestra degli avvisi di Anti-Virus posta, l'oggetto rimane nel messaggio poiché l'azione selezionata in The Bat! ha la precedenza su quelle di Anti-Virus posta.

**Elimina parti infette** – elimina l'oggetto pericoloso nel messaggio, indipendentemente dal fatto che sia infetto o sospetto.

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

**Attenzione!**

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

## 8.2.4. Ripristino delle impostazioni predefinite di Anti-Virus posta

Durante la configurazione di Anti-Virus posta, è sempre possibile tornare alle impostazioni di lavoro predefinite, considerate da Kaspersky Lab come le migliori, e riunite nel livello di sicurezza **Consigliato**.

*Per ripristinare le impostazioni predefinite di Anti-Virus posta*

1. Selezionare **Anti-Virus posta** nella finestra principale e andare alla finestra delle impostazioni del componente facendo clic su Impostazioni.
2. Fare clic sul pulsante **Predefinito** nella sezione **Livello di sicurezza**.

## 8.2.5. Selezione di un'azione per gli oggetti di posta pericolosi

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

All'oggetto di posta in questione può venire assegnato uno dei seguenti stati, dopo la scansione:

- Status di programma nocivo (per esempio, *virus*, *troiano* – per ulteriori informazioni, vedere 1.1 a pag. 11).
- *Potenzialmente infetto*, quando la scansione non è in grado di determinare se l'oggetto è infetto. Ciò significa che il programma ha rilevato nel file una sequenza di codice proveniente da un virus sconosciuto, o modificato da un virus conosciuto.

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

Per modificare un'azione da applicare a un oggetto:

Aprire la finestra delle impostazioni di Kaspersky Anti-Virus for Windows Workstations e selezionare **Anti-Virus posta**. Tutte le possibili azioni per gli oggetti pericolosi sono elencate nella sezione **Azione** (vedere Figura 28).

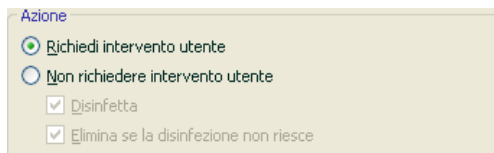


Figura 28. Selezione di un'azione per gli oggetti di posta pericolosi

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

| Se l'azione selezionata è  | Quando viene rilevato un oggetto pericoloso   |
|--|---|
| <input checked="" type="radio"/> <b>Richiedi intervento utente</b>       | Anti-Virus posta visualizza un messaggio di avvertenza contenente informazioni su quale programma nocivo ha infettato o potenzialmente infettato il file e consente di scegliere una delle seguenti azioni. |
| <input checked="" type="radio"/> <b>Non richiedere intervento utente</b> | Anti-Virus posta blocca l'accesso all'oggetto. Le informazioni relative all'evento vengono registrate nel rapporto (vedere 17.3 a pag. 243). In un secondo momento è possibile tentare di pulire l'oggetto. |

| Se l'azione selezionata è  | Quando viene rilevato un oggetto pericoloso  |
|--|--|
| <p><input checked="" type="radio"/> <b>Non richiedere intervento utente</b></p> <p><input checked="" type="checkbox"/> <b>Disinfetta</b></p>   | <p>Anti-Virus posta blocca l'accesso all'oggetto e cerca di disinfettarlo. Se la disinfezione ha esito positivo, il file viene ripristinato per l'uso. Se la disinfezione non è stata possibile, l'oggetto viene spostato in Quarantena (vedere 17.1 a pag. 237). Le informazioni relative all'evento vengono registrate nel rapporto. In un secondo tempo sarà possibile tentare di disinfettare l'oggetto.</p> |
| <p><input checked="" type="radio"/> <b>Non richiedere intervento utente</b></p> <p><input checked="" type="checkbox"/> <b>Disinfetta</b></p> <p><input checked="" type="checkbox"/> <b>Elimina se la disinfezione non riesce<sup>2</sup></b></p> | <p>Anti-Virus posta blocca l'accesso all'oggetto e cerca di disinfettarlo. Se la disinfezione ha esito positivo, il file viene ripristinato per l'uso. Se la disinfezione non riesce, l'oggetto viene eliminato. Una copia dell'oggetto viene memorizzata nella memoria di Backup.</p> <p>Gli oggetti con lo stato di potenzialmente infetti verranno spostati in quarantena.</p>                                |
| <p><input checked="" type="radio"/> <b>Non richiedere intervento utente</b></p> <p><input type="checkbox"/> <b>Disinfetta</b></p> <p><input checked="" type="checkbox"/> <b>Elimina</b></p>  | <p>Quando Anti-Virus posta rileva un oggetto infetto o potenzialmente infetto, lo elimina senza informare l'utente.</p>  |

Prima di disinfettare o eliminare l'oggetto, Kaspersky Anti-Virus for Windows Workstations ne crea una copia di backup (vedere 17.2 a pag. 241), qualora l'oggetto dovesse essere ripristinato o si presentasse la possibilità di trattarlo.

---

<sup>2</sup>Se il client in uso è The Bat!, gli oggetti di posta pericolosi vengono riparati o eliminati quando Mail Anti-Virus esegue questa azione (a seconda dell'azione selezionata in The Bat!).

---

## CAPITOLO 9. WEB ANTI-VIRUS


Ogni volta che si usa Internet, si espongono le informazioni custodite nel computer al rischio di infezione da parte di programmi pericolosi, i quali possono penetrare nel computer quando, ad esempio, si legge un articolo su Internet.

*Web Anti-Virus* è lo speciale componente di Kaspersky Anti-Virus dedicato alla protezione del computer durante la navigazione su Internet. Esso protegge le informazioni che entrano nel computer via HTTP e impedisce il caricamento di script pericolosi sul computer.

### Attenzione!

*Web Anti-Virus* controlla solo il traffico HTTP che passa attraverso le porte elencate nell'elenco delle porte monitorate (vedere 17.7 a pag. 264) Il pacchetto software comprende un elenco delle porte utilizzate più comunemente per trasmettere la posta elettronica e il traffico HTTP. Se si utilizzano porte non presenti in questo elenco è necessario aggiungerle al fine di proteggere il traffico che passa attraverso di esse.


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

L'attività del componente viene indicata dall'icona di Kaspersky Anti-Virus for Windows Workstations nell'area di notifica, che ha il seguente aspetto  ogniqualvolta vengono esaminati gli script.

Osserviamo in dettaglio il funzionamento del componente.

*Web Anti-Virus* è composto da due moduli che gestiscono:

- *Scansione traffico* – scansione degli oggetti che entrano nel computer mediante HTTP.
- *Scansione degli script* – esamina tutti gli script elaborati in Microsoft Internet Explorer, come anche tutti gli script WSH (JavaScript, Visual Basic Script, ecc) che vengono caricati mentre l'utente è al computer.

Al momento dell'installazione di Kaspersky Anti-Virus for Windows Workstations, viene installato uno speciale plug-in per Microsoft Internet Explorer. L'icona  nella barra degli strumenti standard del browser significa che esso è installato. Facendo clic sull'icona, si apre una finestra informativa contenente le statistiche di *Web Anti-Virus* sul numero di script esaminati e bloccati.

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

1. Ogni pagina web o file accessibile all'utente o a un determinato programma via HTTP viene intercettata e analizzata da Web Anti-Virus per escludere la presenza di codici nocivi. Gli oggetti nocivi vengono individuati per mezzo sia degli elenchi delle minacce inclusi in Kaspersky Anti-Virus che tramite l'algoritmo euristico. Gli elenchi contengono le descrizioni di tutti i programmi nocivi noti e dei metodi per neutralizzarli. L'algoritmo euristico è in grado di rilevare nuovi virus non ancora inseriti negli elenchi.
2. Dopo l'analisi è possibile agire come segue:
  - a. Se la pagina Web o l'oggetto contengono codice nocivo, il programma blocca l'accesso ad esso e viene visualizzato un messaggio sullo schermo secondo il quale l'oggetto o la pagina sono infetti.
  - b. Se il file o la pagina web non contengono codici nocivi, il programma concede immediatamente l'accesso al browser Web.

Gli script vengono esaminati secondo il seguente algoritmo:

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

#### Avviso

Web Anti – Virus deve essere abilitato prima di stabilire la connessione Web - sorgente per poter intercettare e controllare il traffico e gli script http e verificare che non contengano virus.

## 9.1. Selezione del livello di protezione web

Kaspersky Anti-Virus for Windows Workstations protegge il computer durante l'uso di Internet a uno dei seguenti livelli (vedere Figura 29):

**Alto** – il livello con il monitoraggio più completo degli script e degli oggetti in entrata via HTTP. Il programma esegue un'accurata scansione di tutti gli oggetti utilizzando l'intero elenco delle minacce. Questo livello di



sicurezza è raccomandato per ambienti aggressivi, quando non sono utilizzati altri strumenti di protezione del traffico HTTP.

**Consigliato** – le impostazioni di questo livello sono quelle raccomandate dagli esperti di Kaspersky Lab. Questo livello esamina gli stessi oggetti presi in considerazione dal livello **Alto**, ma applica una limitazione del tempo di caching per i frammenti di file, accelerando la scansione e rendendo disponibili gli oggetti più rapidamente.

**Basso** – livello di protezione le cui impostazioni consentono di utilizzare applicazioni che assorbono risorse considerevoli, grazie alla restrizione dell'ambito della scansione ottenuta utilizzando un elenco di minacce limitato. Si raccomanda di selezionare questo livello di protezione se di dispone di un ulteriore software di protezione web installato sul computer.

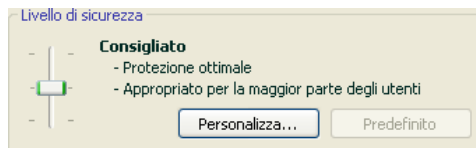


Figura 29. Selezione di un livello di protezione web

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

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

*Per modificare il livello di sicurezza:*

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

Se un livello preimpostato non soddisfa i requisiti dell'utente, è possibile creare un livello di sicurezza con **Impostazioni personalizzate**. Osserviamo un esempio in cui la creazione di un livello personalizzato risulta utile.

Esempio:

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

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

Come proteggere al meglio il computer dalle infezioni penetrate attraverso il traffico HTTP o uno script?

### Suggerimento per la selezione di un livello:

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

Il livello di protezione consigliato è quindi **Alto**, apportando le seguenti modifiche: si consiglia di ridurre il tempo di caching dei frammenti di file durante la scansione.

*Per modificare un livello di protezione predefinito:*

fare clic sul pulsante **Personalizza** nella finestra delle impostazioni di Web Anti-Virus. Modificare le impostazioni di protezione web (vedere 9.2 a pag. 122) nella finestra che si apre e fare clic sul pulsante **OK**.

## 9.2. Configurazione di Web Anti-Virus

Web Anti-Virus prevede la scansione di tutti gli oggetti caricati sul computer tramite il protocollo HTTP e monitora l'esecuzione di tutti gli script WHS (JavaScript, Visual Basic Script, ecc.).

Per accelerare la velocità di Web Anti-Virus è possibile configurarne alcune impostazioni, in particolare:

- Impostare l'algoritmo di scansione selezionando un set di elenchi di minacce completo o ridotto.
- Creazione di un elenco degli indirizzi Web attendibili.

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

Le seguenti sezioni esaminano in dettaglio queste impostazioni.

### 9.2.1. Impostazione di un metodo di scansione

I dati provenienti da Internet possono essere esaminati con uno dei seguenti algoritmi:

- *Scansione di flussi* – questo metodo di rilevamento dei codici nocivi nel traffico di rete esamina i dati al volo: mentre si sta scaricando un file da Internet, Web Anti-Virus esamina le parti del file mentre vengono

scaricate, il che consente di mettere il file a disposizione dell'utente più rapidamente. Per contro, la scansione dei flussi viene eseguita con un elenco delle minacce ridotto (che prende in considerazione solo le minacce più attive), il che diminuisce notevolmente il livello di sicurezza durante l'uso di Internet.

- *Scansione di buffer*- questo metodo esamina gli oggetti solo dopo che sono stati scaricati completamente nel buffer. Una volta completata la scansione, il programma passa l'oggetto all'utente o lo blocca. Con questo tipo di scansione, si utilizza l'elenco dei virus completo, aumentando il livello di rilevamento di codici nocivi. Tuttavia, l'utilizzo di questo algoritmo aumenta il tempo di elaborazione dell'oggetto e quindi rallenta la navigazione sul Web. determina inoltre problemi quando si copiano o si elaborano oggetti di grandi dimensioni poiché la connessione col client HTTP può interrompersi.

*Per selezionare l'algoritmo di scansione utilizzato da Web Anti-Virus:*

1. Fare clic sul pulsante **Personalizza** nella finestra delle impostazioni di Web Anti-Virus.
2. Nella finestra che si apre (vedere Figura 30), selezionare l'opzione desiderata nella sezione **Metodo di scansione**.

Per impostazione predefinita, Web Anti-Virus esegue una scansione dei dati provenienti da Internet tramite buffer e utilizza l'elenco dei virus completo.

#### Attenzione!

In caso di problemi di accesso a risorse quali radio Internet, video streaming o Internet conferencing, utilizzare la scansione del flusso.

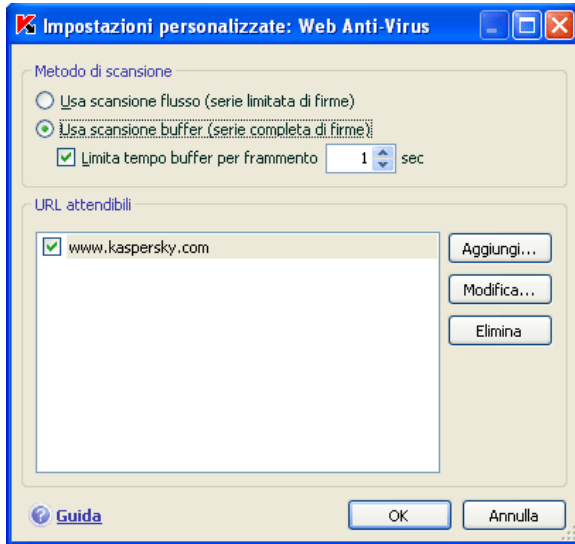


Figura 30. Configurazione di Web Anti-Virus

## 9.2.2. Creazione di un elenco di indirizzi attendibili

È possibile creare un elenco di indirizzi i cui contenuti sono ritenuti attendibili. Web Anti-Virus non analizzerà i dati provenienti da quegli indirizzi. Questa funzione può essere utilizzata nei casi in cui Web Anti-Virus ostacola il download di un file specifico, bloccando i tentativi di scaricarlo.

*Per creare un elenco degli indirizzi attendibili:*

1. Fare clic sul pulsante **Personalizza** nella finestra delle impostazioni di Web Anti-Virus.
2. Nella finestra che si apre (vedere Figura 30), creare una lista dei server attendibili nella sezione **URL attendibili**. A questo scopo utilizzare i pulsanti alla destra dell'elenco.

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

\* - qualsiasi combinazione di caratteri.

Esempio: Creando la maschera **\*abc\***, gli URL contenenti **abc** non saranno esaminati. Per esempio:

[www.virus.com/download\\_virus/page\\_0-9abcdef.html](http://www.virus.com/download_virus/page_0-9abcdef.html)

? – qualsiasi singolo carattere.

Esempio: Creando la maschera **Patch\_123?.com**, gli URL contenenti quella serie di caratteri più qualsiasi singolo carattere che segue il 3 non saranno esaminati. Per esempio: **Patch\_12345.com** Tuttavia, **patch\_12345.com** sarà esaminato.

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

Esempio: Si desidera aggiungere questa URL all'elenco degli indirizzi attendibili: [www.virus.com/download\\_virus/virus.dll?virus\\_name=](http://www.virus.com/download_virus/virus.dll?virus_name=)

Per evitare che Kaspersky Anti-Virus consideri il ? come un carattere jolly, è necessario farlo precedere da una barra inversa ( \ ). Di conseguenza, l'URL aggiunto all'elenco delle esclusioni sarà come segue:

[www.virus.com/download\\_virus/virus.dll?virus\\_name=](http://www.virus.com/download_virus/virus.dll?virus_name=)

### 9.2.3. Ripristino delle impostazioni di Web Anti-Virus

Durante la configurazione di Web Anti-Virus, è sempre possibile tornare alle impostazioni di lavoro predefinite, considerate da Kaspersky Lab come le migliori, e riunite nel livello di sicurezza **Consigliato**.

*Per ripristinare le impostazioni predefinite di Web Anti-Virus:*

1. Selezionare **Web Anti-Virus** nella finestra principale e andare alla finestra delle impostazioni del componente facendo clic su Impostazioni.
2. Fare clic sul pulsante **Predefinito** nella sezione **Livello di sicurezza**.

### 9.2.4. Selezione delle reazioni agli oggetti pericolosi

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

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

Aprire la finestra delle impostazioni di Kaspersky Anti-Virus for Windows Workstations e selezionare **Web Anti-Virus**. Tutte le possibili reazioni per

gli oggetti pericolosi sono elencate nella sezione **Azione** (vedere Figura 31).

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

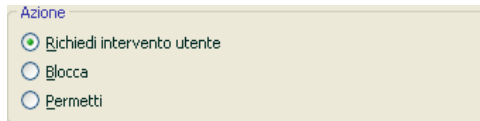


Figura 31. Selezione di azioni da eseguire su script pericolosi

Le azioni selezionabili per l'elaborazione degli oggetti HTTP pericolosi sono le seguenti.

| Se l'azione selezionata è  | Se viene intercettato un oggetto pericoloso nel traffico HTTP   |
|--|---|
| <input checked="" type="radio"/> <b>Richiedi intervento utente</b> | Web Anti-Virus visualizza un messaggio di avviso contenente informazioni sul codice nocivo che potrebbe aver infettato l'oggetto e offre una serie di reazioni possibili.   |
| <input type="radio"/> <b>Blocca</b>                                | Web Anti-Virus blocca l'accesso all'oggetto e visualizza un avviso in merito. Le informazioni relative all'evento vengono registrate nel rapporto (vedere 17.3 a pag. 243). |
| <input type="radio"/> <b>Permetti</b>                              | Web Anti-Virus consente l'accesso all'oggetto. Queste informazioni vengono registrate nel rapporto.   |

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

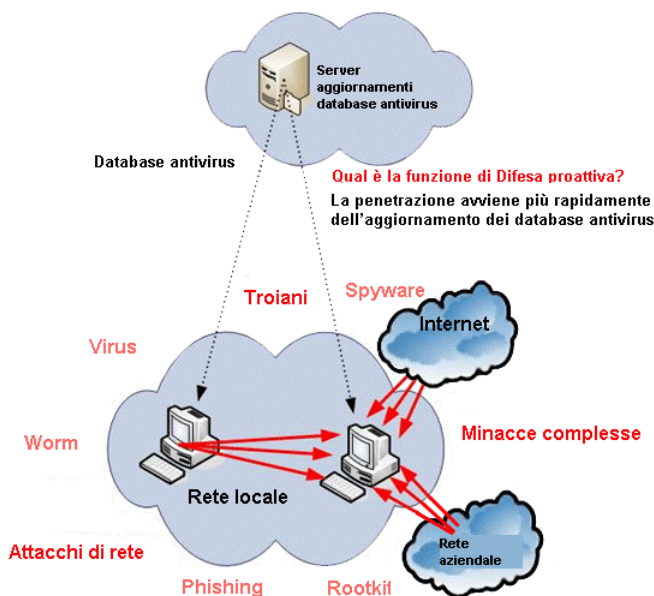
---

# CAPITOLO 10. DIFESA PROATTIVA

## Attenzione!

Questa versione dell'applicazione non comprende il componente di Difesa proattiva **Office Guard** per computer che eseguono Microsoft Windows XP Professional x64 Edition, Vista, o Microsoft Windows Vista x64.

Kaspersky Anti-Virus for Windows Workstations protegge sia dalle minacce note sia da quelle sulle quali non si possiedono ancora informazioni negli appositi elenchi delle minacce. Questa funzione è garantita da un componente specifico – *Difesa proattiva*.



La necessità di un componente come Difesa proattiva si è fatta più pressante man mano che i programmi nocivi hanno iniziato a diffondersi più rapidamente degli aggiornamenti antivirus necessari per neutralizzarli.

La tecnica di reazione sulla quale si basa la protezione antivirus richiede che almeno un computer sia infettato dalla nuova minaccia e comporta il dispendio

temporale necessario per analizzare il codice nocivo e aggiungerlo agli elenchi delle minacce, quindi l'aggiornamento del database sui computer degli utenti. Entro quel lasso di tempo, il nuovo virus potrebbe aver provocato pesanti danni.

Le tecnologie preventive fornite da Difesa proattiva di Kaspersky Anti-Virus for Windows Workstations sono in grado di evitare le perdite di tempo della tecnica reattiva e neutralizzare le nuove minacce prima che possano danneggiare il computer. In che modo? Contrariamente alle tecnologie reattive che analizzano i codici tramite le firme delle minacce, le tecnologie preventive riconoscono una nuova minaccia nel computer in base alle sequenze di azioni eseguite da una determinata applicazione. Il programma include una serie di criteri in grado di identificare il livello di pericolosità delle attività dei vari programmi. Se l'analisi dell'attività di un programma desta sospetti, Kaspersky Anti-Virus esegue l'azione assegnata dalla regola per quel tipo di attività.

Le attività pericolose vengono classificate in base all'insieme totale di azioni del programma. Ad esempio, quando viene individuato un programma che compie azioni come ricopiarsi sulle risorse di rete, la cartella di avvio o il registro di sistema per poi inviare copie di sé stesso, è molto probabile che si tratti di un worm. I comportamenti pericolosi comprendono inoltre:

- Le modifiche al file system
- Moduli che vengono incorporati in altri processi
- Il mascheramento di processi nel sistema
- La modifica di certe chiavi del registro di sistema di Microsoft Windows

Difesa Proattiva rileva e blocca tutte le operazioni pericolose utilizzando un insieme di regole unitamente ad un elenco di applicazioni escluse. Inoltre, individua tutte le macro eseguite nelle applicazioni di Microsoft Office.

Difesa proattiva utilizza una serie di regole incluse nell'applicazione, oppure create dall'utente durante l'utilizzo della stessa. Una *regola* è una serie di criteri che definiscono i comportamenti sospetti nonché la reazione di Kaspersky Anti-Virus ad essi.

Regole individuali sono fornite per l'attività delle applicazioni e per monitorare le modifiche al registro di sistema, alle macro e ai programmi eseguiti sul computer. È possibile modificare le regole a discrezione dell'utente aggiungendone, oppure eliminando e modificando quelle esistenti. Le regole possono bloccare azioni o concedere autorizzazioni.

Esaminiamo gli algoritmi di Difesa proattiva:

1. Immediatamente dopo l'avvio del computer, Difesa proattiva analizza i seguenti fattori, utilizzando l'insieme di regole ed esclusioni:
  - *Azioni di ogni applicazione che viene eseguita sul computer.* Difesa proattiva registra una cronologia delle azioni eseguite in



sequenza e la confronta alle sequenze caratteristiche delle attività pericolose (con il programma è fornito un database dei tipi di attività pericolose che viene aggiornato con gli elenchi dei virus).

- *Le azioni di ogni macro VBA eseguita* vengono analizzate alla ricerca di attività nocive.
  - *Ogni tentativo di modificare il registro di sistema* eliminando o aggiungendo chiavi di registro di sistema, assegnando strani valori alle chiavi, ecc.
2. L'analisi viene eseguita in base alle regole *Permetti* (secondo i relativi criteri, il comportamento non è nocivo) e *Termina* (secondo i relativi criteri, il comportamento è nocivo) di Difesa proattiva.
  3. Dopo l'analisi, sono possibili le seguenti linee di azione:
    - Se l'attività non è considerata pericolosa in base ai relativi criteri (*Permetti* e *Termina*), viene consentita.
    - Se l'attività è considerata pericolosa in base ai relativi criteri, le azioni successive eseguite dal componente corrisponderanno alle istruzioni specificate nella regola: solitamente l'attività viene bloccata. Sul video viene visualizzato un messaggio che specifica il programma nocivo, il suo tipo di attività e una cronologia delle azioni eseguite. L'utente deve accettare la decisione, bloccare o consentire questa attività. È possibile inoltre creare una regola per l'attività e annullare le azioni eseguite sul sistema.

## 10.1. Impostazioni di Difesa proattiva

Le categorie di impostazioni (vedere Figura 32) per il componente Difesa proattiva sono le seguenti:

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

Questa funzione di Difesa proattiva viene abilitata selezionando la casella  **Abilita analisi attività applicazione**. Per impostazione predefinita questa modalità è abilitata, garantendo un attento monitoraggio delle azioni di qualsiasi programma aperto sul computer. Viene evidenziata una serie di attività pericolose per ognuna delle quali è possibile configurare la procedura di elaborazione dell'applicazione (vedere 10.1.1 a pag. 131). Inoltre è possibile creare esclusioni di Difesa proattiva, che escludono dal monitoraggio l'attività delle applicazioni selezionate.

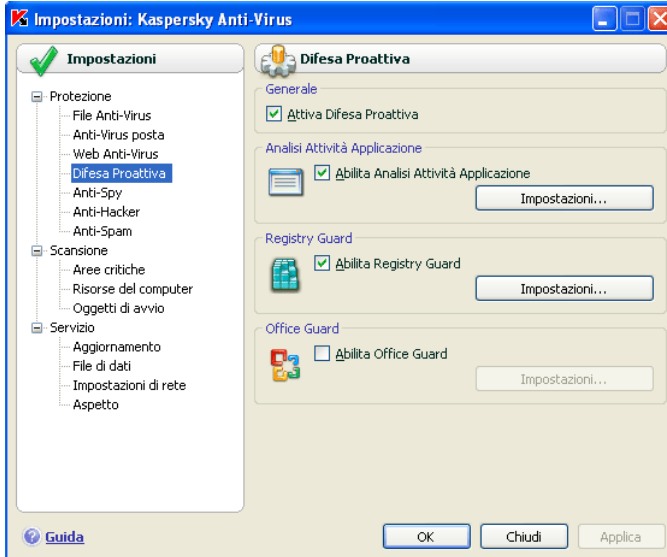


Figura 32. Impostazioni di Difesa proattiva

- Se le variazioni ai registri di sistema vengono monitorate

Come impostazione predefinita, la casella  **Abilita Registry Guard** è selezionata, il che significa che Kaspersky Anti-Virus for Windows Workstations analizza tutti i tentativi di apportare modifiche alle chiavi del registro di sistema di Windows.

È possibile creare regole di monitoraggio personalizzate (vedere 10.1.3.2 a pag. 139) delle chiavi di registro, in base alla chiave di registro di Microsoft Windows.

- Se le macro vengono esaminate

Il monitoraggio delle macro di Visual Basic for Applications sul computer è controllato selezionando la casella  **Abilita Office Guard**, selezionata per impostazione predefinita.

È possibile specificare quali macro considerare pericolose e quali azioni eseguire (vedere 10.1.2 a pag. 135).

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

È possibile inoltre configurare esclusioni (vedere 6.3.1 a pag. 79) per i moduli di Difesa proattiva e creare un elenco delle applicazioni attendibili (vedere 6.3.2 a pag. 84).

Le seguenti sezioni esaminano in maggiore dettaglio questi aspetti.

## 10.1.1. Regole di controllo delle attività

Si noti che il processo di configurazione del controllo delle applicazioni in Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, o Microsoft Windows Vista x64 è diverso rispetto a quello di altri sistemi operativi. Le informazioni sulla configurazione del controllo delle attività per questi sistemi operativi sono fornite alla fine di questa sezione.

Kaspersky Anti-Virus controlla le attività di tutte le applicazioni sul computer. L'applicazione comprende un insieme di descrizioni di eventi che possono essere identificati come pericolosi. Per ciascuno di tali eventi viene creata una regola di monitoraggio. Se l'attività di qualsiasi applicazione è classificata come evento pericoloso, Difesa proattiva applica rigorosamente le istruzioni specificate dalla regola per quel tipo di attività.

Selezionare la casella di controllo  **Abilita analisi attività applicazione** se si desidera monitorare l'attività delle applicazioni.

Analizziamo ora diversi tipi di eventi che si verificano nel sistema che verranno identificati dall'applicazione come pericolosi:

- *Comportamento pericoloso.* Kaspersky Anti-Virus analizza l'attività delle applicazioni installate sul computer, e rileva le azioni pericolose o sospette da parte dei programmi in base alle regole create da Kaspersky Lab. Tali azioni includono, per esempio, l'installazione dissimulata di un programma, o i programmi che si replicano.
- *Avvio del browser Internet con parametri.* Analizzando questo tipo di attività, è possibile rilevare i tentativi di apertura del browser Web con parametri. Questa attività è tipica dell'apertura di un browser Web da parte di un'applicazione con impostazioni specifiche da riga di comando. Per esempio, questo avviene se si fa clic sul collegamento ad un certo URL in un messaggio e-mail pubblicitario.
- *Intrusione nel processo (invasori)* – consiste nell'aggiungere codice eseguibile o creare un flusso supplementare al processo di un certo programma. Questa attività è tipica dei trojan.
- *Processi nascosti (rootkit).* I rootkit sono un insieme di programmi utilizzati per nascondere i programmi nocivi ed i loro processi nel sistema.

Kaspersky Anti-Virus analizza il sistema operativo alla ricerca di processi nascosti.

- *Hook della finestra.* È un'attività utilizzata nei tentativi di lettura di password ed altre informazioni riservate visualizzate nelle finestre di dialogo del sistema operativo. Kaspersky Anti-Virus identifica tali attività, in caso di tentativi di intercettare i dati trasferiti dal sistema operativo alla finestra di dialogo.
- *Valori sospetti nel registro.* Il registro di sistema è un database che conserva le impostazioni di sistema e dell'utente per controllare il funzionamento di Windows, come anche qualsiasi utility presente sul computer. I programmi nocivi, cercando di nascondere la loro presenza nel sistema, copiano valori errati nelle chiavi di registro. Kaspersky Anti-Virus analizza le voci del registro di sistema alla ricerca di valori sospetti.
- *Attività di sistema sospetta.* Il programma analizza le azioni eseguite da Microsoft Windows e rileva le attività sospette. Un esempio di attività sospetta può essere una violazione di integrità, che implica la modifica di uno o più moduli in un'applicazione monitorata rispetto all'ultima volta in cui è stata eseguita.
- *Rilevamento keylogger.* È un'attività utilizzata dai programmi nocivi per tentare di leggere password ed altre informazioni riservate digitate per mezzo della tastiera.
- *Protezione di Microsoft Windows Task Manager.* Kaspersky Anti-Virus protegge Task Manager dai moduli nocivi che s'iniettano al suo interno allo scopo di bloccarne il funzionamento.

La lista delle attività pericolose può essere estesa automaticamente durante l'aggiornamento di Kaspersky Anti-Virus for Windows Workstations, ma non può essere modificata dall'utente. Le opzioni disponibili sono:

- Disattivare il monitoraggio di un'attività deselegzionando la casella  accanto al suo nome
- Modificare la regola usata da Difesa proattiva quando rileva un'attività pericolosa
- Creare un elenco di esclusioni (vedere 6.3 a pag. 78) includendovi le applicazioni con attività che non si considerano pericolose

*Per configurare il monitoraggio delle attività,*

1. Aprire la finestra delle impostazioni di Kaspersky Anti-Virus for Windows Workstations facendo clic su Impostazioni nella finestra principale del programma.
2. Selezionare **Difesa proattiva** nella struttura ad albero delle impostazioni.

### 3. Fare clic sul pulsante **Impostazioni** nella sezione **Abilita analisi attività applicazione**.

I tipi di attività monitorati da Difesa proattiva sono elencati nella finestra **Impostazioni: Analisi attività applicazione** (vedere Figura 33).

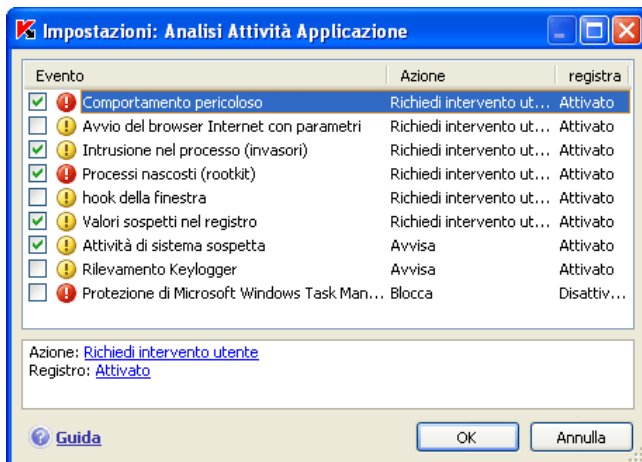


Figura 33. Configurazione del controllo delle attività delle applicazioni

Per modificare un'attività pericolosa, selezionarla dall'elenco e assegnare le impostazioni della regola nella parte inferiore della scheda:

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

Come reazione è possibile assegnare qualsiasi azione tra quelle elencate di seguito: [Permetti](#), [Richiedi intervento utente](#), e [Termina](#). Fare clic con il pulsante sinistro del mouse sul collegamento dell'azione fino a visualizzare quella desiderata. Oltre a terminare il processo, è possibile mettere in quarantena l'applicazione che ha avviato l'attività pericolosa. A tal fine, usare il collegamento [En. Dis.](#) dall'impostazione appropriata. È possibile assegnare un intervallo temporale per quanto riguarda la frequenza di esecuzione della scansione di processi nascosti nel sistema.

- Stabilire se si desidera generare un rapporto sull'operazione eseguita, A tal fine, fare clic sul collegamento accanto a **Registro** finché non visualizza [Attivato](#) o [Disattivato](#) secondo necessità.

Per disattivare il monitoraggio di un'attività pericolosa, deselezionare  accanto al nome delle attività nell'elenco.

### Specifiche di configurazione del controllo dell'attività delle applicazioni di Kaspersky Anti-Virus in Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista o Microsoft Windows Vista x64:

Se si sta utilizzando uno dei sistemi operativi elencati sopra, solo un tipo di evento di sistema viene controllato, *comportamento pericoloso*. Kaspersky Anti-Virus for Windows Workstations analizza l'attività delle applicazioni installate sul computer, e ne rileva le azioni pericolose o sospette in base all'elenco di regole create dagli esperti di Kaspersky Lab.

Se si desidera che Kaspersky Anti-Virus controlli l'attività dei processi di sistema oltre a quelli dell'utente, selezionare la casella di controllo  **Controllo account utenti** (vedere Figura 34). La casella è deselezionata per impostazione predefinita.

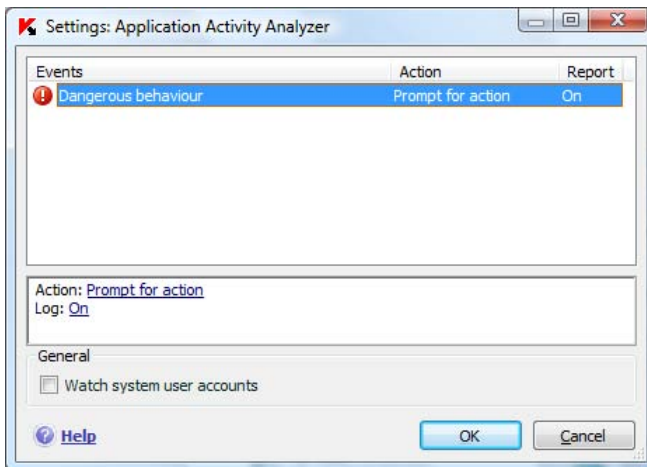


Figura 34. Configurazione del controllo dell'attività delle applicazioni in Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64.

Gli account utente controllano l'accesso al sistema ed identificano l'utente ed il suo ambiente di lavoro, impedendo agli altri utenti di danneggiare il sistema operativo o i dati. I processi di sistema sono processi lanciati dai dagli account utente del sistema.

## 10.1.2. Office Guard

Questo componente di Difesa proattiva non funziona in Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, o Microsoft Windows Vista x64.

È possibile abilitare la scansione e l'elaborazione delle macro pericolose sul computer selezionando  **Abilita Office Guard**. Ogni macro eseguita viene esaminata e, se presente nell'elenco delle macro pericolose, viene elaborata.

### Esempio:

La macro *PDFMaker* è un plug-in della barra degli strumenti di Adobe Acrobat in Microsoft Office Word che consente di creare un file .pdf da qualsiasi documento. Difesa proattiva classifica l'incorporazione di elementi nel software come azioni pericolose. Se Office Guard è abilitato, durante il caricamento di una macro Difesa proattiva visualizza sullo schermo un messaggio che informa che è stato individuato un comando macro pericoloso. Si può scegliere di interrompere la macro o lasciarla continuare.

È possibile configurare quali azioni devono essere eseguite dal programma quando ci sono macro che eseguono azioni sospette. Se l'utente è certo che questa macro non sia pericolosa quando lavora con un file specifico, ad esempio un documento di MS Word, si consiglia di creare un'esclusione. Se si verifica una situazione che corrisponde ai termini della regola di esclusione, l'azione sospetta eseguita dalla macro non viene elaborata da Difesa Proattiva.

### *Per configurare Office Guard:*

1. Aprire la finestra delle impostazioni di Kaspersky Anti-Virus for Windows Workstations facendo clic su Impostazioni nella finestra principale del programma.
2. Selezionare **Difesa proattiva** nella struttura ad albero delle impostazioni.
3. Fare clic sul pulsante **Impostazioni** nel riquadro **Office Guard**.

Le regole di elaborazione delle macro pericolose vengono configurate nella finestra **Impostazioni: Office Guard**, (vedere Figura 35) che contiene le regole predefinite per i comportamenti che Kaspersky Lab classifica come pericolosi, e le reazioni impostate per Difesa Proattiva. Le azioni delle macro pericolose includono, per esempio, l'incorporazione di moduli all'interno di programmi e l'eliminazione di file.

Se non si considera pericoloso un comportamento presente nell'elenco, deselegionare la casella accanto al nome dell'azione. Per esempio, l'utente

potrebbe lavorare spesso con un programma che usa le macro per aprire i file (non in sola lettura) ed è certo che questa operazione non è nociva.



Figura 35. Configurazione delle impostazioni di Office Guard

*Per fare in modo che Kaspersky Anti-Virus for Windows Workstations non blocchi la macro:*

deselezionare la casella a fianco dell'azione. Il programma non considererà più quel comportamento come pericoloso e Difesa Proattiva non l'elaborerà.

Come impostazione predefinita, ogni qualvolta il programma rileva un'azione avviata da una macro sul computer, chiede all'utente se desidera eseguirla o bloccarla.

*Per far sì che il programma blocchi automaticamente tutti i comportamenti pericolosi senza interrogare l'utente:*

Nella finestra dell'elenco delle macro, selezionare  **Termina**.

### 10.1.3. Registry Guard

Uno degli obiettivi di molti programmi nocivi è quello di modificare il registro di sistema di Windows nel computer. Questo obiettivo può essere raggiunto attraverso innocui joke o tramite programmi nocivi più pericolosi che rappresentano una reale minaccia per il computer.



Per esempio, i programmi nocivi possono copiare le proprie informazioni sulle chiavi di registro che determinano l'apertura automatica delle applicazioni all'avvio. I programmi nocivi verranno allora avviati automaticamente all'avvio del sistema operativo.

*Per configurare il monitoraggio del registro di sistema:*

1. Aprire la finestra delle impostazioni di Kaspersky Anti-Virus for Windows Workstations facendo clic su Impostazioni nella finestra principale del programma.
2. Selezionare **Difesa proattiva** nella struttura ad albero delle impostazioni.
3. Fare clic sul pulsante **Impostazioni** nella sezione **Registry Guard**.

Kaspersky Lab ha creato un elenco di regole per controllare le operazioni relative sul file del registro e lo ha incluso nel programma. Le operazioni che implicano file del registro sono classificate in gruppi logici come *System security*, *Internet Security*, ecc. Ciascuno di questi sottogruppi elenca i file del registro di sistema e regole per lavorare con essi. Questo elenco viene aggiornato quando si aggiorna il resto dell'applicazione.

La finestra **Impostazioni: Registry Guard** (vedere Figura 36) visualizza l'elenco completo delle regole.

Ogni gruppo di regole ha una priorità di esecuzione che è possibile aumentare o diminuire utilizzando i pulsanti **Sposta su** e **Sposta giù**. Più in alto si trova il gruppo, maggiore è la priorità ad esso assegnata. Se lo stesso file del registro è presente in più gruppi, la prima regola applicata ad esso è quella del gruppo con la priorità più elevata.

Per smettere di usare qualsiasi gruppo di regole agire come segue:

- Deselezionare la casella  accanto al nome del gruppo. In questo modo, il gruppo di regole rimane nell'elenco ma non sarà utilizzato.
- Eliminare il gruppo di regole dall'elenco. Si sconsiglia di eliminare i gruppi creati da Kaspersky Lab poiché contengono un elenco di file del registro di sistema utilizzati più frequentemente dai programmi nocivi.

È possibile creare i propri gruppi di file del registro di sistema monitorati. A tal fine, fare clic su **Aggiungi** nella finestra del gruppo di file.

Nella finestra che si apre eseguire questi passaggi:

1. Immettere il nome del nuovo gruppo di regole per il monitoraggio dei file del registro di sistema nel campo **Nome gruppo**.
2. Selezionare la scheda **Chiavi**, e creare un elenco di file del registro che verranno inclusi nel gruppo monitorato (vedere 10.1.3.1 a pag. 138) per il quale si desidera creare delle regole. Può trattarsi di una o più chiavi.

3. Selezionare la scheda **Regole**, e creare una regola per i file (vedere 10.1.3.2 a pag. 139) che si applichi alle chiavi selezionate nella scheda Chiavi. È possibile creare diverse regole e impostarne l'ordine di applicazione.



Figura 36. Gruppi chiavi di registro controllati

### 10.1.3.1. Selezione delle chiavi di registro per creare una regola

Il gruppo di file creato deve contenere almeno un file del registro di sistema. La scheda **Chiavi** visualizza l'elenco di file ai quali applicare le diverse regole.

*Per aggiungere un file di registro del sistema:*

1. Fare clic sul pulsante **Aggiungi** nella finestra **Modifica gruppo** (vedere Figura 37).
2. Nella finestra che si apre, selezionare il file del registro (o la cartella di file), per il quale si desidera creare una regola.
3. Specificare il valore dell'oggetto o la maschera per un gruppo di oggetti, al quale si intende applicare la regola nel campo **Valore**.
4. Selezionare  **Includi sottochiavi** per applicare la regola a tutte i file allegati al file del registro di sistema selezionato per la regola.

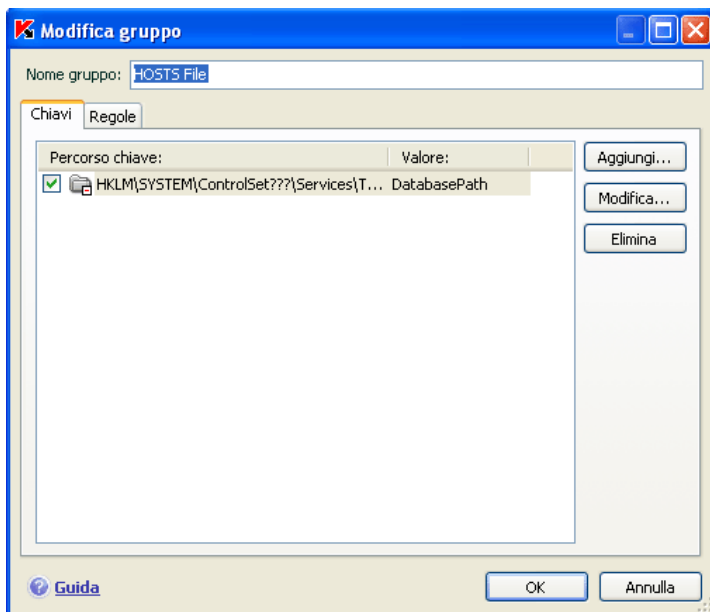


Figura 37. Aggiunta di chiavi di registro controllate

Se per il nome della chiave sono stati utilizzati caratteri jolly, sono necessarie solo le maschere con un asterisco e un punto interrogativo unitamente alla funzione  **Includi sottochiavi**.

Se si seleziona una cartella di file di registro utilizzando una maschera e si specifica un valore per tale gruppo, la regola sarà applicata a quel valore per qualsiasi chiave appartenente al gruppo selezionato.

### 10.1.3.2. Creazione di una regola per Registry Guard

Una regola di Registry Guard specifica:

- Il programma il cui accesso al registro di sistema viene monitorato
- la reazione di Difesa Proattiva ad un'applicazione che tenta di eseguire un'operazione con un file del registro di sistema

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

1. Fare clic su **Nuovo** sulla scheda **Regole**. La nuova regola viene aggiunta in cima all'elenco (vedere Figura 38).
2. Selezionare una regola dall'elenco e assegnare le impostazioni della regola sulla parte inferiore della scheda:
  - Specificare l'applicazione.

La regola viene creata per qualsiasi applicazione per impostazione predefinita. Se si desidera applicare la regola a una specifica applicazione, fare clic con il tasto sinistro del mouse su qualsiasi e questo valore si modificherà in selezionata. Quindi fare clic sul collegamento specificare nome applicazione. Si aprirà un menu di scelta rapida: fare clic su **Sfoggia** per visualizzare la finestra standard di selezione file, oppure fare clic su **Applicazioni** per visualizzare un elenco di applicazioni aperte e selezionarne una secondo necessità.

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

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

- Stabilire se si desidera generare un rapporto sull'operazione eseguita, facendo clic su registra / non registrare.

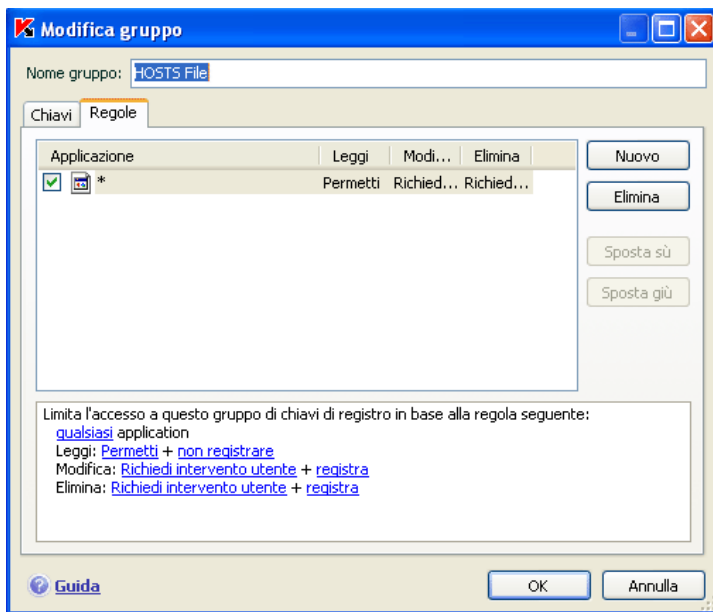


Figura 38. Creazione di una regola di monitoraggio delle chiavi di registro

È possibile creare diverse regole e modificarne la priorità per mezzo dei pulsanti **Sposta su** e **Sposta giù**. Più in alto si trova la regola, maggiore è la priorità ad essa assegnata.

È possibile inoltre creare una regola di *autorizzazione* (vale a dire che tutte le azioni sono consentite) per un oggetto del registro del sistema dalla finestra di notifica che comunica che un programma sta cercando di eseguire un'operazione con la chiave. A tal fine, fare clic su Crea regola di autorizzazione nella finestra di notifica e specificare l'oggetto del registro di sistema al quale verrà applicata la regola nella finestra che si apre.

---

## CAPITOLO 11. ANTI-SPY

Il componente di Kaspersky Anti-Virus for Windows Workstations che protegge i file del computer da tutti i tipi di malware è *Anti-Spy*. Recentemente, il software nocivo include sempre più programmi che hanno lo scopo di:

- Impadronirsi di informazioni confidenziali, tra cui password, numeri di carte di credito, documenti importanti, ecc.
- Intercettare le operazioni dell'utente al computer e analizzare il software installato su di esso.
- Visualizzare contenuti pubblicitari importuni in browser, finestre popup e banner in vari programmi.
- Accedere a Internet senza autorizzazione da computer altrui e aprire vari siti web.

Il phishing e i keylogger sono programmati specificamente per impadronirsi di informazioni confidenziali; gli autodialer, i joke e gli adware possono provocare perdite di tempo e denaro. Anti-Spy è concepito appositamente per proteggere l'utente da questi programmi.

Anti-Spy comprende i seguenti moduli:

- Il componente *Anti-Phishing* protegge dall'attività di phishing.

Il phishing consiste solitamente di messaggi e-mail inviati da sedicenti istituzioni finanziarie, e contenenti collegamenti ai loro siti web. Il testo del messaggio convince l'utente a seguire un link e inserire i propri dati riservati in una pagina Web, per esempio il numero di carta di credito o il nome utente e la password per accedere a un vero sito di Internet banking.

Un esempio diffuso di phishing è una e-mail proveniente da una banca utilizzata dall'utente, con un collegamento al sito ufficiale. Facendo clic sul link, si accede a una copia esatta del sito web della banca che riporta perfino l'indirizzo nella barra del browser, anche se si tratta di un sito contraffatto. Da questo momento in poi, tutte le operazioni eseguite sul sito possono essere ricostruite e utilizzate per prelevare denaro dal conto dell'utente.

I link a siti di phishing vengono solitamente inviati in messaggi e-mail o tramite programmi di instant messaging. Anti-Phishing intercetta i tentativi di aprire siti di phishing e li blocca.

L'elenco delle minacce di Kaspersky Anti-Virus for Windows Workstations include gli indirizzi di tutti i siti di phishing attualmente noti. Gli esperti


Kaspersky Lab lo arricchiscono man mano con gli indirizzi ottenuti dall'Anti-Phishing Working Group, un'organizzazione internazionale che si occupa del problema. Questo elenco viene aggiornato automaticamente insieme agli elenchi delle minacce.

- Il componente *Popup Blocker* blocca le finestre popup contenenti inserzioni pubblicitarie con collegamenti a diversi siti web.

Le informazioni contenute in tali finestre di solito non sono di alcun interesse per il navigatore comune. Tali finestre si aprono automaticamente all'apertura di un determinato sito web o portano su una finestra diversa per mezzo di un ipertesto. Essi contengono pubblicità e altre informazioni non richieste. Il componente Popup Blocker blocca queste finestre, e un apposito messaggio sopra la barra delle applicazioni ne informa l'utente. È possibile determinare direttamente in questo messaggio se si desidera bloccare la finestra oppure no.

Popup Blocker funziona correttamente con il modulo di bloccaggio dei popup di Microsoft Internet Explorer incluso nel Service Pack 2 di Microsoft Windows XP. Quando si installa il Kaspersky Anti-Virus for Windows Workstations, viene installato anche un plug-in nel browser che consente di autorizzare l'apertura delle finestre popup direttamente dal browser.

Alcuni siti utilizzano legittimamente i popup per fornire informazioni in maniera più rapida e accessibile. Se si utilizzano tali siti con frequenza e le informazioni riportate nelle finestre popup sono importanti per l'utente, essi possono essere aggiunti all'elenco dei siti attendibili (vedere 11.1.1 a pag. 144).

Quando si usa Microsoft Internet Explorer, quando viene bloccato una finestra pop-up compare l'icona  nella barra di stato del browser. Questo pop-up può essere sbloccato oppure il sito può essere aggiunto alla lista degli indirizzi attendibili facendo clic sull'icona.

- Il componente *Anti-Banner* blocca i messaggi pubblicitari su banner speciali sulle pagine Web o incorporati nelle interfacce di vari programmi installati sul computer.

I banner pubblicitari non sono solo privi di informazioni utili, a distraggono l'utente dal lavoro e aumentano il traffico sul computer. Anti-Banner blocca i banner pubblicitari più diffusi, in base a maschere create da Kaspersky Anti-Virus for Windows Workstations. È possibile disabilitare il blocco dei banner o creare degli elenchi di banner autorizzati e bloccati.

Per integrare Anti-Banner in **Opera**, aggiungere la seguente riga a *standard\_menu.ini*, sezione **[Image Link Popup Menu]**:

```
Item, "New banner" = Copy image address & Execute program, "...\\Program Files\\Kaspersky Lab\\Kaspersky Anti-Virus 6.0 for Windows Workstations\\opera_banner_deny.vbs", "//nologo %C"
```

- Il componente *Anti-Dialer* protegge dalle connessioni via modem non autorizzate.

*Anti-Dialer* funziona su Microsoft Windows 2000, Microsoft Windows XP, Microsoft Windows XP x64, Microsoft Windows Vista, e Microsoft Windows Vista x64.

I dialer generalmente stabiliscono connessioni con siti Web specifici, come i siti con materiale pornografico. L'utente quindi è costretto a pagare costose tariffe telefoniche per un traffico non desiderato né utilizzato. Per escludere determinati numeri dall'elenco bloccato, occorre inserirli nella lista dei numeri attendibili (vedere 11.1.3 a pag. 149).

## 11.1. Configurazione di Anti-Spy

Anti-Spy protegge il computer da tutti i programmi noti agli esperti di Kaspersky Lab che potrebbero trafugare informazioni confidenziali o sottrarre denaro. È possibile configurare più specificamente il componente nei seguenti modi:

- Creando un elenco di siti Web attendibili (vedere 11.1.1 a pag. 144) dei quali non si intende bloccare i pop-up
- Creando liste "bianche" e "nere" di banner (vedere 11.1.2 a pag. 146)
- Creando un elenco dei numeri telefonici attendibili (vedere 11.1.3 a pag. 149) per le connessioni di accesso remoto che l'utente intende autorizzare

### 11.1.1. Creazione di elenchi di indirizzi attendibili per Popup Blocker

Per impostazione predefinita, Popup Blocker blocca gran parte delle finestre automatiche di popup. Fanno eccezione i popup dei siti web aggiunti all'elenco dei siti attendibili in Microsoft Internet Explorer e i siti Intranet di cui l'utente fa attualmente parte.



Se si esegue Windows XP con Service Pack 2, Internet Explorer dispone già di un'applicazione che blocca i popup, che può essere configurata selezionando le finestre da bloccare e quelle da non bloccare. Popup Blocker è compatibile con questa applicazione in base ai seguenti principi: una regola di blocco ha la precedenza, ovvero, se Internet Explorer o Popup Blocker hanno una regola di blocco per una finestra popup, la finestra viene bloccata. Per questo motivo, se si esegue Microsoft Windows XP Service Pack 2, si raccomanda di configurare insieme il browser e Popup Blocker.

Se per qualsiasi ragione si desidera visualizzare una finestra pop-up, occorre aggiungerla all'elenco degli indirizzi attendibili. Per fare ciò:

1. Aprire la finestra delle impostazioni di Kaspersky Anti-Virus for Windows Workstations e selezionare Anti-Spy nella struttura ad albero.
2. Fare clic su **Siti attendibili** nella sezione **Blocco popup**.
3. Fare clic su **Aggiungi** nella finestra che si apre (vedere Figura 39) e immettere una maschera per i siti dei quali non si intende bloccare le finestre pop-up.

**Suggerimento:**

Quando si immette la maschera di un indirizzo attendibile, si possono usare i caratteri \* o ?.

Per esempio, la maschera [http://www.test\\*](http://www.test*) esclude i pop-up provenienti da qualsiasi sito che inizia con quella serie di caratteri.

4. Specificare se si intende escludere dalla scansione gli indirizzi appartenenti alla zona di sicurezza di Internet Explorer o gli indirizzi sulla rete locale. Come impostazione predefinita, il programma li considera attendibili e non blocca i pop-up generati da questi indirizzi.

La nuova esclusione sarà aggiunta in testa all'elenco degli indirizzi attendibili. Per smettere di usare l'esclusione aggiunta, deselezionare la casella  accanto al nome. Per rimuovere un'esclusione completamente, selezionarla sulla lista e fare clic su **Elimina**.



Figura 39. Creazione dell'elenco degli indirizzi attendibili

Per bloccare le finestre pop-up provenienti dalla intranet o dai siti web compresi nella lista degli indirizzi attendibili di Microsoft Internet Explorer, deselezionare le caselle corrispondenti nella sezione **Siti attendibili**.

Quando un popup non incluso nell'elenco dei siti attendibili cerca di aprirsi, viene visualizzato un messaggio sopra l'icona del programma che informa dell'avvenuto blocco della finestra. Seguendo i collegamenti all'interno del messaggio è possibile eliminare il blocco e aggiungere l'indirizzo della finestra all'elenco dei siti attendibili.

È possibile inoltre sbloccare le finestre tramite Internet Explorer se si dispone del Service Pack 2 di Windows XP. A tal fine, utilizzare il menu di scelta rapida che si apre facendo clic sull'icona del programma che lampeggia nella parte inferiore del browser quando vengono bloccati dei popup.

## 11.1.2. Elenco di blocco dei banner pubblicitari

*Anti-Banner* è il componente di Kaspersky Anti-Virus for Windows Workstations che blocca i banner pubblicitari. Gli esperti Kaspersky Lab hanno compilato un elenco di maschere dei più comuni banner pubblicitari sulla base di ricerche specifiche, e l'hanno incluso nel programma. Se Anti-Banner non è disabilitato, blocca i banner pubblicitari selezionati tramite le maschere in questo elenco.

Inoltre è possibile creare liste bianche e liste nere dei banner pubblicitari, in base alle quali autorizzare o bloccare la visualizzazione degli stessi.

Si noti che se l'elenco dei banner bloccati o una lista nera contiene una maschera per filtrare domini, è comunque possibile continuare ad accedere al sito principale.

Per esempio, se la lista dei banner bloccati include una maschera per **truehits.net**, sarà possibile accedere a **http://truehits.net**, mentre l'accesso a **http://truehits.net/a.jpg** sarà bloccato.

### 11.1.2.1. Configurazione dell'elenco di blocco dei banner pubblicitari standard

Kaspersky Anti-Virus for Windows Workstations include maschere per i banner pubblicitari più diffusi sui siti web e sulle interfacce dei programmi. Questo elenco è stato compilato dagli esperti Kaspersky Lab e viene aggiornato con gli elenchi delle minacce.

È possibile selezionare quali maschere standard di banner pubblicitari si desidera usare durante l'esecuzione di Anti-Banner. Per fare ciò:

1. Aprire la finestra delle impostazioni di Kaspersky Anti-Virus for Windows Workstations e selezionare Anti-Spy nella struttura ad albero.
2. Fare clic sul pulsante **Impostazioni** nella sezione Anti-Banner.
3. Aprire la scheda **Generale** (vedere Figura 40). Anti-Banner blocca le maschere dei banner pubblicitari elencate nella scheda. È possibile utilizzare caratteri jolly in qualsiasi punto dell'indirizzo del banner.

La lista delle maschere bloccate standard non può essere modificata. Se non si intende bloccare un banner coperto da una maschera standard, deselezionare la casella  accanto alla maschera.

Per analizzare i banner pubblicitari che non corrispondono alle maschere incluse negli elenchi standard, selezionare  **Usa metodi di analisi euristica**. L'applicazione analizzerà le immagini caricate alla ricerca di segnali tipici dei banner pubblicitari. Grazie a tale analisi, l'immagine può essere identificata come banner e quindi bloccata.

È inoltre possibile creare liste personalizzate di banner autorizzati e bloccati. Questa operazione si esegue dalle schede **Elenco consentiti** e **Elenco bloccati**.

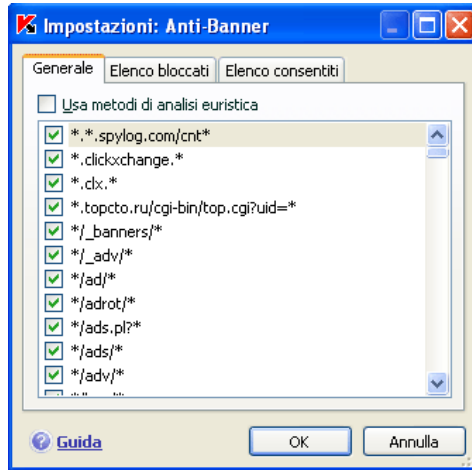


Figura 40. Elenco dei banner bloccati

### 11.1.2.2. Liste bianche dei banner pubblicitari

È possibile creare una lista bianca per consentire la visualizzazione di certi banner. Le liste bianche contengono le maschere dei banner pubblicitari autorizzati.

*Per aggiungere una nuova maschera all'elenco consentiti:*

1. Aprire la finestra delle impostazioni di Kaspersky Anti-Virus for Windows Workstations e selezionare Anti-Spy nella struttura ad albero.
2. Fare clic sul pulsante **Impostazioni** nella sezione Anti-Banner.
3. Aprire la scheda **Elenco consentiti**.

Aggiungere la maschera del banner autorizzato mediante il pulsante **Aggiungi**. È possibile specificare l'URL completo per il banner o una maschera per esso. In quest'ultimo caso, quando un banner tenta di caricarsi, il programma ne analizza l'indirizzo in base alla maschera specificata.

Quando si crea una maschera, si possono usare i caratteri \* o ?. (dove \* rappresenta una sequenza di caratteri e ? qualsiasi singolo carattere).

Per sospendere l'uso di una maschera creata, è possibile eliminarla dalla lista o deselezionare la casella  accanto alla stessa. I banner che rientrano in questa maschera non verranno più bloccati.

Tramite i pulsanti **Importa** ed **Esporta** , è possibile copiare da un computer a un altro gli elenchi di banner autorizzati.

### 11.1.2.3. Liste nere dei banner pubblicitari

Oltre all'elenco standard dei banner bloccati (vedere 11.1.2.1 a pag. 147) da Anti-Banner, l'utente può creare una lista personalizzata. Per fare ciò:

1. Aprire la finestra delle impostazioni di Kaspersky Anti-Virus for Windows Workstations e selezionare Anti-Spy nella struttura ad albero.
2. Fare clic sul pulsante **Impostazioni** nella sezione dei banner pubblicitari bloccati.
3. Aprire la scheda **Elenco bloccati**.

Mediante il pulsante **Aggiungi** immettere una maschera per il banner che deve essere bloccato da Anti-Banner. È possibile specificare l'URL completo per il banner o una maschera per esso. In quest'ultimo caso, quando un banner tenta di caricarsi, il programma ne analizza l'indirizzo in base alla maschera specificata.

Quando si crea una maschera, si possono usare i caratteri \* o ?. (dove \* rappresenta una sequenza di caratteri e ? qualsiasi singolo carattere).

Per sospendere l'uso di una maschera creata, è possibile eliminarla dalla lista o deselegionare la casella  accanto alla stessa.

Tramite i pulsanti **Importa** ed **Esporta** , è possibile copiare da un computer a un altro gli elenchi di banner bloccati.

### 11.1.3. Creazione di una lista dei numeri attendibili con Anti-Dialer

Il componente *Anti-Dialer* monitora i numeri di telefono utilizzati per collegarsi furtivamente a Internet. Una connessione è considerata segreta se configurata in modo da non informare l'utente della connessione in corso o se non è inizializzata dall'utente stesso.

Ogni qualvolta si ha un tentativo di connessione segreta, il programma informa l'utente visualizzando un messaggio specifico, che chiede all'utente se bloccare o meno la chiamata. Se la connessione non è stata avviata dall'utente, è molto probabile che sia stata configurata da un programma nocivo.

Per autorizzare le connessioni a certi numeri senza che il programma chieda conferma ogni volta, occorre aggiungerli alla lista dei numeri attendibili. Per fare ciò:

1. Aprire la finestra delle impostazioni di Kaspersky Anti-Virus for Windows Workstations e selezionare Anti-Spy nella struttura ad albero.
2. Fare clic su **Numeri attendibili** nella sezione Anti-Dialer.
3. Fare clic su **Aggiungi** nella finestra che si apre (vedere Figura 41) e immettere un numero o una maschera per i numeri telefonici legittimi.

**Suggerimento:**

Quando si immette la maschera di un numero attendibile, si possono usare i caratteri \* o ?.

Per esempio, la maschera 0???? 79787\* copre qualsiasi numero che inizi con 79787 e con prefisso di quattro cifre.

Il nuovo numero di telefono sarà aggiunto in testa alla lista dei numeri attendibili. Per smettere di usare l'esclusione aggiunta, deselezionare la casella  accanto al nome sulla lista. Per rimuovere un'esclusione completamente, selezionarla sulla lista e fare clic su **Elimina**.



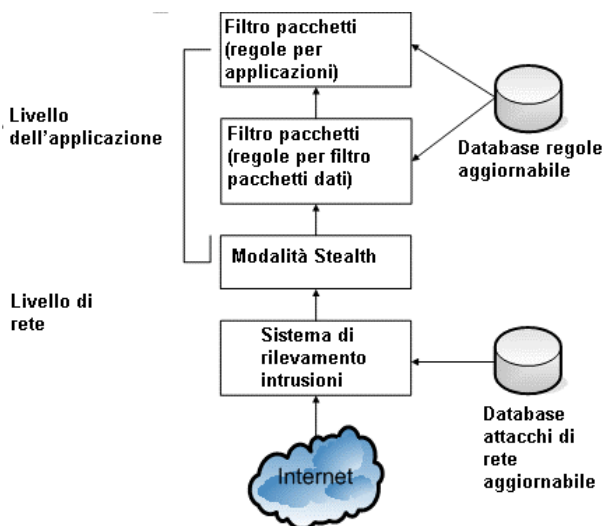
Figura 41. Creazione di una lista di indirizzi attendibili

---

# CAPITOLO 12. PROTEZIONE CONTRO GLI ATTACCHI DI RETE

I computer di oggi sono diventati estremamente vulnerabili durante la connessione a Internet. Essi sono soggetti a infezioni virali e ad altri tipi di attacco che sfruttano le vulnerabilità dei sistemi operativi e del software.

Il componente *Anti-Hacker* di Kaspersky Anti-Virus for Windows Workstations garantisce la sicurezza sulle reti locali e su Internet, proteggendo il computer a livello di rete e delle applicazioni, e mascherando il computer sulla rete per prevenire gli attacchi di rete. Esaminiamo più da vicino il funzionamento di Anti-Hacker.



La protezione a livello di rete è garantita da regole globali di filtraggio pacchetti, nelle quali le attività di rete sono consentite o bloccate in base ad un'analisi delle impostazioni quali: direzione dei pacchetti, il protocollo di trasferimento dati e la porta pacchetti in uscita. Le regole per i pacchetti di dati stabiliscono l'accesso alla rete, indipendentemente dalle applicazioni installate sul computer che utilizzano la rete.

Oltre alle regole di filtro pacchetti, il *Sistema di rilevamento intrusioni* (IDS) fornisce ulteriore sicurezza a livello della rete. L'obiettivo del sistema IDS è analizzare le connessioni in entrata, rilevare le scansioni delle porte del computer e filtrare i pacchetti di rete volti a sfruttare le vulnerabilità del software. Quando è attivato, l'IDS blocca tutte le connessioni in entrata da parte del computer che intende perpetrare l'attacco per un certo intervallo di tempo e l'utente riceve un messaggio che lo informa che il computer è stato sottoposto a un tentativo di attacco di rete.

L'IDS si avvale di uno speciale database degli attacchi di rete (vedere 12.9 a pag. 170) per l'analisi, che viene espanso regolarmente dagli esperti di Kaspersky Lab ed aggiornato insieme agli elenchi delle minacce.

A livello delle applicazioni il computer è protetto facendo sì che le applicazioni installate sul computer si attengano alle regole per l'utilizzo delle risorse di rete imposte da Anti-Hacker. Come per la sicurezza a livello di rete, la sicurezza a livello delle applicazioni si basa sull'analisi dei pacchetti di dati in termini di direzione, protocollo di trasferimento e porte utilizzate. Tuttavia, a livello delle applicazioni, sono prese in considerazione sia le caratteristiche dei pacchetti di dati che la specifica applicazione che invia e riceve i pacchetti.

L'uso delle regole delle applicazioni consente di configurare in modo più specifico la protezione facendo sì, per esempio, che un determinato tipo di connessione venga precluso ad alcune applicazioni ma non ad altre.

Esistono due tipi di regole per Anti-Hacker, basati sui due livelli di sicurezza di Anti-Hacker:

- Regole di filtraggio pacchetti (vedere 12.3 a pag. 158). Utilizzate per creare restrizioni di carattere generale all'attività di rete, a prescindere dalle applicazioni installate. Esempio: Se si crea una regola di filtraggio pacchetti che blocca le connessioni in entrata sulla porta 21, nessuna delle applicazioni che utilizza quella porta (un server ftp, per esempio) sarà accessibile dall'esterno.
- Regole per le applicazioni (vedere 12.2 a pag. 154). Utilizzate per creare restrizioni all'attività di rete per applicazioni specifiche. Esempio: Se le connessioni sulla porta 80 vengono bloccate per tutte le applicazioni, è possibile creare una regola che consenta le connessioni su tale porta solo per Firefox.

Esistono due tipi di regole per applicazioni e filtro pacchetti: *Permetti* e *Blocca*. L'installazione del programma include una serie di regole che definiscono l'attività di rete per le applicazioni più diffuse e l'utilizzo dei protocolli e delle porte più diffusi. Kaspersky Anti-Virus for Windows Workstations include anche una serie di regole di autorizzazione per applicazioni attendibili la cui attività di rete non è sospetta.

Kaspersky Anti-Virus for Windows Workstations suddivide l'intero spazio di rete in zone in modo da semplificare le impostazioni e le regole: *Internet* e *zone di*



*sicurezza*, che corrispondono ampiamente alle sottoreti a cui appartiene il computer dell'utente. È possibile assegnare uno stato a ogni zona (*Internet, Rete locale, Attendibile*), che determina l'applicazione delle regole e il monitoraggio dell'attività di rete in quella zona (vedere 12.5 a pag. 164).

Una speciale funzione di Anti-Hacker, la *Modalità Mascheramento* (modalità invisibile), impedisce che il computer sia rilevato dall'esterno, in modo che gli hacker non possano rilevarlo e quindi attaccarlo. Questa modalità non compromette le prestazioni del computer su Internet: si consiglia di non utilizzare la modalità Stealth se il computer opera come server.

## 12.1. Selezione di un livello di protezione di Anti-Hacker

Durante il lavoro sulla rete, Kaspersky Anti-Virus for Windows Workstations protegge il computer a uno dei seguenti livelli (vedere Figura 42):

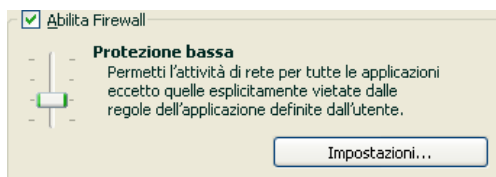


Figura 42. Selezione di un livello di protezione di Anti-Hacker

**Protezione alta** – consente solo le attività di rete permesse, tramite regole di autorizzazione incorporate nel programma o create dall'utente. La serie di regole incluse con Kaspersky Anti-Virus for Windows Workstations include le regole di autorizzazione per applicazioni la cui attività di rete non è sospetta e per i pacchetti di dati il cui invio e ricezione sono assolutamente sicuri. Se tuttavia esiste una regola di blocco per un'applicazione con priorità più elevata rispetto a quella di autorizzazione, il programma blocca ogni attività di rete dell'applicazione.

### Attenzione!

Se si seleziona questo livello di sicurezza, tutte le attività di rete non registrate in una regola di autorizzazione di Anti-Hacker saranno bloccate. Pertanto si raccomanda di utilizzare questo livello solo se si è certi che tutti i programmi necessari sono autorizzati alla connessione di rete dalle regole in vigore e se non si prevede di installare nuovo software.

**Modalità Apprendimento** – livello di protezione durante il quale vengono create le regole di Anti-Hacker. A questo livello, ogni volta che un programma tenta di utilizzare una risorsa di rete, Anti-Hacker controlla se esiste una regola per tale connessione. In presenza di una regola, Anti-Hacker la applica. Se non esiste alcuna regola, sullo schermo viene visualizzato un messaggio contenente una descrizione della connessione di rete (quale programma l'ha avviata, quale porta, il protocollo, ecc.). L'utente deve decidere se autorizzare questa connessione o no. Utilizzando uno speciale pulsante nella finestra del messaggio, è possibile creare una regola per quella connessione in modo tale che in futuro Anti-Hacker utilizzi la nuova regola per quella connessione senza visualizzare il messaggio sullo schermo.

**Protezione bassa** – blocca solo le attività di rete non consentite, tramite regole di blocco incorporate nel programma o create dall'utente. Se tuttavia esiste una regola di autorizzazione per un'applicazione con priorità più elevata rispetto a quella di blocco, il programma permette ogni attività di rete di quell'applicazione.

**Consenti tutti** – ammette tutta l'attività di rete sul computer. Si consiglia di impostare questo livello di protezione in casi molto rari, dove non siano stati osservati attacchi di rete e dove tutta l'attività di rete sia considerata attendibile.

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

*Per modificare un livello di sicurezza di rete:*

1. Selezionare **Anti-Hacker** nella finestra delle impostazioni di Kaspersky Anti-Virus for Windows Workstations.
2. Regolare il cursore nella sezione **Abilita Firewall** ad indicare il livello di sicurezza desiderato.

*Per configurare il livello di sicurezza di rete:*

1. Selezionare il livello di sicurezza che meglio soddisfa le preferenze dell'utente, come sopra.
2. Fare clic sul pulsante **Impostazioni** e modificare le impostazioni di sicurezza di rete nella finestra che appare.

## 12.2. Regole delle applicazioni

Kaspersky Anti-Virus for Windows Workstations include una serie di regole per le più diffuse applicazioni di Windows. Si tratta di programmi la cui attività di rete è stata analizzata in dettaglio dagli esperti Kaspersky Lab e definita come pericolosa oppure come attendibile.

In funzione del livello di sicurezza selezionato per il Firewall (vedere 12.1 a pag. 153) e del tipo di rete (vedere 12.5 a pag. 164) sul quale opera il computer, l'elenco di regole per i programmi può essere utilizzato in vari modi. Ad esempio, con **Protezione alta** tutta l'attività di rete delle applicazioni che non corrisponde alle regole di autorizzazione viene bloccata.

*Per lavorare con l'elenco delle regole per le applicazioni:*

1. Fare clic su **Impostazioni** nella sezione Abilita Firewall della finestra delle impostazioni di Anti-Hacker.
2. Nella finestra che si apre, selezionare la scheda **Regole per applicazioni** (vedere Figura 43).

Tutte le regole su questa scheda possono essere raggruppate in due modi:

- **Regole per applicazioni** Se è selezionata l'opzione  **Raggruppa regole per applicazione**, ogni applicazione per la quale siano state create regole verrà visualizzata in un'unica riga nell'elenco. Per ogni applicazione sono riportate le seguenti informazioni: nome e icona dell'applicazione, numero di regole create per essa, cartella nella quale si trova il file eseguibile, e riga di comando.

Mediante il pulsante **Modifica**, è possibile andare alla lista delle regole per l'applicazione selezionata sulla lista e modificarla: aggiungere una nuova regola, modificarne una esistente e modificare la priorità relativa.

Il pulsante **Aggiungi** consente di aggiungere una nuova applicazione alla lista e di creare una regola apposita.

I pulsanti **Esporta** e **Importa** consentono di trasferire le regole create su altri computer, il che favorisce una rapida configurazione di Anti-Hacker.

- **Elenco generale di regole** Se l'opzione  **Raggruppa regole per applicazione** non è selezionata, ogni riga dell'elenco generale visualizza informazioni complete relative ad una regola: il nome dell'applicazione e il comando per lanciarla, se autorizzare o bloccare l'attività di rete, il protocollo di trasferimento dati, la direzione dei dati (in entrata o in uscita), e altre informazioni.

Il pulsante **Aggiungi** consente di creare una nuova regola, ed è possibile modificarne una esistente selezionandola sulla lista e facendo clic sul pulsante **Modifica**. È inoltre possibile modificare le impostazioni di base nella parte inferiore della scheda.

Per modificare l'ordine di priorità, utilizzare i pulsanti **Sposta su** e **Sposta giù**.

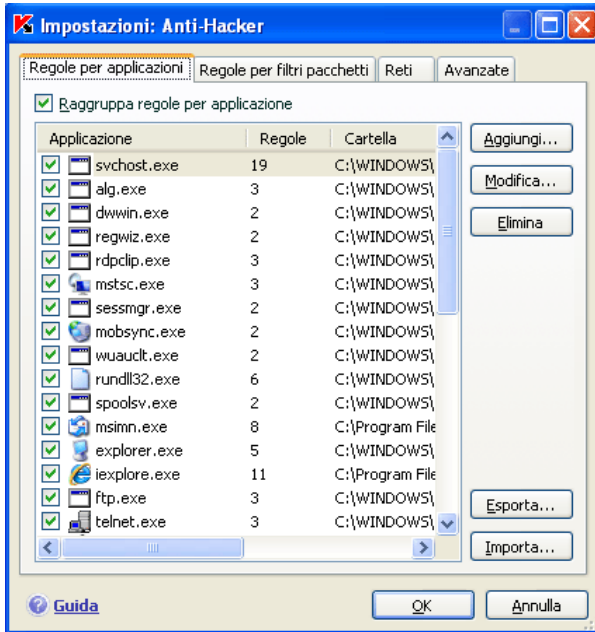


Figura 43. Elenco di regole per le applicazioni installate sul computer

## 12.2.1. Creazione manuale delle regole

*Per creare manualmente una regola per applicazioni:*

1. Selezionare l'applicazione. A tal fine, fare clic su **Aggiungi** sulla scheda **Regole per applicazioni** (vedere Figura 43). Verrà visualizzato un menu di scelta rapida che aprirà una finestra di dialogo standard per la selezione dei file tramite l'opzione **Sfoglia**, oppure ad un elenco di applicazioni in esecuzione tramite l'opzione **Applicazioni**, consentendo di effettuare la selezione. Si apre un elenco di regole per l'applicazione selezionata. Se esistono già delle regole per l'applicazione, esse sono elencate nella parte superiore della finestra. In assenza di regole, la finestra appare vuota.
2. Fare clic sul pulsante **Aggiungi** nella finestra delle regole per l'applicazione selezionata.

La finestra **Nuova regola** che si apre contiene un modulo che può essere utilizzato per definire in dettaglio una regola (vedere 12.6 a pag. 165).

## 12.2.2. Creazione di regole da un modello

Kaspersky Anti-Virus include modelli di regole già pronti che possono essere usati per creare regole personalizzate.

L'intera gamma di applicazioni di rete esistenti può essere suddivisa in diversi tipi: client di posta, browser Web, ecc. Ciascun tipo è caratterizzato da un insieme di attività specifiche, quali l'invio e la ricezione della posta o la ricezione e la visualizzazione di pagine html. Ciascun tipo utilizza un determinato insieme di protocolli e porte di rete. Ecco perché disporre di modelli di regole aiuta ad effettuare rapidamente e velocemente la configurazione iniziale delle regole in base al tipo di applicazione.

*Per creare una regola per applicazioni da un modello:*

1. Selezionare  **Raggruppa regole per applicazione** nella scheda **Regole per applicazioni**, se non è già stato fatto, e fare clic sul pulsante **Aggiungi**.
2. Verrà visualizzato un menu di scelta rapida che aprirà una finestra di dialogo standard per la selezione dei file tramite l'opzione **Sfoggia**, oppure ad un elenco di applicazioni in esecuzione tramite l'opzione **Applicazioni**, consentendo di effettuare la selezione. Si apre una finestra contenente le regole per l'applicazione selezionata. Le regole per l'applicazione verranno visualizzate nella parte superiore della finestra. Se non esiste alcuna regola, la finestra sarà vuota.
3. Fare clic su **Modello** nella finestra delle regole per le applicazioni e selezionare uno dei modelli dal menu di scelta rapida (vedere Figura 44).

**Condnti tutti** è una regola che ammette qualsiasi attività di rete sul computer per quell'applicazione. **Blocca tutti** è una regola che blocca qualsiasi attività di rete sul computer per quell'applicazione. Qualsiasi tentativo di stabilire una connessione di rete da parte dell'applicazione in questione sarà bloccato senza informare l'utente.

Gli altri modelli elencati sul menu di scelta rapida creano regole tipiche per i tipi di programmi corrispondenti. Per esempio, il modello **Client di posta** crea una serie di regole che autorizzano l'attività di rete standard per i client di posta, come l'invio delle e-mail.

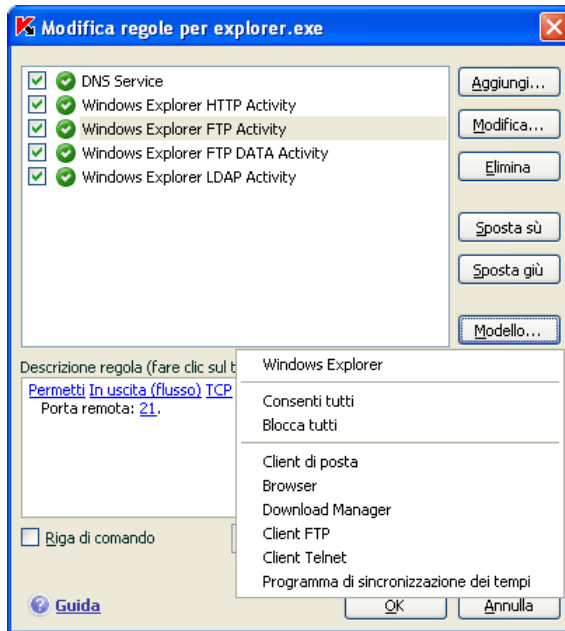


Figura 44. Selezione di un modello per la creazione di una nuova regola

4. Eventualmente, le regole create per un'applicazione possono essere modificate. È possibile modificare azioni, direzione della connessione di rete, indirizzo remoto, porte (locale e remota) e l'intervallo temporale da assegnare alla regola.
5. Per applicare la regola ad un programma aperto con determinate impostazioni di riga di comando, selezionare  **Riga di comando** e immettere la stringa nel campo a destra.

La regola o la serie di regole create saranno aggiunte in coda alla lista con la priorità più bassa. La priorità della regola può essere aumentata (vedere 12.5 a pag. 164)

Una regola può essere creata dalla finestra di avviso di rilevamento di attività di rete (vedere 12.10 a pag. 173).

## 12.3. Regole di filtraggio pacchetti

Il pacchetto di installazione di Kaspersky Anti-Virus include una serie di regole che utilizza per filtrare i pacchetti di dati in entrata e in uscita dal computer. Il

trasferimento dei pacchetti di dati può essere avviato dall'utente stesso o da un programma installato sul computer. Il programma include le regole di filtraggio dei pacchetti studiate da Kaspersky Lab, che determinano se i pacchetti sono pericolosi o no.

In funzione del livello di sicurezza selezionato per il Firewall e del tipo di rete sul quale opera il computer, la lista di regole per i programmi può essere utilizzata in vari modi. Ad esempio, con il livello **Protezione alta**, tutta l'attività di rete che non corrisponde alle regole di autorizzazione viene bloccata.

### Importante!

Si noti che le regole per le zone di sicurezza (vedere 12.6 a pag. 165) hanno una priorità maggiore rispetto a quelle di blocco dei pacchetti. Quindi, ad esempio, se si seleziona lo stato **Rete locale**, gli scambi di pacchetti saranno consentiti così come l'accesso alle cartelle condivise, a prescindere dalle regole di blocco dei pacchetti.

*Per lavorare con l'elenco delle regole di filtraggio dei pacchetti:*

1. Fare clic su **Impostazioni** nella sezione Firewall della finestra delle impostazioni di Anti-Hacker.
2. Nella finestra che si apre, selezionare la scheda **Regole per filtri pacchetti** (vedere Figura 45).

Per ogni regola di filtraggio pacchetti sono riportate le seguenti informazioni: azione (ovvero, se autorizza o blocca il trasferimento dei pacchetti), nome della regola, protocollo di trasferimento dati, direzione dei pacchetti e impostazioni della connessione di rete utilizzata per trasferire i pacchetti.

Se la casella accanto al nome della regola è selezionata, la regola verrà utilizzata.

È possibile lavorare con l'elenco delle regole utilizzando i pulsanti a destra dell'elenco.

*Per creare una nuova regola di filtraggio pacchetti:*

Fare clic sul pulsante **Aggiungi** nella scheda **Regole per filtri pacchetti**.

La finestra **Nuova regola** che si apre contiene un modulo che può essere utilizzato per rifinire in dettaglio una regola (vedere la sezione 12.4 a pag. 160).

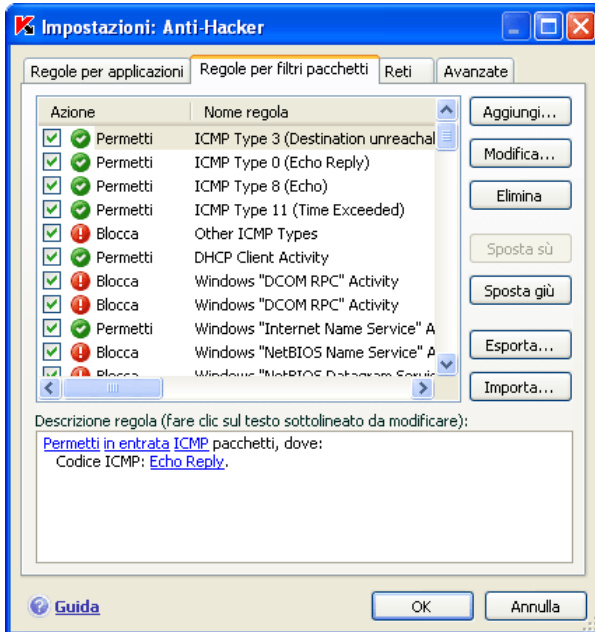


Figura 45. Elenco delle regole di filtraggio pacchetti

## 12.4. Aggiustamento delle regole per applicazioni e filtro pacchetti

La finestra **Nuova regola** per l'impostazione di regole avanzate è praticamente identica sia per le applicazioni che per i pacchetti di dati (vedere Figura 46).

### Passaggio 1:

- Immettere un nome per la regola. Il programma usa un nome predefinito che è meglio sostituire.
- Selezionare le impostazioni della connessione di rete per la regola: indirizzo IP remoto, porta remota, indirizzo IP locale, e ore in cui la regola viene applicata. Verificare tutte le impostazioni che si desidera applicare alla regola.
- Configurare le altre impostazioni per le notifiche all'utente. Se si desidera la comparsa di un messaggio a comparsa sullo schermo al momento



dell'applicazione di una regola, corredato da un breve commento, selezionare  **Visualizza avviso**. Se si desidera che il programma registri le invocazioni di una regola nel rapporto di Anti-Hacker, selezionare  **Registra evento**. Per impostazione predefinita, al momento della creazione della regola la casella non è selezionata. Si consiglia di utilizzare impostazioni supplementari quando si creano regole di blocco.

Si noti che quando si crea una regola di blocco nella modalità di addestramento di Anti-Hacker, le informazioni sulla regola da applicare verranno automaticamente inserite nel rapporto. Se non è necessario che il programma registri tali informazioni, deselezionare la casella di controllo **Registra evento** nelle impostazioni di tale regola.

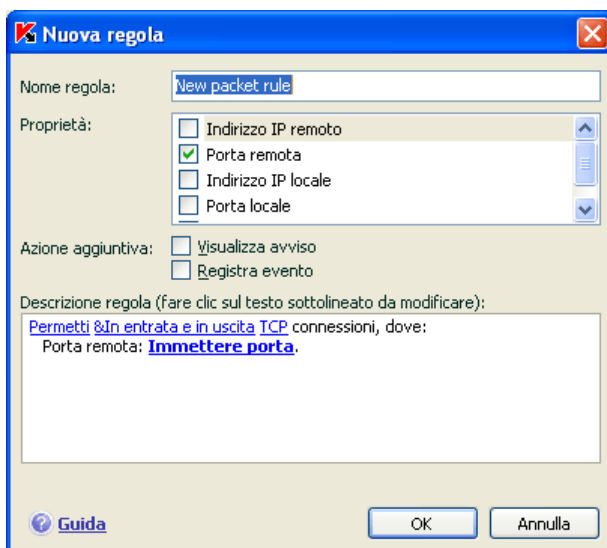


Figura 46. Creazione di una nuova regola per applicazioni

Il punto numero due nella creazione di una regola è l'assegnazione dei valori dei parametri e la selezione delle azioni da intraprendere. Queste operazioni sono eseguite nella sezione **Descrizione regola**.

1. L'azione predefinita per ogni nuova regola è *Permetti*. Per modificarla in una regola di tipo *Blocca*, fare clic sul collegamento Permetti nella sezione di descrizione della regola. Questa sarà modificata in Blocca.

Kaspersky Anti-Virus esaminerà comunque il traffico di rete per i programmi ed i pacchetti per i quali è stata creata una regola di autorizzazione. Ciò può avere come conseguenza una trasmissione più lenta dei dati.

2. Se non si era selezionata un'applicazione prima di creare la regola, è necessario farlo adesso facendo clic su specificare nome applicazione. Fare clic sul collegamento e, nella finestra standard di selezione che si apre, selezionare il file eseguibile dell'applicazione per la quale si sta creando la regola.
3. Determinare la direzione della connessione di rete per la regola. Come impostazione predefinita, la regola si applica ad una connessione bidirezionale, vale a dire sia in entrata che in uscita. Per modificare la direzione, fare clic con il tasto sinistro del mouse su in entrata e in uscita e selezionare la direzione della connessione di rete nella finestra che si apre:
  - ⊙ **Flusso in entrata.** La regola viene applicata alle connessioni di rete aperte da un computer remoto.
  - ⊙ **Pacchetto in entrata.** La regola si applica ai pacchetti di dati ricevuti dal computer in uso, eccezion fatta per i pacchetti TCP.
  - ⊙ **Flussi in entrata e in uscita.** La regola viene applicata al traffico sia in entrata che in uscita, a prescindere da quale computer, sia esso quello dell'utente o un computer remoto, ha avviato la connessione di rete.
  - ⊙ **Flusso in uscita.** La regola viene applicata solo alle connessioni di rete aperte dal computer in uso.
  - ⊙ **Pacchetto in uscita.** La regola si applica ai pacchetti di dati inviati dal computer dell'utente, eccezion fatta per i pacchetti TCP.

Se è importante impostare la direzione dei pacchetti specificamente nella regola, selezionare se si tratta di pacchetti in entrata o in uscita. Se si desidera creare una regola per il trasferimento dei dati in streaming, selezionare flusso: in entrata, in uscita o entrambi.

La differenza tra la *direzione del flusso* e la *direzione dei pacchetti* è che quando si crea una regola per un flusso, si definisce la direzione della connessione. La direzione dei pacchetti quando si trasferiscono i dati su questa connessione non è presa in considerazione.

Per esempio, se si configura una regola per lo scambio di dati con un server FTP in esecuzione in modalità FTP passiva, è necessario autorizzare un flusso in uscita. Per scambiare dati con un server FTP in modalità FTP attiva, è necessario autorizzare i flussi sia in entrata che in uscita.

4. Se è stato selezionato un indirizzo remoto come proprietà di una connessione di rete, fare clic su Immettere indirizzo IP e digitare l'indirizzo IP, la gamma di indirizzi IP o l'indirizzo di sottorete per la regola nella finestra che si apre. È possibile usare uno o più tipi di indirizzo IP per una regola. Possono essere specificati più indirizzi di ciascun tipo.
5. Impostare il protocollo utilizzato dalla connessione di rete. TCP è il protocollo predefinito per la connessione. Se si sta creando una regola per applicazioni, è possibile selezionare il protocollo TCP o l'UDP, facendo clic con il pulsante sinistro del mouse sul link con il nome del protocollo fino a visualizzare quello desiderato. Se si sta creando una regola per il filtro pacchetti e si desidera modificare il protocollo predefinito, fare clic sul suo nome e selezionare il protocollo nella finestra che si apre. Se si seleziona ICMP, potrebbe essere necessario indicare il tipo.
6. Se si sono selezionate le impostazioni della connessione di rete (indirizzo, porta, intervallo temporale), è necessario assegnare loro anche dei valori esatti.

Una volta aggiunta alla lista delle regole per l'applicazione, la regola può essere ulteriormente configurata (vedere Figura 47). Per applicare la regola a un'applicazione aperta con determinati parametri da riga di comando, selezionare  **Riga di comando** e immettere la stringa di parametri nel campo a destra. Questa regola non sarà applicata ad applicazioni avviate con una diversa istruzione da riga di comando.

Microsoft Windows 98 non offre l'opzione delle impostazioni iniziali della riga di comando.

Una regola può essere creata dalla finestra di avviso di rilevamento di attività di rete (vedere 12.10 a pag. 173).

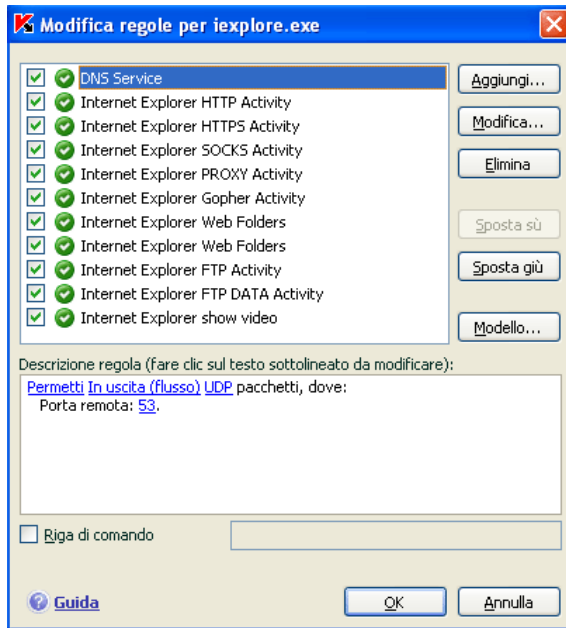


Figura 47. Impostazioni avanzate di una nuova regola

## 12.5. Assegnazione della priorità alle regole

Ogni regola creata per un'applicazione o un pacchetto ha una priorità di esecuzione. A parità di altre condizioni (per esempio le impostazioni della connessione di rete), l'azione applicata all'attività del programma sarà quella della regola con la priorità più elevata.

La priorità di una regola dipende dalla sua posizione nell'elenco delle regole. La prima regola dell'elenco è quella con la massima priorità. Ogni regola creata manualmente viene aggiunta in testa all'elenco. Le regole create da modelli o da un avviso vengono aggiunte in fondo all'elenco delle regole.

*Per assegnare una priorità alle regole per applicazioni procedere come segue:*

1. Selezionare il nome dell'applicazione nella scheda **Regole per le applicazioni** e fare clic sul pulsante **Modifica**.

2. Utilizzare i pulsanti **Sposta su** e **Sposta giù** nella scheda delle regole per le applicazioni per spostare le regole all'interno dell'elenco, modificandone la priorità.

*Per assegnare una priorità alle regole di filtraggio dei pacchetti procedere come segue:*

1. Selezionare la regola nella scheda **Regole per il filtro pacchetti**.
2. Utilizzare i pulsanti **Sposta su** e **Sposta giù** nella scheda dei filtri pacchetti per spostare le regole all'interno dell'elenco, modificandone la priorità.

## 12.6. Regole per zone di sicurezza

Dopo l'installazione, Anti-Hacker analizza l'ambiente di rete del computer. In base ai risultati dell'analisi, l'intero spazio di rete viene suddiviso in zone:

*Internet* – la rete a livello mondiale. In questa zona, Kaspersky Anti-Virus for Windows Workstations opera come personal firewall, utilizzando regole per le applicazioni e regole di filtro pacchetti predefinite per controllare tutta l'attività di rete e garantire la massima sicurezza. Quando si lavora in questa zona, le impostazioni di sicurezza non possono essere modificate, tranne che per abilitare la modalità Stealth sul computer per maggiore sicurezza.

*Zone di sicurezza* – alcune zone convenzionali che più corrispondono alle sottoreti in cui è incluso il computer (potrebbero essere sottoreti locali domestiche o al lavoro). Solitamente, queste zone sono definite a medio rischio. È possibile modificare lo stato di queste zone in base a quanto si ritiene affidabile una determinata sottorete, e configurare regole appropriate per il filtraggio pacchetti e le applicazioni.

Se è abilitata la modalità Training di Anti-Hacker, si apre una finestra ogni volta che il computer si connette a una nuova zona, visualizzandone una breve descrizione. È necessario assegnare uno status alla zona: in base ad esso l'attività di rete sarà autorizzata oppure no. I valori di stato possibili sono i seguenti:

- **Internet.** Questo è lo stato predefinito assegnato a Internet, poiché, su Internet, il computer è soggetto potenzialmente a tutti i tipi di minacce. Questo stato è raccomandato anche per reti che non sono protette da nessun programma antivirus, firewall, filtro, ecc. Selezionando questo stato, il programma garantisce la massima sicurezza all'interno di questa zona, in particolare:
  - Blocco di qualsiasi attività di rete NetBios all'interno della sottorete

- Blocco delle regole per applicazioni e filtraggio pacchetti che consentono un'attività NetBios all'interno della sottorete

Anche se è stata creata una cartella condivisa, le informazioni nella stessa non saranno disponibili ad utenti appartenenti a sottoreti con questo stato. Inoltre, se questo stato è selezionato per una certa sottorete, non sarà possibile accedere ai file ed alle stampanti di questa sottorete.

- **Rete locale.** Il programma assegna questo stato a tutte le zone rilevate durante l'analisi dell'ambiente di rete del computer, con l'eccezione delle zone Internet. Si raccomanda di applicare questo stato alle zone caratterizzate da un fattore di rischio medio (per esempio LAN aziendali). Selezionando questo stato, il programma consente:
  - Qualsiasi attività di rete NetBios all'interno della sottorete
  - Regole per applicazioni e filtraggio pacchetti che consentono un'attività NetBios all'interno della sottorete

Selezionare questo stato per concedere l'accesso a certe cartelle o stampanti sul computer ma bloccare qualsiasi altra attività dall'esterno.

- **Attendibile.** Questo stato è raccomandato solo per le zone ritenute assolutamente sicure, in cui il computer non è esposto ad attacchi o tentativi di accesso. Se si seleziona questo stato, tutte le attività di rete sono consentite. Anche se è selezionato il livello Protezione massima e sono state create regole di blocco, queste non funzionano per computer remoti appartenenti a una zona attendibile.

Osservare che qualsiasi restrizione o autorizzazione all'accesso ai file ha valore solo all'esterno di questa sottorete.

È possibile utilizzare la modalità Mascheramento per maggiore sicurezza quando si usano reti classificate come **Internet**. Questa funzione consente solo le attività di rete avviate dal computer in uso, in modo che il computer risulti invisibile per l'ambiente circostante. Questa modalità non pregiudica le prestazioni del computer su Internet.

Si sconsiglia l'uso della modalità Mascheramento se il computer viene utilizzato come server (per esempio, un server di posta o HTTP), poiché i computer che si connettono al server non lo vedranno come collegato.

L'elenco delle zone sulle quali è registrato il computer è visualizzato nella scheda **Reti** (vedere Figura 48). Ad ogni zona è assegnato uno stato, una breve descrizione della rete ed è specificato se sia utilizzata la modalità Mascheramento.

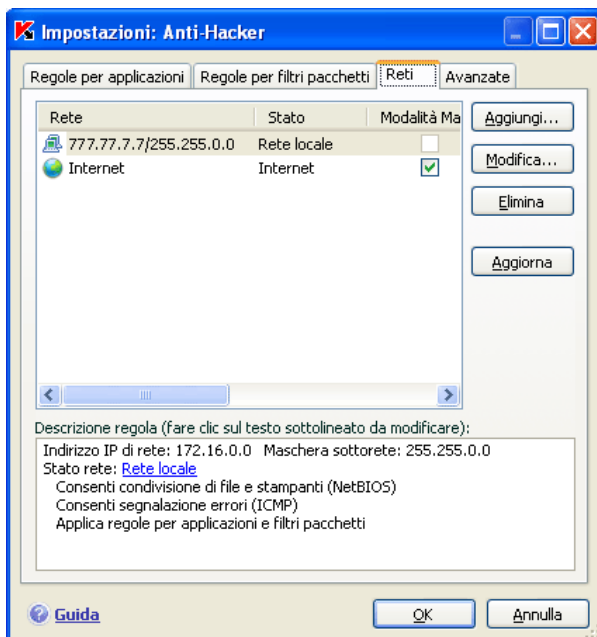


Figura 48. Elenco delle regole per le zone

Per modificare lo stato di una zona o per abilitare/disabilitare la modalità Mascheramento, selezionare la zona dall'elenco e utilizzare i collegamenti appropriati nel riquadro **Descrizione regola** sotto l'elenco. È possibile eseguire attività simili e modificare indirizzi e subnet mask nella finestra **Impostazioni rete** che si apre facendo clic su **Modifica**.

È possibile aggiungere una nuova zona all'elenco durante la visualizzazione. A tal fine, fare clic su **Aggiorna**. Anti-Hacker cerca le potenziali zone di registrazione, chiedendo eventualmente di selezionare uno stato da assegnare a quelle rilevate. È possibile inoltre aggiungere manualmente nuove zone all'elenco (per esempio se si connette il laptop a una nuova rete). A tal fine, fare clic su **Aggiungi** e compilare i dati necessari nella finestra **Impostazioni rete**.

Per eliminare la rete dall'elenco, selezionarla e fare clic sul pulsante **Elimina**.

## 12.7. Modalità Firewall

La modalità Firewall (vedere Figura 49) controlla la compatibilità di Anti-Hacker con i programmi che stabiliscono più connessioni di rete e con i giochi in rete.

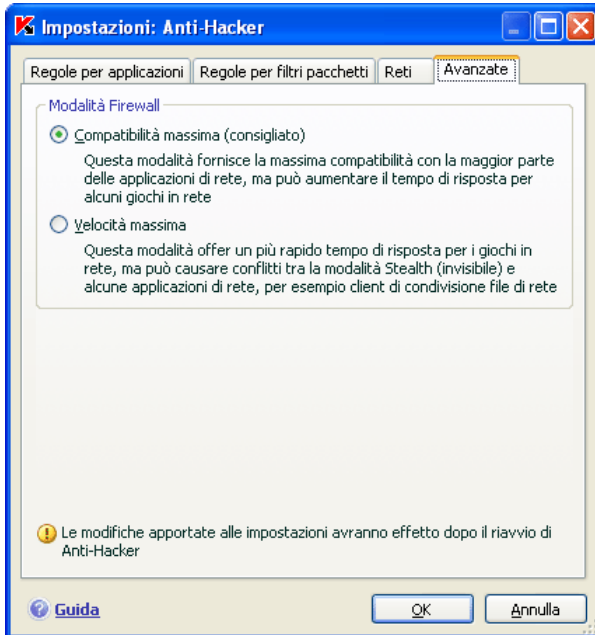


Figura 49. Selezione di una modalità Anti-Hacker

**Compatibilità massima**– il Firewall garantisce che Anti-Hacker operi in modo ottimale con programmi che stabiliscono più connessioni di rete, ad esempio i client di rete che condividono i file. Questa modalità tuttavia può comportare un rallentamento del tempo di reazione nei giochi in rete. In tal caso, si consiglia di utilizzare l'impostazione Massima velocità.

**Velocità massima**– il Firewall garantisce i tempi di reazione migliori possibile durante i giochi in rete. Tuttavia, i client di rete di condivisione file e le altre applicazioni di rete potrebbero entrare in conflitto in questa modalità. Per risolvere il problema, disabilitare la modalità Mascheramento.

*Per selezionare una modalità Firewall:*

1. Aprire la finestra delle impostazioni dell'applicazione e selezionare **Anti-Hacker** in **Protezione**.
2. Fare clic su **Impostazioni** nella sezione Abilita Firewall della finestra delle impostazioni di Anti-Hacker.
3. Selezionare la scheda **Avanzate** nella finestra che si apre e selezionare la modalità desiderata, Compatibilità massima o Velocità massima.



Le modifiche alle impostazioni del Firewall non saranno effettive fino a dopo il riavvio di Anti-Hacker.

## 12.8. Configurazione del Sistema di rilevamento intrusioni

Tutti gli attacchi di rete correntemente noti che potrebbero mettere in pericolo il computer dell'utente sono presenti nell'elenco delle minacce, che viene aggiornato insieme a quello dei virus. Per impostazione predefinita, Kaspersky Anti-Virus non aggiorna il database degli attacchi (vedere 16.4.2 a pag. 229).

Il Sistema di rilevamento intrusioni rileva l'attività di rete tipica degli attacchi di rete, e se individua un tentativo di attacco al computer, blocca tutta l'attività di rete tra il computer remoto ed il computer dell'utente per un'ora.

*È possibile configurare il Sistema di rilevamento intrusioni. Per fare ciò:*

1. Aprire la finestra delle impostazioni dell'applicazione e selezionare **Anti-Hacker** in **Protezione**.
2. Fare clic su **Impostazioni** nella sezione **Sistema rilevamento intrusioni**.
3. Nella finestra che si apre (vedere Figura 50), decidere se bloccare il computer da cui proviene l'attacco e, se sì, per quanto tempo. Per impostazione predefinita, il computer viene bloccato per 60 minuti. Il tempo di blocco può essere aumentato o diminuito modificando il valore nel campo accanto a  **Blocca il computer che attacca per ... min.** Per smettere di bloccare il traffico proveniente da un computer che attacca la macchina dell'utente, deselezionare la casella.

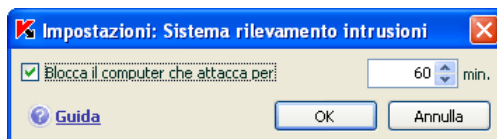


Figura 50. Configurazione del tempo di blocco di computer pirata

## 12.9. Elenco degli attacchi di rete intercettati

Esistono attualmente svariati attacchi di rete che sfruttano le vulnerabilità dei sistemi operativi e di altri software, sistemi o altro, installati sul computer. I pirati informatici perfezionano continuamente i metodi di attacco, imparando come trafugare informazioni confidenziali, provocare anomalie di funzionamento del sistema o “impadronirsi” del computer per utilizzarlo come elemento di una rete fantasma da cui lanciare nuovi attacchi.

Per garantire la sicurezza del computer, occorre conoscere i tipi di attacchi possibili. Gli attacchi di rete noti possono essere suddivisi in tre categorie principali:

- **Scansione porte** – non si tratta di un attacco vero e proprio, ma solitamente precede un attacco, in quanto è uno dei modi più comuni per ottenere informazioni su un computer remoto. Le porte UDP/TCP utilizzate dai programmi di rete vengono esaminate per scoprire il loro stato (se siano cioè aperte o chiuse).

Dalla scansione delle porte, un pirata è in grado di capire quali tipi di attacco funzioneranno sul sistema e quali no. Inoltre, le informazioni ottenute dalla scansione consentono di identificare il sistema operativo utilizzato dal computer remoto. Questo, a sua volta, circoscrive ulteriormente il numero degli attacchi possibili e, di conseguenza, il tempo necessario a lanciarli. Inoltre consente al pirata di sfruttare le vulnerabilità specifiche del sistema operativo.

- **Attacchi DoS (Denial of Service)** – in seguito a questi attacchi il sistema attaccato diventa instabile o completamente inoperativo. Questi attacchi possono danneggiare le risorse o corrompere le risorse informative, lasciandole inutilizzabili.

Esistono due tipi principali di attacchi DoS:

- L’invio al computer attaccato di pacchetti appositamente creati che tale computer non si aspetta, per provocare il riavvio o l’arresto del sistema.
- L’invio al computer attaccato di numerosi pacchetti in un lasso temporale estremamente breve che non consente al computer di elaborarli, esaurendo le risorse di sistema.

Quelli descritti di seguito sono esempi comuni di attacchi di questo tipo:

- *Ping of death* consiste nell'invio di un pacchetto ICMP di dimensioni superiori a quelle massime di 64 KB. Questo attacco può mandare in crash certi sistemi operativi.
  - *Land* consiste nell'invio di una richiesta ad una porta aperta sul computer per stabilire una connessione. Questo manda il computer in un ciclo che intensifica il carico sul processore e può terminare con il crash di alcuni sistemi operativi.
  - *ICMP Flood* consiste nell'invio di un elevato numero di pacchetti ICMP al computer. L'attacco fa sì che il computer sia costretto a rispondere a ogni pacchetto in entrata, e questo sovraccarica notevolmente il processore.
  - *SYN Flood* consiste nell'invio di un elevato numero di query al computer per stabilire una finta connessione. Il sistema riserva determinate risorse a ciascuna di queste connessioni, che prosciugano completamente le risorse di sistema e il computer smette di reagire ad altri tentativi di connessione.
- **Attacchi intrusivi**, che hanno lo scopo di controllare completamente il computer. Questo è il tipo di attacco più pericoloso, in quanto se ha esito positivo, determina il controllo completo del computer da parte dell'hacker.

I pirati utilizzano questo tipo di attacco per ottenere informazioni confidenziali da un computer remoto (per esempio, numeri di carte di credito o password) o per utilizzarne in seguito le risorse per fini illeciti (ad, esempio, il sistema catturato sarà usato come elemento di reti fantasma o come piattaforma per nuovi attacchi).

Questo gruppo contiene inoltre più diversi tipi attacchi di ogni altro. Essi possono essere suddivisi in tre sottogruppi a seconda del sistema operativo: attacchi a Microsoft Windows, attacchi a Unix e attacchi efficaci con entrambi i sistemi operativi.

I tipi di attacco più comuni che utilizzano strumenti del sistema operativo sono:

- *Attacchi di sovraccarico del buffer* – tipo di vulnerabilità del software che emerge a causa di controllo assente o insufficiente nel gestire grandi quantità di dati. È uno dei tipi di vulnerabilità note da più tempo e il più facile da utilizzare.
- *Attacchi attraverso le stringhe di formato* – tipo di vulnerabilità nel software che deriva 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, un pirata può ottenere il controllo completo del sistema servendosi di query create con una tecnica speciale.

IL Sistema di rilevamento intrusioni analizza e blocca automaticamente i tentativi di sfruttare le vulnerabilità dei più comuni strumenti di rete (FTP, POP3, IMAP) eseguiti sul computer dell'utente.

Gli *attacchi a Microsoft Windows* sono basati sullo sfruttamento delle vulnerabilità nel software installato sul computer (per esempio programmi come Microsoft SQL Server, Microsoft Internet Explorer, Messenger, e componenti di sistema ai quali è possibile accedere attraverso la rete – DCom, SMB, Wins, LSASS, IIS5).

Anti-Hacker protegge il computer dagli attacchi che utilizzano le seguenti vulnerabilità di sistema note (questa lista di vulnerabilità è citata con il sistema di numerazione del database di Microsoft):

- (**MS03-026**) DCOM RPC Vulnerability(Lovesan worm)
- (**MS03-043**) Microsoft Messenger Service Buffer Overrun
- (**MS03-051**) Microsoft FrontPage 2000 Server Extensions Buffer Overflow
- (**MS04-007**) Microsoft Windows ASN.1 Vulnerability
- (**MS04-031**) Microsoft NetDDE Service Unauthenticated Remote Buffer Overflow
- (**MS04-032**) Microsoft Windows XP Metafile (.emf) Heap Overflow
- (**MS05-011**) Microsoft Windows SMB Client Transaction Response Handling
- (**MS05-017**) Microsoft Windows Message Queuing Buffer Overflow Vulnerability
- (**MS05-039**) Microsoft Windows Plug-and-Play Service Remote Overflow
- (**MS04-045**) Microsoft Windows Internet Naming Service (WINS) Remote Heap Overflow
- (**MS05-051**) Microsoft Windows Distributed Transaction Coordinator Memory Modification

Vi sono inoltre casi isolati di attacchi intrusivi effettuati utilizzando vari script nocivi, inclusi gli script elaborati da Microsoft Internet Explorer e dai worm di tipo Helkern. Questo tipo di attacco consiste essenzialmente nell'invio di speciali pacchetti UDP a un computer remoto in grado di eseguire il codice nocivo.

Si tenga presente che, quando si è collegati alla rete, il computer è costantemente a rischio di attacchi degli hacker. Per garantire la sicurezza del computer, abilitare Anti-Hacker quando si usa Internet ed aggiornare regolarmente l'elenco degli attacchi degli hacker a intervalli regolari (vedere 16.4.2 a pag. 229).

## 12.10. Blocco e autorizzazione di attività di rete

Se il livello di sicurezza del Firewall è impostato sulla **modalità Apprendimento**, ad ogni tentativo di connessione di rete che non è provvista di una regola compare un apposito avviso sullo schermo.

Per esempio, dopo aver aperto Microsoft Outlook, il programma scarica la posta da un server remoto di Exchange. Per visualizzare la casella di posta in arrivo, il programma si connette al server di posta. Anti-Hacker rileva sempre questo tipo di attività di rete. Sullo schermo compare un messaggio (vedere Figura 51) contenente:

- *Descrizione dell'attività* – nome dell'applicazione ed una breve descrizione della connessione che viene avviata, che include solitamente il tipo di connessione, la porta locale dalla quale viene inizializzata, la porta remota e l'indirizzo al quale avviene il collegamento. Fare clic ovunque nell'area per ottenere informazioni dettagliate sulla connessione, il processo che l'ha avviata ed il distributore dell'applicazione.
- *Azione* – serie di operazioni che Anti-Hacker eseguirà relativamente all'attività di rete rilevata.



Figura 51. Notifica degli attacchi di rete

Consultare con attenzione le informazioni sull'attività di rete e solo dopo selezionare le azioni di Anti-Hacker. Si raccomanda di decidere tenendo conto dei seguenti suggerimenti:

1. Prima di qualsiasi cosa, decidere se autorizzare o bloccare l'attività di rete. È possibile che nella situazione specifica una serie di regole già create per l'applicazione o pacchetto possa essere di aiuto (supponendo che sia stata creata). A tal fine, usare il collegamento **Modifica regola** . A questo punto si apre una finestra con una lista completa di regole create per l'applicazione o il pacchetto di dati.
2. Decidere se eseguire l'azione una sola volta o automaticamente ogni volta che viene intercettata questa attività.

*Per eseguire l'azione solo questa volta:*

deselezionare  **Crea una regola** e fare clic sul pulsante con il nome dell'azione, per esempio **Permetti**.

*Per eseguire automaticamente l'azione selezionata ogni volta che questa attività viene iniziata sul computer:*

1. Verificare che la casella  **Crea una regola** sia selezionata.
2. Selezionare il tipo di attività a cui si intende applicare l'azione dall'elenco a discesa nella sezione **Azione**:
  - **Tutta l'attività** – tutta l'attività di rete lanciata da questa applicazione.
  - **Personalizzata** – una singola attività che deve essere definita nella finestra di dialogo delle regole (vedere 12.2.1 a pag. 156).

- **<Template>** – nome del modello che include la serie di regole tipiche dell'attività di rete del programma. Questo tipo di attività compare sulla lista se Kaspersky Anti-Virus for Windows Workstations include un modello appropriato per l'applicazione che ha avviato l'attività di rete (vedere 12.2.2 a pag. 157). In tal caso non è necessario personalizzare le attività da autorizzare o da bloccare. È sufficiente usare il modello per creare automaticamente una serie di regole per l'applicazione.

3. Fare clic sul pulsante con il nome dell'azione (**Permetti** o **Blocca**).

Ricordare che la regola creata sarà usata solo quando tutti i parametri della connessione corrispondono a quelli indicati. Per esempio, questa regola non viene applicata a connessioni stabilite da una porta locale diversa.

Per non disattivare la visualizzazione dei messaggi di Anti-Hacker quando le applicazioni tentano di stabilire una connessione di rete, fare clic su Disabilita modalità Training. Anti-Hacker passa alla modalità Autorizza tutto, che autorizza tutte le connessioni di rete tranne quelle esplicitamente non autorizzate dalle regole.

---

# CAPITOLO 13. PROTEZIONE DALLA POSTA INDESIDERATA

Il componente di Kaspersky Anti-Virus for Windows Workstations che rileva la posta spam, la elabora secondo un insieme di regole prestabilite e risparmia tempo quando si utilizza la posta elettronica è denominato *Anti-Spam*.

Anti-Spam usa il seguente metodo per determinare se un messaggio è posta spam o no:

1. L'indirizzo del mittente viene confrontato con le liste bianche e le liste nere degli indirizzi.
  - Se l'indirizzo del mittente è sulla lista bianca, al messaggio viene assegnato lo stato *non spam*.
  - Se l'indirizzo del mittente è sulla lista nera, al messaggio viene assegnato lo stato *spam*. L'ulteriore elaborazione dipende dall'azione selezionata (vedere 13.3.7 a pag. 194).
2. Se l'indirizzo del mittente non è rilevato su una lista bianca o nera, il messaggio viene analizzato utilizzando la tecnologia PDB (vedere 13.3.2 a pag. 185).
3. Anti-Spam esamina il testo del messaggio in dettaglio e lo analizza confrontandolo con le righe della lista nera o bianca.
  - Se il testo del messaggio contiene righe dalla lista bianca delle righe, ad esso viene assegnato lo stato *non spam*.
  - In presenza di frasi contenute nella lista nera, il messaggio è classificato come *spam*. L'ulteriore elaborazione dipende dall'azione specificata.
4. Se il messaggio non contiene frasi presenti nella lista bianca o nella lista nera, viene sottoposto a scansione anti-phishing. Se il testo nel messaggio contiene un indirizzo presente nel database anti-phishing, il messaggio è classificato come *spam*. L'ulteriore elaborazione dipende dall'azione specificata.
5. Se il messaggio non contiene righe di phishing, viene sottoposto all'analisi anti-spam utilizzando tecnologie speciali:
  - Analisi grafica mediante tecnologia GSG



- Analisi del testo mediante l'algoritmo iBayes per il riconoscimento della spam.
6. Infine, il messaggio viene esaminato per individuare ulteriori fattori di filtraggio anti-spam (vedere 13.3.5 a pag. 192) impostati dall'utente durante l'installazione di Anti-Spam. Questa fase potrebbe includere l'analisi dei tag HTML, delle dimensioni dei caratteri o degli eventuali caratteri nascosti.

Ciascuna di queste fasi dell'analisi può essere abilitata o disabilitata.

Sono disponibili plug-in Anti-Spam per i seguenti client di posta:

- Microsoft Outlook (vedere 13.3.8 a pag. 195)
- Microsoft Outlook Express (Windows Mail) (vedere 13.3.9 a pag. 198)
- The Bat! (vedere 13.3.10 a pag. 199)

**Questa versione di Kaspersky Anti-Virus non supporta un plug-in Anti-Hacker per Microsoft Office Outlook su Microsoft Windows 98.**

Il pannello delle attività dei client Microsoft Office Outlook e Outlook Express (Windows Mail) è dotato di due pulsanti, **Spam** e **Non spam**, che configurano Anti-Spam per rilevare la spam direttamente nella casella di posta. The Bat! non offre tali pulsanti: il programma può essere addestrato utilizzando elementi speciali come **Mark as spam** e **Mark as NOT spam** sul menu **Special**. Inoltre, a tutte le impostazioni del client di posta vengono sono aggiunti speciali parametri di elaborazione (vedere 13.3.1 a pag. 184) per lo spam.

Anti-Spam utilizza uno speciale algoritmo di autoaddestramento iBayes, che nel tempo consente al componente di distinguere più precisamente tra *spam* e *non spam*. L'origine dei dati per l'algoritmo è costituita dai contenuti del messaggio di posta.

Si presentano situazioni in cui iBayes non è in grado di classificare con precisione un determinato messaggio come spam o non spam. Tali messaggi vengono contrassegnati come *probabile spam*.

Per ridurre il numero di messaggi classificati come probabile spam, si consiglia di addestrare ulteriormente Anti-Spam (vedere 13.2 a pag. 179) su tali messaggi. A tal fine, occorre specificare quali di questi messaggi devono essere classificati come *spam* e quali come *non spam*.

I messaggi considerati *spam* o *probabile spam* vengono modificati: Le diciture **[!! SPAM]** o **[?? Probabile Spam]**, vengono aggiunte rispettivamente alla riga dell'oggetto.

Le regole per l'elaborazione della spam o della probabile spam per Microsoft Office Outlook, Microsoft Outlook Express (Windows Mail), o The Bat! vengono specificate in speciali componenti plug-in all'interno del client di posta stesso.

Per altri client di posta, è possibile configurare regole di filtraggio che ricerchino la riga d'oggetto modificata contenete le diciture **[!! SPAM]** o **[?? Probabile Spam]** e spostino i risultati della ricerca in una cartella apposita. Per ulteriori informazioni sul meccanismo di filtraggio, consultare la documentazione del client di posta.

## 13.1. Selezione di un livello di sensibilità per Anti-Spam

Kaspersky Anti-Virus for Windows Workstations protegge dalla spam a uno dei seguenti livelli (vedere Figura 52):

**Blocca tutto** – il livello di sensibilità più severo, in base al quale solo i messaggi contenenti frasi comprese nella lista bianca delle frasi (vedere 13.3.4.1 a pag. 188) e provenienti dai mittenti elencati sulla lista bianca vengono accettati: tutto il resto viene considerato spam. A questo livello, i messaggi vengono esaminati solo a fronte della lista bianca. Tutte le altre funzioni sono disabilitate.

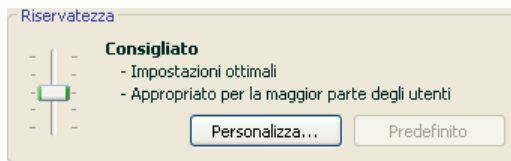


Figura 52. Selezione di un livello di protezione di Anti-Spam

**Alto** – un livello severo che, quando attivato, aumenta la probabilità che qualche messaggio non spam sia marcato come *spam*. A questo livello, il messaggio viene analizzato a fronte delle liste bianca e nera, utilizzando anche le tecnologie PDB e GSG e l'algoritmo iBayes (vedere 13.3.2 a pag. 185).

Questo livello deve essere adottato solo nei casi in cui la probabilità che l'indirizzo del destinatario sia ignoto agli spammer è elevata, per esempio quando il destinatario non è iscritto a nessuna mailing list e non possiede un indirizzo e-mail su server gratuiti/non aziendali.

**Consigliato** – il livello con impostazioni standard per la classificazione della posta elettronica.

A questo livello è possibile che alcuni messaggi spam non siano intercettati, segnalando così un training di Anti-Spam insufficiente. Si consiglia di effettuare un ulteriore addestramento per il modulo utilizzando la Procedura guidata di training (vedere 13.2.1 a pag. 180) o i pulsanti **Spam/Non spam** (o le corrispondenti voci di menu in the Bat!) per i messaggi classificati erroneamente.

**Basso** – il livello d'impostazione più flessibile. È consigliato agli utenti la cui corrispondenza in entrata contiene un numero significativo di parole riconosciute da Anti-Spam come spam, ma che non lo sono. Ciò può essere dovuto all'attività professionale del destinatario, che richiede per la corrispondenza con i colleghi l'uso di un linguaggio ampiamente diffuso tra gli spammer. Tutte le tecnologie di intercettazione dello spam sono utilizzate per analizzare i messaggi a questo livello.

**Consenti tutto** – il livello di sensibilità più bassa. Vengono riconosciuti come spam solo i messaggi che contengono frasi presenti nella lista nera delle frasi e i cui mittenti sono presenti nella lista nera degli indirizzi. A questo livello, i messaggi di posta vengono elaborati utilizzando la lista nera, e tutte le altre funzioni sono disabilitate.

Per impostazione predefinita, Anti-Spam è impostato al livello di sensibilità **Consigliato**. È possibile tuttavia aumentare o ridurre il livello di protezione oppure modificare le impostazioni del livello corrente.

*Per modificare il livello di protezione:*

Nella sezione Riservatezza, spostare il cursore in alto o in basso all'impostazione desiderata. Regolando il livello di sensibilità, si definisce la correlazione tra i fattori spam, probabile spam e posta accettata (vedere 13.3.3 a pag. 186).

*Per modificare le impostazioni del livello corrente:*

Aprire la finestra delle impostazioni dell'applicazione e fare clic su **Anti-Spam** per visualizzare le impostazioni del componente. Fare clic sul pulsante **Personalizza** nella sezione Riservatezza. Modificare il fattore di spam nella finestra che si apre e fare clic su **OK**.

Il nome del livello di sicurezza passa a **Impostazioni personalizzate**.

## 13.2. Addestramento di Anti-Spam

Anti-Spam è dotato di un database preinstallato di messaggi di posta contenente cinquanta esempi di spam. Si consiglia tuttavia di sottoporre il modulo Anti-Spam ad ulteriore addestramento in base ai propri messaggi.

Esistono diversi approcci di addestramento di Anti-Spam:

- Tramite la procedura guidata di apprendimento (vedere 13.2.1 a pag. 180)
- Addestrare Anti-Spam con i messaggi in uscita (vedere 13.2.2 a pag. 181)

- Effettuando l'addestramento direttamente mentre si lavora con la posta elettronica (vedere 13.2.3 a pag. 181) utilizzando gli speciali pulsanti nel pannello strumenti o le voci di menu del client di posta
- Addestramento nei rapporti di Anti-Spam (vedere 13.2.4 a pag. 182)

Il metodo migliore è quello di utilizzare la procedura guidata di training appena s'inizia ad utilizzare Anti-Spam, dato che può addestrare Anti-Spam su un gran numero di e-mail.

Si noti che non è possibile effettuare il training di Anti-Spam con oltre 50 messaggi per cartella. In presenza di cartelle contenenti un numero superiore di messaggi, il programma ne utilizzerà solo 50 ai fini del training.

L'addestramento supplementare utilizzando gli speciali pulsanti nell'interfaccia del client di posta è preferibile quando si sceglie di lavorare direttamente sui messaggi.

### 13.2.1. Procedura di apprendimento guidato

La procedura di apprendimento guidato consente di addestrare Anti-Spam indicando le cartelle di posta che contengono spam e i messaggi accettabili.

*Per avviare la procedura di apprendimento guidato:*

1. Aprire la finestra delle impostazioni dell'applicazione e selezionare **Anti-Spam** in **Protezione**.
2. Fare clic sul pulsante **Apprendimento guidato** nella sezione Preparazione della finestra delle impostazioni.

La procedura di apprendimento guidato conduce l'utente passo passo nell'addestramento di Anti-Spam. Utilizzare i pulsanti **Indietro** e **Avanti** per navigare tra i passaggi.

Il punto uno della procedura guidata di training consiste nel selezionare le cartelle contenenti corrispondenza valida. In questa fase, l'utente deve solo selezionare le cartelle i cui contenuti ritiene completamente attendibili.

Il punto due della procedura guidata di training consiste nel selezionare le cartelle contenenti spam. Saltare questo passo se il client di posta utilizzato non dispone di cartelle spam.

Il punto tre è l'inizio dell'addestramento automatico di Anti-Spam sulle cartelle selezionate. I messaggi presenti in queste cartelle costituiranno il database di Anti-Spam. I mittenti dei messaggi validi sono automaticamente aggiunti alla lista bianca degli indirizzi.

Durante il punto quattro, i risultati del training vengono salvati utilizzando uno dei seguenti metodi: Aggiungere i risultati dell'addestramento al database corrente di Anti-Spam, oppure sostituire il database corrente con i risultati dell'addestramento. Si tenga presente che, affinché l'algoritmo iBayes funzioni correttamente, è necessario addestrare il programma su un minimo di 50 messaggi accettabili e 50 messaggi di spam.

Per risparmiare tempo, la procedura guidata di training limita l'addestramento a 50 messaggi tra quelli presenti in ciascuna cartella selezionata.

## 13.2.2. Addestramento con i messaggi in uscita

È possibile addestrare Anti-Spam con i messaggi in uscita direttamente dal client di posta. La lista bianca degli indirizzi di Anti-Spam viene integrata con i indirizzi dei messaggi in uscita. Per il training si usano solo i primi cinquanta messaggi, dopodiché è completato.

*Per addestrare Anti-Spam con i messaggi in uscita:*

1. Aprire la finestra delle impostazioni dell'applicazione e selezionare **Anti-Spam** in **Protezione**.
2. Selezionare  **Apprendimento con i messaggi di posta in uscita** nella sezione **Preparazione**.

### Attenzione!

Anti-Spam effettuerà il training solo sulle e-mail in uscita inviate attraverso il protocollo MAPI se si seleziona l'opzione  **Scansione all'invio** nel plug-in di Microsoft Office Outlook Anti-Virus posta (vedere 13.3.8 a pag. 195).

## 13.2.3. Training mediante il client di posta

Per addestrare il programma direttamente dalla casella di posta, è possibile utilizzare gli appositi pulsanti sul pannello degli strumenti del client.

Al momento dell'installazione sul computer, Anti-Spam installa i plug-in per i seguenti client di posta:

- Microsoft Outlook
- Outlook Express (Windows Mail)
- The Bat!

Ad esempio, la barra delle attività di Outlook ha due pulsanti, **Spam** e **Non Spam**, ed una scheda di impostazioni **Kaspersky Anti-Spam** (vedere 13.3.8 a pag. 195) nel menu della finestra di dialogo Opzioni (voce di menu **Strumenti**→**Opzioni**). Outlook Express, oltre ai pulsanti **Spam** e **Non Spam**, aggiunge un pulsante **Configurazione** al riquadro delle attività che apre una finestra con azioni (vedere 13.3.9 a pag. 198) quando viene rilevata posta spam. The Bat! non è dotato di pulsanti simili, benché il programma possa essere addestrato utilizzando elementi speciali come **Mark as spam (segna come spam)** e **Mark as NOT spam (segna come non spam)** sul menu **Special (speciale)**.

Se si decide che il messaggio attualmente aperto è da considerare spam, fare clic sul pulsante **Spam**. Se il messaggio non è da considerare spam, fare clic su **Non spam**. Anti-Spam esegue quindi il training utilizzando la posta elettronica. Se si selezionano diversi messaggi di posta elettronica, verranno tutti utilizzati per il training.

#### Attenzione!

Nei casi in cui si abbia necessità di selezionare immediatamente più messaggi, o si sia assolutamente certi che una determinata cartella contiene solo messaggi appartenenti a un unico gruppo (spam o non spam), è possibile adottare un approccio globale al training tramite la Procedura guidata di training (vedere 13.2.1 a pag. 180).

## 13.2.4. Training sui rapporti di Anti-Spam

Esiste inoltre l'opzione di addestrare Anti-Spam attraverso i rapporti.

*Per visualizzare i rapporti del componente:*

1. Selezionare il componente **Anti-Spam** nella sezione **Protezione** della finestra principale del programma.
2. Fare clic sulla sezione **Statistiche** (vedere Figura 53).

In base ai rapporti del componente è possibile trarre conclusioni sull'accuratezza della configurazione e, se necessario, apportare determinate correzioni ad Anti-Spam.

*Per segnare una determinato messaggio come spam o non spam:*

1. Selezionarlo dalla lista dei rapporti nella scheda **Eventi** e utilizzare il pulsante **Azioni**.
2. Selezionare una delle quattro opzioni seguenti:
  - **Contrassegna come spam**
  - **Contrassegna come non spam**

- **Aggiungi all'elenco consentiti**
- **Aggiungi all'elenco bloccati**

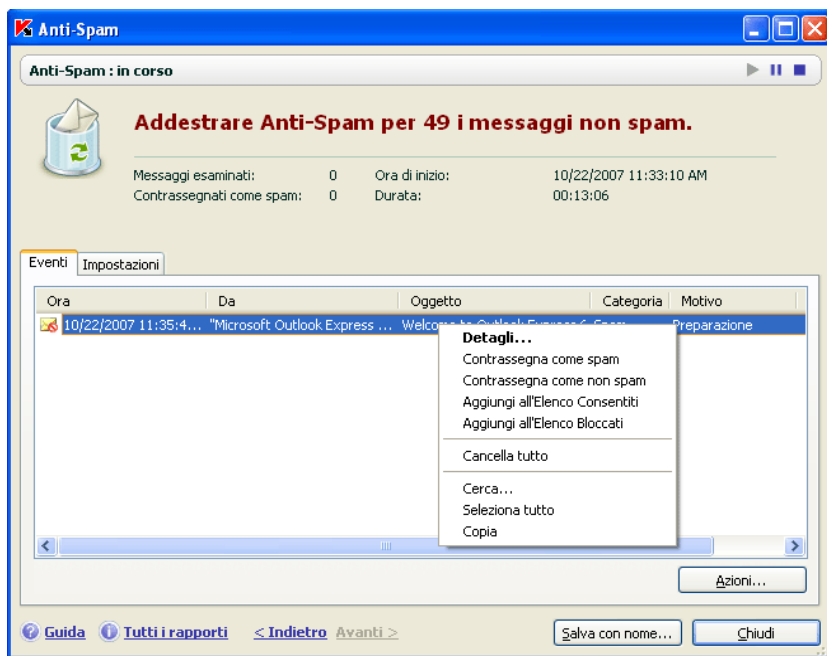


Figura 53. Addestramento di Anti-Spam dai rapporti

Anti-Spam esegue un ulteriore addestramento sulla base di questo messaggio.

### 13.3. Configurazione di Anti-Spam

La configurazione di precisione di Anti-Spam è essenziale ai fini di un'efficace intercettazione dello spam. Tutte le impostazioni per il funzionamento del componente si trovano nella finestra delle impostazioni di Kaspersky Anti-Virus for Windows Workstations e consentono di:

- Determinare i dettagli di funzionamento di Anti-Spam (vedere 13.3.1 a pag. 184)
- Scegliere la tecnologia di filtraggio messaggi da utilizzare (vedere 13.3.2 a pag. 185)

- Regolare la precisione di riconoscimento della spam e della possibile spam (vedere 13.3.3 a pag. 186)
- Creare liste bianche e liste nere di mittenti e frasi chiave (vedere 13.3.4 a pag. 187)
- Configurare ulteriori funzioni di filtraggio spam (vedere 13.3.5 a pag. 192)
- Ridurre al massimo la quantità di spam nella cassetta di posta in arrivo visualizzandola in anteprima in Mail dispatcher (vedere 13.3.6 a pag. 193)

Le seguenti sezioni esaminano in dettaglio queste impostazioni.

### 13.3.1. Configurazione delle impostazioni di scansione

È possibile configurare le seguenti impostazioni di scansione:

- Inclusione o meno del traffico tramite protocolli POP3/IMAP nella scansione. Kaspersky Anti-Virus esamina per impostazione predefinita la posta su tutti questi protocolli.
- Attivazione o meno dei plug-in per Outlook, Outlook Express (Windows Mail) e The Bat!.
- Visualizzazione o meno dei messaggi via POP3 su E-mail Dispatcher (vedere 13.3.6 a pag. 193) prima di scaricarle dal server di posta nella cassetta di posta in arrivo dell'utente.

*Per configurare queste impostazioni:*

1. Aprire la finestra delle impostazioni dell'applicazione e selezionare **Anti-Spam** in **Protezione**.
2. Selezionare o deselezionare le caselle nella sezione connettività, che corrispondono alle tre opzioni discusse sopra (vedere Figura 54).
3. Se necessario modificare le impostazioni di rete.

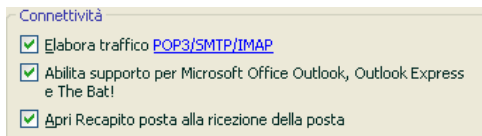


Figura 54. Configurazione delle impostazioni di scansione



**Attenzione!**

Se si utilizza Microsoft Outlook Express, riavviarlo quando si cambia lo stato della casella Attiva supporto per Outlook, Outlook Express e The Bat!

### 13.3.2. Selezione delle tecnologie di filtraggio antispam

I messaggi di posta sono sottoposti all'analisi anti-spam utilizzando tecnologie di filtro allo stato dell'arte:

- **iBayes**, basata sul teorema di Bayes, analizza il testo dei messaggi per individuare frasi ricorrenti nello spam. L'analisi utilizza le statistiche ottenute attraverso il training di Anti-Spam (vedere 13.2 a pag. 179).
- **GSG**, che analizza gli elementi grafici contenuti nei messaggi utilizzando particolari firme grafiche per rilevare lo spam nelle figure.
- **PDB**, che analizza le intestazioni dei messaggi e li classifica come spam in base a una serie di regole euristiche.

Per impostazione predefinita tali tecnologie di filtraggio sono abilitate, sottoponendo i messaggi a una scansione antispam più completa possibile.

*Per disabilitare una delle tecnologie di filtraggio:*

1. Aprire la finestra delle impostazioni dell'applicazione e selezionare **Anti-Spam** in **Protezione**.
2. Fare clic sul pulsante **Personalizza** nella sezione **Riservatezza** e nella finestra che si apre, selezionare la scheda **Riconoscimento spam** (vedere Figura 55).
3. Deselezionare le caselle a fianco delle tecnologie di filtraggio che non si desidera utilizzare ai fini del riconoscimento.

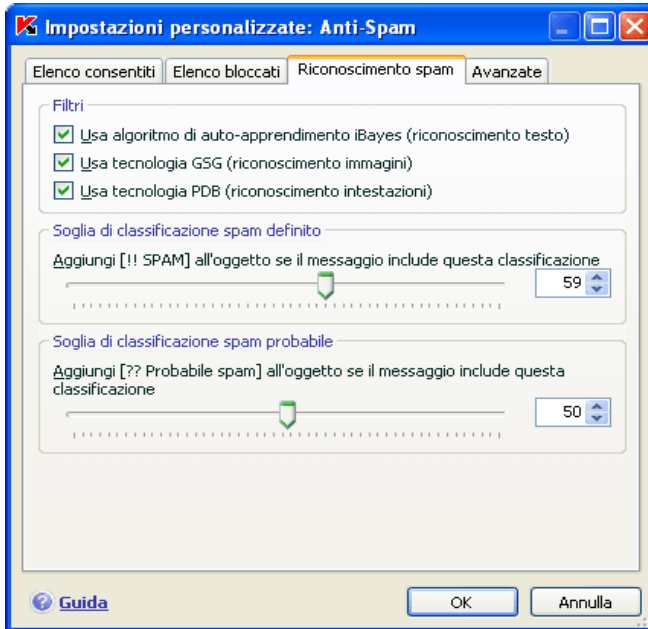


Figura 55. Configurazione delle impostazioni di riconoscimento della spam

### 13.3.3. Definizione dei fattori di spam e probabile spam

Gli esperti Kaspersky Lab hanno configurato Anti-Spam in maniera ottimale per riconoscere la spam e la probabile spam.

Il riconoscimento della spam si basa su tecnologie di filtraggio all'avanguardia (vedere 13.3.2 a pag. 185) che addestrano Anti-Spam all'identificazione della spam e della probabile spam e non spam con un elevato grado di precisione utilizzando i messaggi presenti nella casella della posta in arrivo.

Il training di Anti-Spam avviene utilizzando la procedura di Apprendimento guidato e i clienti di posta. Durante l'addestramento, ad ogni singolo elemento dei messaggi accettati o della spam viene assegnato un fattore. Quando un messaggio entra nella casella della posta in arrivo, Anti-Spam lo esamina con iBayes cercando eventuali elementi di spam e di messaggi accettati. I fattori di ciascun elemento vengono sommati ottenendo un *fattore di spam* ed un *fattore di posta accettata*.

Il fattore di probabile spam definisce la probabilità con cui il messaggio sarà classificato come potenziale spam. Utilizzando il livello **Consigliato**, ogni messaggio ha una possibilità compresa tra il 50% e il 59% di essere considerato *potenziale spam*. La posta accettabile è quella che, dopo essere stata esaminata, ha un fattore di spam inferiore al 50%.

Il fattore di spam determina la probabilità con la quale Anti-Spam classifica un messaggio come spam. Qualsiasi messaggio con probabilità superiori a quella sopra indicata saranno classificate come spam. Il fattore di spam predefinito è 59% per il livello **Consigliato**. Ciò significa che tutti i messaggi con una probabilità superiore al 59% sono segnati come *spam*.

Complessivamente, esistono cinque livelli di sensibilità (vedere 13.1 a pag. 178), tre dei quali (**Alto**, **Consigliato** e **Basso**) sono basati sui vari valori dei fattori di spam e potenziale spam.

*È possibile modificare manualmente l'algoritmo Anti-Spam. Per fare ciò:*

1. Aprire la finestra delle impostazioni dell'applicazione e selezionare **Anti-Spam** in **Protezione**.
2. Nella sezione **Riservatezza** della parte destra della finestra, fare clic su **Personalizza**.
3. Nella finestra che si apre, regolare i fattori di spam e spam potenziale nelle relative sezioni della scheda **Riconoscimento spam** (vedere Figura 55).

### 13.3.4. Creazione manuale di liste bianche e liste nere

L'utente può creare manualmente liste bianche e liste nere utilizzando Anti-Spam con i propri messaggi di posta elettronica. Queste liste contengono informazioni sugli indirizzi che l'utente considera sicuri o spam, e varie parole chiave e frasi che identificano i messaggi come spam o non spam.

L'utilizzo principale delle liste di espressioni chiave, in particolare la lista bianca, è la possibilità di coordinare con i destinatari attendibili, per esempio i colleghi, firme contenenti una determinata frase. Per esempio, si può usare la firma PGP come firma della posta elettronica. È possibile utilizzare caratteri jolly nelle firme e negli indirizzi: \* e ?. L'asterisco \* rappresenta una sequenza qualsiasi di caratteri di lunghezza non definita. Il punto interrogativo rappresenta un carattere singolo qualsiasi.

Se la firma contiene asterischi e punti interrogativi, per evitare errori durante l'elaborazione da parte di Anti-Spam essi devono essere preceduti da una barra inversa. Così al posto di un solo carattere ne vengono utilizzati due: \`*` e \`?`.

### 13.3.4.1. Liste bianche di indirizzi e frasi

La lista bianca contiene frasi chiave tratte dai messaggi segnati come *non spam*, e indirizzi di mittenti affidabili dai quali non si riceve posta indesiderata. La lista bianca viene compilata manualmente, mentre l'elenco degli indirizzi dei mittenti viene creato automaticamente durante il training del componente Anti-Spam. L'elenco può essere modificato dall'utente.

*Per configurare la lista bianca:*

1. Aprire la finestra delle impostazioni dell'applicazione e selezionare **Anti-Spam** in **Protezione**.
2. Fare clic sul pulsante **Personalizza** nella parte destra della finestra delle impostazioni.
3. Aprire la scheda **Elenco consentiti** (vedere Figura 56).

La tabella è suddivisa in due sezioni: la parte superiore contiene gli indirizzi dei mittenti della posta valida, mentre quella inferiore contiene frasi chiave tratte da tali messaggi.

Per abilitare le liste bianche delle frasi e degli indirizzi durante il filtraggio anti-spam, selezionare le caselle corrispondenti nelle sezioni **Mittenti consentiti** e **Frase consentite**.

È possibile modificare le liste servendosi degli appositi pulsanti in ciascuna sezione.

È possibile assegnare alla lista degli indirizzi sia indirizzi completi sia maschere di indirizzi. Quando si immette un indirizzo, l'utilizzo della maiuscole viene ignorato. Osserviamo alcuni esempi di maschere di indirizzi:

- *ivanov@test.ru* – i messaggi provenienti da questo indirizzo saranno sempre classificati come spam;
- *\*@test.ru* – i messaggi provenienti da qualsiasi mittente all'interno del dominio *test.ru* sono considerati validi, per esempio: *petrov@test.ru*, *sidorov@test.ru*;
- *ivanov@\** – un mittente con questo nome, indipendentemente dal dominio di posta, invia sempre solo messaggi validi, per esempio: *ivanov@test.ru*, *ivanov@mail.ru*;
- *\*@test\** – i messaggi provenienti da qualsiasi mittente all'interno di un dominio che inizia per *test* sono considerati spam, per esempio: *ivanov@test.ru*, *petrov@test.com*;
- *ivan.\*@test.???* – i messaggi provenienti da un mittente il cui nome inizia per *ivan.* e il cui nome di dominio inizia per *test* e finisce con tre caratteri

qualsiasi è sempre valido, per esempio: *ivan.ivanov@test.com*, *ivan.petrov@test.org*.

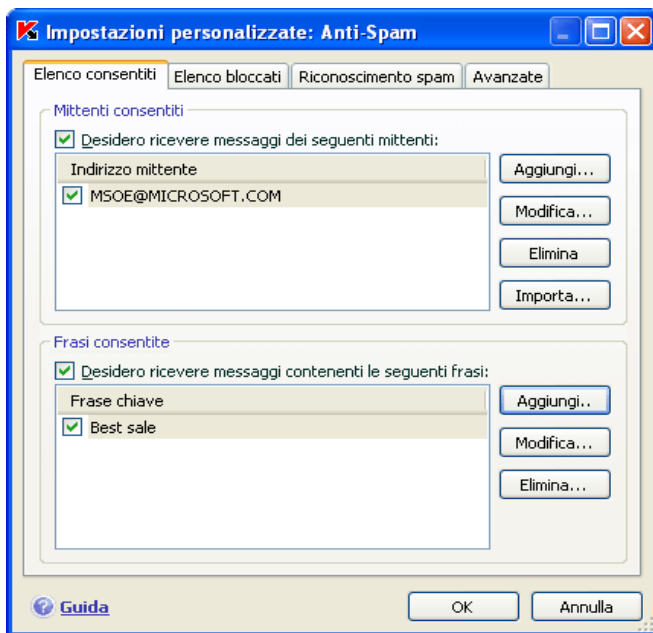


Figura 56. Configurazione delle liste bianche di indirizzi e frasi

È possibile utilizzare maschere anche per le frasi. Quando si immette una frase, l'utilizzo della maiuscole viene ignorato. Ecco alcuni esempi:

- *Caro Ivan!* – un messaggio contenente solo questo testo è considerato accettabile. Si sconsiglia di utilizzare questa frase per una lista bianca.
- *Ciao, Ivan!\** – qualsiasi messaggio che inizia con la frase *Ciao, Ivan!* è accettato.
- *Ciao, \*! \** – i messaggi che iniziano con il saluto *Ciao* e un punto esclamativo in qualsiasi punto del messaggio non saranno considerati spam.
- *\* Ivan? \** – il messaggio contiene un saluto a un utente con il nome *Ivan*, il cui nome è seguito da qualsiasi carattere e non è considerato spam.
- *\* Ivan\? \** – i messaggi contenenti la frase *Ivan?* sono accettati.

Per disabilitare l'utilizzo di un certo indirizzo o frase come attributi di posta accettabile, eliminarli con il pulsante Cancella, oppure deselezionare la casella a fianco per disabilitare l'opzione.

L'utente può scegliere di importare file in formato CSV nella lista bianca degli indirizzi.

### 13.3.4.2. Liste nere di indirizzi e frasi

La lista nera dei mittenti contiene frasi ricorrenti individuate nei messaggi classificati come *spam* nonché gli indirizzi di provenienza. L'elenco viene compilato manualmente.

Per compilare la lista nera:

1. Selezionare **Anti-Spam** nella finestra delle impostazioni di Kaspersky Anti-Virus for Windows Workstations.
2. Fare clic sul pulsante **Personalizza** nella parte destra della finestra delle impostazioni.
3. Aprire la scheda **Elenco bloccati** (vedere Figura 57).

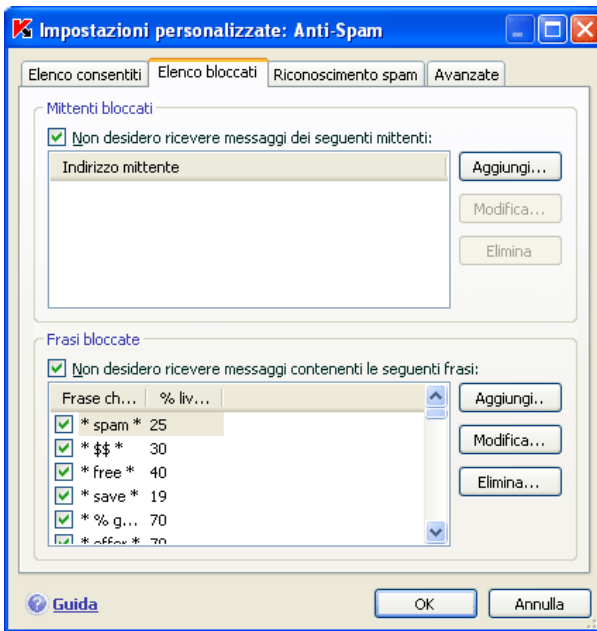


Figura 57. Configurazione delle liste nere di indirizzi e frasi

La tabella è suddivisa in due sezioni: quella superiore, contenente gli indirizzi dei mittenti di messaggi spam, e quella inferiore, contenente le frasi ricorrenti nei loro messaggi.

Per abilitare le liste nere delle frasi e degli indirizzi durante il filtraggio anti-spam, selezionare le caselle corrispondenti nelle sezioni **Mittenti bloccati** e **Frasi bloccate**.

È possibile modificare le liste servendosi degli appositi pulsanti in ciascuna sezione.

È possibile assegnare alla lista degli indirizzi sia indirizzi completi sia maschere di indirizzi. Quando si immette un indirizzo, l'utilizzo della maiuscole viene ignorato. Osserviamo alcuni esempi di maschere di indirizzi:

- *ivanov@test.ru* - i messaggi provenienti da questo indirizzo saranno sempre classificati come spam;
- *\*@test.ru* - i messaggi provenienti da qualsiasi mittente all'interno del dominio *test.ru* sono considerati validi, per esempio: *petrov@test.ru*, *sidorov@test.ru*;
- *ivanov@\** - un mittente con questo nome, indipendentemente dal dominio di posta, invia sempre solo messaggi validi, per esempio: *ivanov@test.ru*, *ivanov@mail.ru*;
- *\*@test\** - i messaggi provenienti da qualsiasi mittente all'interno di un dominio che inizia per *test* sono considerati spam, per esempio: *ivanov@test.ru*, *petrov@test.com*;
- *ivan.\*@test.???* – i messaggi provenienti da un mittente il cui nome inizia per *ivan*. e il cui nome di dominio inizia per *test* e finisce con tre caratteri qualsiasi è sempre valido, per esempio: *ivan.ivanov@test.com*, *ivan.petrov@test.org*.

È possibile utilizzare maschere anche per le frasi. Quando si immette una frase, l'utilizzo della maiuscole viene ignorato. Ecco alcuni esempi:

- *Caro Ivan!* - un messaggio contenente solo questo testo è considerato accettabile. Si sconsiglia di utilizzare questa frase per una lista bianca.
- *Ciao, Ivan!\** - qualsiasi messaggio che inizia con la frase *Ciao, Ivan!* è accettato.
- *Ciao, \*! \** – i messaggi che iniziano con il saluto *Ciao* e un punto esclamativo in qualsiasi punto del messaggio non saranno considerati spam.
- *\* Ivan? \** - il messaggio contiene un saluto a un utente con il nome *Ivan*, il cui nome è seguito da qualsiasi carattere e non è considerato spam.
- *\* Ivan!?* \* - i messaggi contenenti la frase *Ivan?* sono accettati.

Per disabilitare l'utilizzo di un certo indirizzo o frase come attributi di spam, eliminarli con il pulsante **Cancella**, oppure deselezionare la casella a fianco per disabilitare l'opzione.

## 13.3.5. Ulteriori funzioni di filtraggio antispam

Oltre alle principali funzioni utilizzate per il filtraggio dello spam (creazione di liste bianche e liste nere, analisi antiphishing, tecnologie di filtraggio), Kaspersky Anti-Virus for Windows Workstations consente di utilizzare funzioni avanzate.

Per configurare le funzioni avanzate di filtraggio antispam:

1. Aprire la finestra delle impostazioni dell'applicazione e selezionare **Anti-Spam** in **Protezione**.
2. Fare clic sul pulsante **Personalizza** nella sezione Riservatezza della finestra delle impostazioni.
3. Aprire la scheda **Avanzate** (vedere Figura 58).

Essa contiene una serie di indicatori che classificano un messaggio come probabile spam.

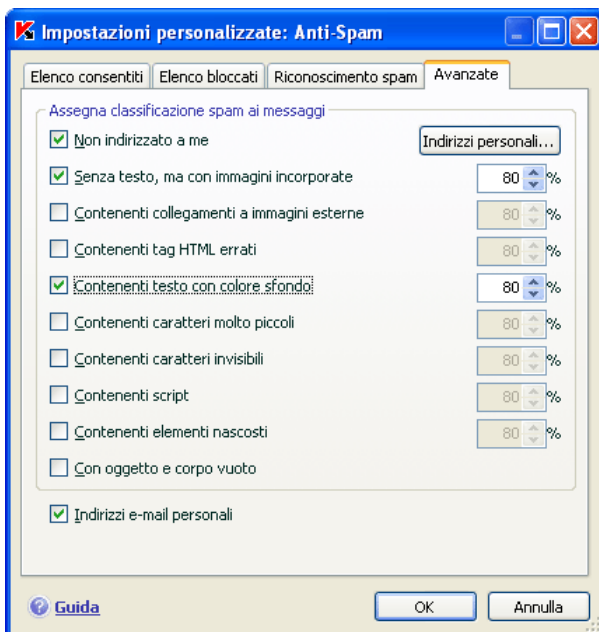


Figura 58. Impostazioni avanzate di riconoscimento dello spam



Per utilizzare eventuali indicatori supplementari di filtraggio, selezionare la casella corrispondente. Ciascuno degli indicatori richiede inoltre l'impostazione di un fattore di spam (in punti percentuali) che definisce la probabilità che un messaggio sia classificato come spam. Il valore predefinito del fattore di spam è 80%. Il messaggio sarà classificato come spam se la somma delle probabilità di tutti i fattori supplementari supera il 100%.

La spam può consistere in messaggi vuoti (nessun soggetto o corpo del messaggio), messaggi contenenti collegamenti ad immagini o con immagini incorporate, con testo dello stesso colore dello sfondo dell'immagine, o testo in caratteri molto piccoli. La spam può consistere in messaggi con caratteri invisibili (il testo è dello stesso colore dello sfondo), messaggi contenenti elementi nascosti (gli elementi non vengono visualizzati affatto) o tag html errate, come anche messaggi contenenti script (una serie di istruzioni eseguite all'apertura del messaggio).

Se si attiva un filtro per catturare i "messaggi non indirizzati a me", sarà necessario creare un elenco di indirizzi affidabili accessibile attraverso il pulsante **Indirizzi personali**. L'indirizzo del destinatario viene esaminato durante l'analisi del messaggio. Se l'indirizzo non corrisponde a nessun indirizzo nella lista, l'e-mail sarà classificata come *spam*.

È possibile creare e modificare una lista di indirizzi nella sezione **Indirizzi personali** utilizzando i pulsanti **Aggiungi**, **Modifica**, ed **Elimina**.

Per escludere i messaggi inviati nell'intranet (ad esempio, i messaggi aziendali) dalla scansione della spam, selezionare  **Indirizzi e-mail personali**. Si noti che i messaggi saranno considerati messaggi interni se tutti i computer della rete utilizzano Microsoft Office Outlook come client di posta, e se le caselle di posta dell'utente sono ubicate su un server di Exchange, o se tali server sono collegati con connettori X400. Se si desidera che Anti-Spam analizzi tali messaggi, deselezionare la casella.

### 13.3.6. Recapito posta

#### Attenzione!

Recapito posta è disponibile solo se si riceve la posta attraverso il protocollo POP3.

Recapito Posta è concepito per visualizzare la lista dei messaggi di posta sul server senza scaricarli sul computer. In tal modo è possibile rifiutare dei messaggi, risparmiando tempo e denaro e riducendo la probabilità di scaricare spam e virus sul computer.

Recapito Posta si apre se è selezionata la casella della finestra delle impostazioni di **Anti-Spam**  **Apri Recapito Posta alla ricezione della posta**.

*Per eliminare i messaggi dal server senza scaricarli sul computer:*

selezionare le caselle a sinistra dei messaggi da eliminare e scegliere il pulsante **Elimina**. I messaggi selezionati saranno eliminati dal server. Il resto della posta sarà scaricato sul computer dopo aver chiuso la finestra di Recapito Posta.

Talvolta, può essere difficile decidere se accettare o meno un determinato messaggio giudicandolo solo dal mittente e dalla riga dell'oggetto del messaggio. In tali casi, Recapito Posta offre ulteriori informazioni scaricando l'intestazione del messaggio.

*Per visualizzare le intestazioni dei messaggi:*

selezionare il messaggio dalla lista della posta in arrivo. Le intestazioni del messaggio vengono visualizzate nella parte inferiore del modulo.

Le intestazioni della posta non sono pesanti, generalmente pesano poche dozzine di byte e non possono contenere codici nocivi.

Ecco un esempio in cui la visualizzazione delle intestazioni dei messaggi può essere utile: gli spammer hanno installato un programma nocivo sul computer di un collega che invia spam con il proprio nome a tutti i destinatari nella sua rubrica del client di posta. La probabilità di trovarsi nella rubrica del collega è estremamente elevata, facendo sì che la casella della posta in arrivo si riempia di messaggi spam provenienti da lui. È impossibile stabilire a priori, sulla base del solo indirizzo del mittente, se il messaggio sia stato inviato dal collega o da uno spammer. Tuttavia, l'intestazione rivelerà questo dettaglio, consentendo di verificare chi ha inviato il messaggio, quando, e che dimensione ha, e di tracciare il percorso del messaggio dal mittente al proprio server di posta. Tutte queste informazioni dovrebbero essere contenute nelle intestazioni dei messaggi. Sarà quindi possibile decidere se sia il caso di scaricare il messaggio dal server, o se sia meglio eliminarlo.

**Nota:**

È possibile ordinare i messaggi in base a qualsiasi colonna dell'elenco di posta. Per ordinarli fare clic sull'intestazione della colonna. Le righe vengono quindi riorganizzate in ordine crescente. Per modificare l'ordine di visualizzazione, fare di nuovo clic sull'intestazione della colonna.

### 13.3.7. Azioni da eseguire sui messaggi di spam

Se dopo la scansione si scopre che un messaggio è spam o probabile spam, le fasi successive della procedura di Anti-Spam dipendono dallo status dell'oggetto e dall'azione selezionata. Per impostazione predefinita, i messaggi considerati

*spam* o *potenziale spam* vengono modificati: le diciture [!! **SPAM**] o [?? **Probabile Spam**], vengono aggiunte rispettivamente alla riga dell'oggetto.

È possibile selezionare ulteriori azioni da eseguire in caso di *spam* o *probabile spam*. In Microsoft Outlook, Outlook Express (Windows Mail) e The Bat! sono previsti speciali plug-in a tal fine. Per altri clienti di posta è possibile configurare delle regole di filtraggio.

### 13.3.8. Configurazione dell'elaborazione della spam in Microsoft Office Outlook

Ossevare che non è disponibile un plug-in antis spam per Microsoft Outlook se l'applicazione è installata in Windows 9x.

I messaggi classificati da Anti-Spam come *spam* o *probabile spam* sono marcate con i contrassegni speciali [!! **SPAM**] o [?? **Probabile Spam**] nella riga dell'**Oggetto**.

Ulteriori possibili azioni da intraprendere su *spam* e *probabile spam* in Outlook si trovano nella scheda speciale **Anti-Spam** del menu **Strumenti**→ **Opzioni** (vedere Figura 59).

Si apre automaticamente alla prima apertura del client di posta dopo l'installazione del programma e chiede se si desidera configurare l'elaborazione dello *spam*.

È possibile assegnare le seguenti regole sia ai messaggi di *spam* che a quelli di *probabile spam*:

**Sposta nella cartella** – lo *spam* è spostato nella cartella specificata.

**Copia nella cartella** – viene creata una copia dell'e-mail, che è poi trasferita nella cartella specificata. Il messaggio originale resta nella casella della posta in arrivo.

**Elimina** – elimina lo *spam* dalla casella di posta dell'utente.

**Salta** – lascia il messaggio nella casella della posta in arrivo.

A tal fine, selezionare l'opzione desiderata dall'elenco a discesa nella sezione **Spam** o **Probabile Spam**.

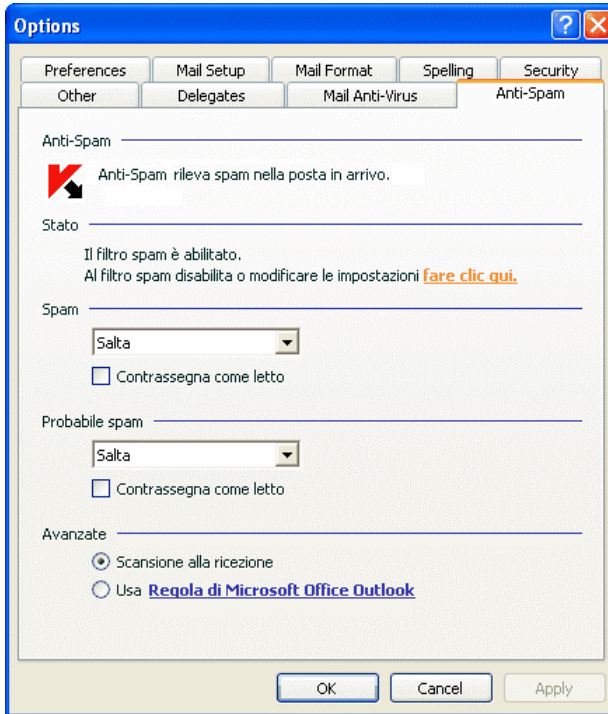


Figura 59. Configurazione dell'elaborazione dello spam in Microsoft Office Outlook

È inoltre possibile configurare Microsoft Office Outlook e Anti-Spam affinché funzionino insieme:

- Scansione alla ricezione.** Tutti i messaggi che entrano nella casella della posta in arrivo dell'utente vengono elaborati secondo le regole di Outlook. Al termine dell'elaborazione, il plug-in di Anti-Spam elabora i messaggi rimanenti che non rientrano in alcuna regola. In altre parole, i messaggi vengono elaborati secondo la priorità delle regole. Talvolta la sequenza delle priorità può essere ignorata se, per esempio, viene consegnato nella casella della posta in arrivo un gran numero di messaggi contemporaneamente. In tal caso possono verificarsi situazioni in cui le informazioni relative a un messaggio elaborato in base a una regola di Outlook vengono registrate nel rapporto di Anti-Spam come *spam*. Per evitare questo inconveniente si raccomanda di configurare il plug-in di Anti-Spam come una regola di Outlook.
- Usa regola di Microsoft Office Outlook.** Questa opzione consente di elaborare i messaggi in arrivo in base alla gerarchia delle regole di Outlook create. Una delle regole deve essere riguardare l'elaborazione dei messaggi

da parte di Anti-Spam. Si tratta della configurazione ottimale. Non ci saranno conflitti tra Outlook e il plug-in di Anti-Spam. L'unico svantaggio di questa configurazione consiste nel fatto che occorre creare ed eliminare le regole di elaborazione dello spam manualmente tramite Outlook.

A causa di un errore di Outlook XP non è possibile utilizzare il plug-in di Anti-Spam come una regola di Outlook in Microsoft Office XP se si esegue 9x/ME/NT4.

*Per creare una regola di elaborazione dello spam:*

1. Aprire Microsoft Outlook e andare a **Strumenti** → **Regole e avvisi** nel menu principale. Il comando di apertura della creazione guidata dipende dalla versione di Microsoft Office Outlook. Questo manuale d'uso descrive come creare una regola utilizzando Microsoft Office Outlook 2003.
2. Nella finestra **Regole e avvisi** che viene visualizzata, fare clic su **Nuova regola** nella scheda **Regole posta elettronica** per aprire la creazione guidata regole. La **Creazione guidata regole** guida l'utente attraverso le finestre e i passaggi che seguono:

#### Passaggio 1

È possibile scegliere di creare una regola ex novo o sulla base di un modello esistente. Selezionare **Crea nuova regola** e selezionare **Controlla messaggi in arrivo**. Fare clic sul pulsante **Avanti**.

#### Passaggio 2

Nella finestra **Condizioni da verificare**, fare clic su **Avanti** senza selezionare alcuna casella. Confermare nella finestra di dialogo che si desidera applicare questa regola a tutti i messaggi ricevuti.

#### Passaggio 3

Nella finestra di selezione delle azioni da applicare ai messaggi, selezionare  **esegui un'azione personalizzata** dall'elenco di azioni. Nella porzione inferiore della finestra, fare clic su azione personalizzata. Nella finestra che si apre, selezionare **Kaspersky Anti-Spam** dal menu a discesa e fare clic su **OK**.

#### Passaggio 4

Nella finestra di selezione delle eccezioni alla regola, fare clic su **Avanti** senza selezionare alcuna casella.

#### Passaggio 5

Nella finestra per terminare la creazione della regola, è possibile modificarne il nome (il nome predefinito è **Kaspersky Anti-Spam**).

Verificare che la casella  **Attiva regola** sia selezionata e fare clic su **Fine**.

3. La posizione predefinita per la nuova regola è in cima alla lista delle regole nella finestra **Regole posta elettronica**. Se si preferisce, è possibile spostare questa regola alla fine della lista in modo da applicarla al messaggio per ultima.

Tutti messaggi in entrata sono sottoposti a queste regole. L'ordine in cui le regole vengono applicate dipende dalla loro priorità; le regole in cima all'elenco hanno priorità maggiore rispetto a quelle sotto. La priorità di applicazione delle regole ai messaggi può essere modificata.

Se si desidera che la regola Anti-Spam non elabori ulteriormente i messaggi dopo l'applicazione di una regola, selezionare  **Arresta l'elaborazione di altre regole** nelle impostazioni delle regole (vedere punto tre della creazione di una regola).

Se si possiede una certa esperienza nella creazione di regole di elaborazione dei messaggi in Outlook, si possono creare regole personalizzate per Anti-Spam sulla base della configurazione suggerita.

### 13.3.9. Configurazione dell'elaborazione dello spam in Outlook Express (Windows Mail)

I messaggi classificati da Anti-Spam come *spam* o *probabile spam* sono marcate con i contrassegni speciali **[!! SPAM]** o **[?? Probabile Spam]** nella riga dell'**Oggetto**.

Ulteriori azioni su spam e probabile spam in Outlook Express (Windows Mail) si trovano in un'apposita finestra che si apre (vedere Figura 60) facendo clic sul pulsante **Configurazione** vicino agli altri pulsanti **Spam** e **Non Spam** sulla barra delle attività.

Si apre automaticamente alla prima apertura del client di posta dopo l'installazione del programma e chiede se si desidera configurare l'elaborazione dello spam.

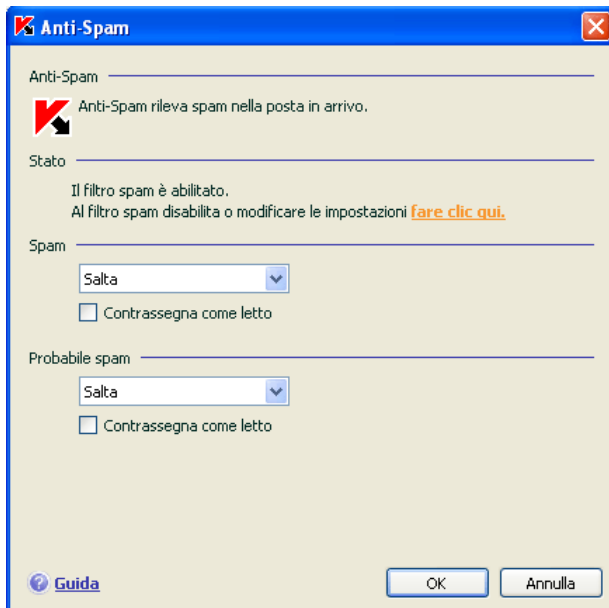


Figura 60. Configurazione dell'elaborazione dello spam in Microsoft Outlook Express

È possibile assegnare le seguenti regole sia ai messaggi di spam sia al probabile spam:

**Sposta nella cartella** – lo spam è spostato nella cartella specificata.

**Copia nella cartella** – viene creata una copia dell'e-mail, che è poi trasferita nella cartella specificata. Il messaggio originale resta nella casella della posta in arrivo.

**Elimina** – elimina lo spam dalla casella di posta dell'utente.

**Salta** – lascia il messaggio nella casella della posta in arrivo.

Per assegnare tali regole, selezionare l'opzione desiderata dall'elenco a discesa nella sezione **Spam** o **Probabile Spam**.

### 13.3.10. Configurazione dell'elaborazione della spam in The Bat!

I client di posta deve essere riavviato dopo aver abilitato/disabilitato il plug-in per Microsoft Outlook Express.

Le azioni per lo spam e il probabile spam in The Bat! sono definite mediante gli strumenti propri del client di posta.

*Per impostare le regole di protezione dello spam in The Bat!:*

1. Selezionare **Settings (Impostazioni)** dal menu **Properties (Proprietà)** del client di posta.
2. Selezionare **Anti-Spam** nella struttura ad albero delle impostazioni (vedere Figura 61).

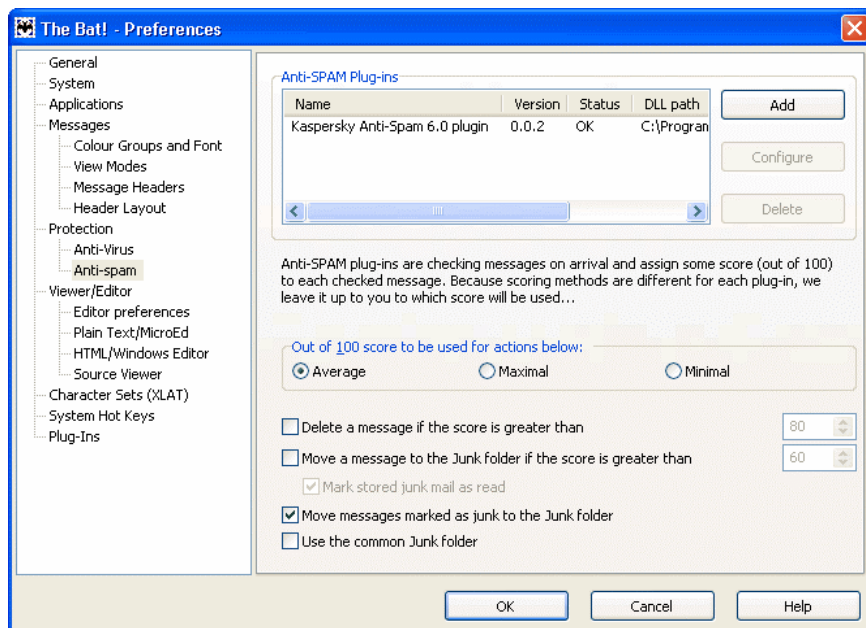


Figura 61. configurazione del riconoscimento e dell'elaborazione della spam in The Bat!

Le impostazioni di protezione antispam visualizzate valgono per tutti i moduli antispam installati nel computer che supportano The Bat!

L'utente deve impostare il livello percentuale e specificare come rispondere ai messaggi con una determinata classificazione (nel caso di Anti-Spam, alla probabilità che un messaggio sia indesiderato):

- Eliminare i messaggi con un punteggio più elevato di un determinato valore.
- Spostare i messaggi con una determinata percentuale in un'apposita cartella per lo spam.



- Trasferire nella cartella dello spam i messaggi contrassegnati da apposite intestazioni.
- Lasciare lo spam nella casella della posta in arrivo.

**Attenzione!**

Dopo aver elaborato un'e-mail, Kaspersky Anti-Virus for Windows Workstations assegna lo stato di spam o probabile spam all'e-mail in base a un fattore (vedere 13.3.3 a pag. 186) dal valore regolabile. The Bat! possiede il proprio metodo di valutazione dello spam, basato anch'esso su un fattore di spam. Per fare in modo che non ci sia discrepanza tra il fattore spam di Kaspersky Anti-Virus for Windows Workstations e quello di The Bat!, tutti i messaggi esaminati da Anti-Spam vengono contrassegnati da una percentuale in base allo stato dei messaggi utilizzato da The Bat!: *non spam*– 0%, *potenziale spam* – 50 %, *spam* – 100 %.

In tal modo, il punteggio spam in The Bat! corrisponde non al fattore di posta assegnato in Anti-Spam ma al fattore dello stato corrispondente.

Per ulteriori informazioni sulle regole di valutazione e di elaborazione dello spam, consultare la documentazione relativa a The Bat!.

---

# CAPITOLO 14. SCANSIONE ANTI-VIRUS DEL COMPUTER

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

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

## **Aree critiche**

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

## **Risorse del computer**

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

## **Oggetti di avvio**

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

Le impostazioni raccomandate per queste modalità sono quelle predefinite. È possibile modificare tali impostazioni (vedere 14.4.4 a pag. 212) o pianificare l'esecuzione delle attività (vedere 6.5 a pag. 89).

È inoltre possibile creare modalità di scansione personalizzate (vedere 14.4.3 a pag. 212) e pianificarne l'esecuzione. Per esempio, si può pianificare un'attività di scansione del database di posta per ricercare eventuali virus una volta alla settimana, oppure una scansione antivirus per la cartella **Documenti**.

È comunque possibile eseguire la scansione anti-virus di singoli oggetti (come ad esempio il disco fisso contenente programmi e giochi, l'archivio di posta elettronica prelevato al lavoro, un archivio allegato ad una e-mail, ecc.) senza dover impostare una modalità di scansione specifica. L'oggetto da esaminare


può essere selezionato dall'interfaccia di Kaspersky Anti-Virus for Windows Workstations o tramite gli strumenti standard del sistema operativo Windows Server (per esempio, dalla finestra di **Esplora risorse** o dal **Desktop**).

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

## 14.1. Gestione delle attività di scansione antivirus


La scansione antivirus può essere avviata manualmente, oppure in maniera automatica, a scadenze predefinite (vedere 6.5 a pag. 89).

*Per avviare manualmente un'attività di scansione:*


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

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

*Per sospendere un'attività:*

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

*Per terminare un'attività di scansione:*

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

## 14.2. Creazione di un elenco di oggetti da esaminare

Per visualizzare una lista di oggetti da sottoporre a scansione con una particolare attività, selezionare il nome dell'attività (per esempio, Risorse del computer) nella sezione **Scansione** della finestra principale del programma. L'elenco degli oggetti sarà visualizzato sul lato destro della finestra, sotto la barra di stato (vedere Figura 62).

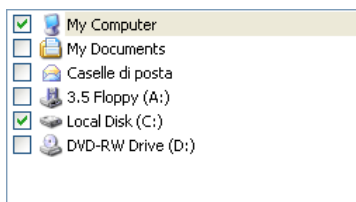


Figura 62. Elenco di oggetti su cui operare la scansione

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

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

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

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

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

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

Inoltre, l'oggetto da esaminare può essere selezionato dagli strumenti standard del sistema operativo Windows (per esempio dalla finestra di Esplora risorse o dal Desktop, ecc.) (vedere Figura 63). Selezionare l'oggetto, aprire il menù di scelta rapida di Windows facendo clic col tasto destro del mouse, e selezionare **Ricerca virus**.

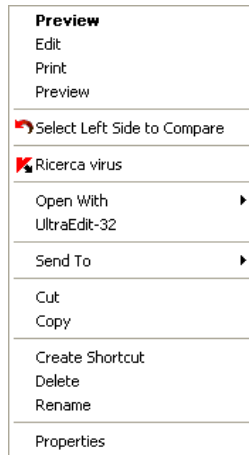


Figura 63. Scansione di oggetti attraverso il menu di scelta rapida di Windows

## 14.3. Creazione di attività di scansione antivirus

Per eseguire la scansione antivirus di oggetti presenti sul computer, è possibile utilizzare le modalità di scansione predefinite offerte dal programma o crearne di nuove. Le nuove attività di scansione vengono create utilizzando le attività esistenti come modello.

*Per creare una nuova attività di scansione antivirus:*

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

**Attenzione!**

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

La nuova attività è una copia di quella sulla quale è stata basata. Per mettere ulteriormente a punto la nuova attività è necessario creare l'elenco di oggetti su cui operare la scansione (vedere 14.2 a pag. 204), impostarne le proprietà (vedere 14.4 a pag. 206), e, se necessario, pianificarne (vedere 6.5 a pag. 89) l'esecuzione automatica.

*Per rinominare un'attività creata:*

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

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

*Per eliminare un'attività creata:*

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

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

**Attenzione!**

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

## 14.4. Configurazione delle attività di scansione antivirus

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

*Per configurare le impostazioni dell'attività:*

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

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

- selezionare il livello di sicurezza che sarà utilizzato dall'attività (vedere 14.4.1 a pag. 207)
- modificare le impostazioni avanzate:
  - definire i tipi di file da sottoporre a scansione antivirus (vedere 14.4.2 a pag. 208)
  - configurare l'avvio dell'attività utilizzando un profilo utente diverso (vedere 6.4 a pag. 88)
  - configurare le impostazioni avanzate di scansione (vedere 14.4.5 a pag. 214)
- configurare le impostazioni predefinite di scansione (vedere 14.4.3 a pag. 212)
- selezionare l'azione che il programma deve intraprendere non appena venga rilevato un oggetto infetto, o presunto tale (vedere 14.4.4 a pag. 212)
- pianificare (vedere 6.5 a pag. 89) l'avvio automatico delle attività.
- è inoltre possibile configurare le impostazioni globali (vedere 14.4.6 a pag. 216) applicabili all'esecuzione di tutte le attività.

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

## 14.4.1. Selezione di un livello di sicurezza

A ciascuna attività di scansione antivirus può essere assegnato un livello di sicurezza (vedere Figura 64):

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

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

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

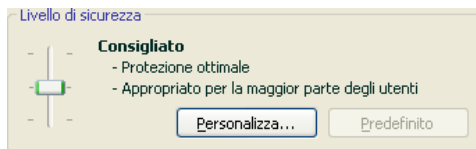


Figura 64. Selezione di un livello di sicurezza per la scansione antivirus

Per impostazione predefinita, la scansione dei file è impostata su **Consigliato**.

È possibile aumentare o diminuire la sicurezza della scansione anti-virus selezionando il livello desiderato, oppure cambiando le impostazioni del livello corrente.

*Per modificare il livello di sicurezza:*

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

Se nessuno dei livelli di sicurezza è ritenuto soddisfacente, è possibile personalizzare le impostazioni di scansione. Selezionare a tal fine il livello che più si approssima alle esigenze di sicurezza del computer, e utilizzarlo come punto di partenza per modificarne le impostazioni. In tal caso, il livello verrà rinominato come **Impostazioni personalizzate**.

*Per modificare le impostazioni di un livello di sicurezza:*

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

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

## 14.4.2. Definizione dei tipi di oggetti da sottoporre a scansione

Specificando i tipi di oggetti da analizzare, si stabilisce il formato dei file, la dimensione e i dischi che saranno sottoposti a scansione anti virus in una specifica modalità.

I tipi di file esaminati vengono definiti nella sezione **Tipi di file** (vedere Figura 65). Selezionare una delle seguenti tre opzioni:



- 🕒 **Esamina tutti i file.** Con questa opzione, tutti gli oggetti vengono sottoposti a scansione, senza eccezioni.
- 🕒 **Esamina programmi e documenti (in base al contenuto).** Selezionando questo gruppo di programmi, si sottopongono a scansione solo i file a rischio di infezione – quelli in cui si potrebbe nascondere un virus.

**Nota:**

Ci sono file nei quali non possono annidarsi virus, poiché il codice di tali file non contiene alcun elemento a cui il virus possa attaccarsi. Un esempio è costituito dai file .txt. Un esempio ne sono i file .txt.

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

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

- 🕒 **Esamina programmi e documenti (in base all'estensione).** In questo caso, il programma esaminerà solo i file potenzialmente infetti, determinandone il formato in base all'estensione. Utilizzando il link, è possibile accedere ad un elenco di estensioni file che, con questa opzione, vengono sottoposti a scansione (vedere A.1 a pagina 327).

**Suggerimento:**

Ricordare che è possibile inviare virus all'interno di file con estensione .txt che sono in realtà file eseguibili rinominati come file di testo. Selezionando l'opzione **Esamina programmi e documenti (in base all'estensione)**, tale file sarebbe escluso dalla scansione. Selezionando invece l'opzione **Esamina programmi e documenti (in base al contenuto)**, il programma analizzerà l'intestazione dei file, determinandone così la reale natura di file .exe ed esaminandolo attentamente alla ricerca di virus.

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

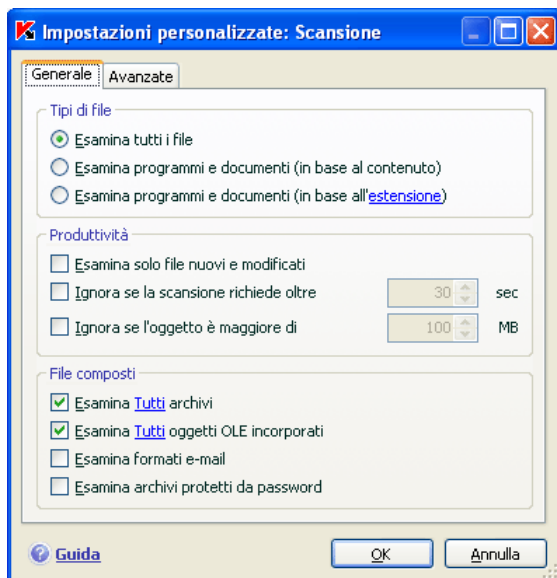


Figura 65. Configurazione delle impostazioni di scansione

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

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

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

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

**Attenzione!**

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

Per eliminare questi file compressi, fare clic sul collegamento Elimina archivi nella notifica di rilevamento di un oggetto pericoloso. Tale notifica verrà visualizzata sullo schermo dopo che il programma ha iniziato a trattare gli oggetti rilevati durante la scansione. È anche possibile eliminare gli archivi infetti manualmente.

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

Per ogni tipo di file complesso è possibile selezionare ed esaminare tutti i file o solo quelli nuovi. A tal fine, utilizzare il collegamento a fianco del nome dell'oggetto. Facendovi clic sopra con il pulsante sinistro del mouse, il suo valore cambia. Se la sezione **Produttività** è stata impostata per analizzare solo i file nuovi e modificati, non sarà possibile selezionare il tipo di file composti da esaminare.

**Esamina formati e-mail** – esamina i file in formato e-mail ed i database della posta elettronica. Se questa casella di controllo è abilitata, Kaspersky Anti-Virus disseziona il file in formato di posta elettronica ed analizza ciascun componente del messaggio (corpo, allegati, ecc.) alla ricerca di virus. Se la casella non è selezionata, il file verrà esaminato come oggetto singolo.

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

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

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

### 14.4.3. Ripristino delle impostazioni di scansione predefinite

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

*Per ripristinare le impostazioni di scansione predefinite:*

1. Selezionare il nome dell'attività nella sezione **Scansione** della finestra principale e usare il collegamento Impostazioni per aprire la finestra delle impostazioni dell'attività.
2. Fare clic sul pulsante **Predefinito** nella sezione **Livello di sicurezza**.

### 14.4.4. Selezione delle azioni da applicare agli oggetti

Se durante una scansione viene rilevato un file infetto, o presunto tale, il programma reagirà in base allo stato del file e all'azione selezionata.

All'oggetto in questione può venire assegnato uno dei seguenti stati, dopo la scansione:

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

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

*Per modificare un'azione da applicare a un oggetto:*

selezionare il nome dell'attività nella sezione **Scansione** della finestra principale del programma e usare il collegamento Impostazioni per aprire la finestra delle impostazioni dell'attività. Nelle sezioni corrispondenti vengono visualizzate tutte le potenziali reazioni (vedere Figura 66).

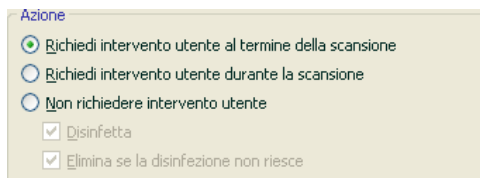


Figura 66. Selezione di un'azione per gli oggetti pericolosi

| Se l'azione selezionata è   | Se viene rilevato un oggetto nocivo o potenzialmente infetto  |
|---|---|
| <input checked="" type="radio"/> <b>Richiedi intervento utente al termine della scansione</b>                                     | Il programma non elabora gli oggetti prima della fine della scansione. Al termine del processo, una finestra di statistiche relative alla scansione appena ultimata mostrerà l'elenco degli oggetti rilevati, chiedendo all'utente se intervenire su di essi o meno.  |
| <input checked="" type="radio"/> <b>Richiedi intervento utente durante la scansione</b>   | Il programma mostrerà un messaggio di allarme contenente informazioni sul codice dannoso che ha, o che potrebbe avere, infettato un file, e offrirà all'utente la possibilità di scegliere tra una delle seguenti azioni.   |
| <input checked="" type="radio"/> <b>Non richiedere intervento utente</b>  | Il programma registra nel rapporto le informazioni relative agli oggetti rilevati, senza intervenire su di essi né notificare l'utente. Si sconsiglia di utilizzare quest'opzione, poiché gli oggetti infetti e potenzialmente infetti restano sul computer, ed è praticamente impossibile evitare l'infezione. |
| <input checked="" type="radio"/> <b>Non richiedere intervento utente</b><br><input checked="" type="checkbox"/> <b>Disinfetta</b> | Il programma cerca di trattare l'oggetto rilevato senza chiedere conferma all'utente. Se la disinfezione non riesce, il file verrà considerato <i>potenzialmente infetto</i> e spostato in Quarantena (vedere 17.1 a pag. 237). Le informazioni relative all'evento   |

| Se l'azione selezionata è   | Se viene rilevato un oggetto nocivo o potenzialmente infetto  |
|---|---|
|   | vengono registrate nel rapporto (vedere 17.3 a pag. 243). In un secondo tempo sarà possibile tentare di disinfettare l'oggetto.                 |
| <input checked="" type="radio"/> <b>Non richiedere intervento utente</b><br><input checked="" type="checkbox"/> <b>Disinfetta</b><br><input checked="" type="checkbox"/> <b>Elimina se la disinfezione non riesce</b> | Il programma cerca di trattare l'oggetto rilevato senza chiedere conferma all'utente. Se la disinfezione non riesce, l'oggetto viene eliminato. |
| <input checked="" type="radio"/> <b>Non richiedere intervento utente</b><br><input type="checkbox"/> <b>Disinfetta</b><br><input checked="" type="checkbox"/> <b>Elimina</b>  | Il programma elimina automaticamente l'oggetto rilevato.  |

Prima di disinfettare o eliminare un oggetto, Kaspersky Anti-Virus for Windows Workstations e ne crea una copia di backup e la invia nella cartella di Backup, (vedere 17.2 a pag. 241), qualora l'oggetto dovesse essere ripristinato o si presentasse successivamente la possibilità di trattarlo.

## 14.4.5. Ulteriori impostazioni di scansione antivirus

Oltre alle impostazioni di base per la scansione anti-virus, è possibile configurare una serie di impostazioni avanzate (vedere Figura 67):

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

Per esempio, si dispone di un file archivio che è stato scansionato dal programma ed è contrassegnato dallo stato *non infetto*. alla successiva scansione il programma ignorerà questo file, a meno che non sia stato modificato nel frattempo, o che non siano state cambiate le impostazioni di scansione.. Se la struttura dell'archivio risulta modificata perché è stato aggiunto un nuovo oggetto o perché le impostazioni di scansione sono state modificate o gli elenchi dei virus aggiornati, il programma sottoporrà nuovamente l'archivio a scansione anti-virus.

iChecker™ presenta tuttavia delle limitazioni: non funziona con file di grandi dimensioni e si applica solo ad oggetti con una struttura che Kaspersky Anti-

Virus for Windows Workstations è in grado di riconoscere (per esempio file di tipo *exe*, *.dll*, *.lnk*, *.ttf*, *.inf*, *.sys*, *.com*, *.chm*, *.zip*, *.rar*).

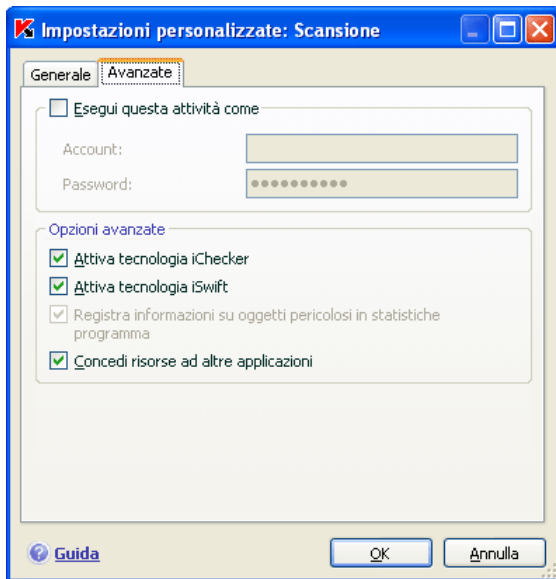


Figura 67. Impostazioni di scansione avanzate

- ✓ **Attiva tecnologia iSwift.** Questa tecnologia è stata sviluppata a partire dalla tecnologia iChecker per i computer che utilizzano un file system di tipo NTFS. Anche iSwift presenta delle limitazioni: è legato ad una posizione specifica dei file nel file system e può essere applicato esclusivamente agli oggetti di un file system NTFS.

La tecnologia iSwift non è disponibile su computer dotati di sistema operativo Microsoft Windows 98SE/ME/XP64.

- ✓ **Registra informazioni su oggetti pericolosi in statistiche programma** – salva le informazioni sugli oggetti pericolosi rilevati nelle statistiche generali del programma e visualizza un elenco di minacce rilevate durante la scansione nella scheda **Rilevati** della finestra di rapporto (vedere 17.3.2 a pag. 247) . Se questa opzione è disabilitata le informazioni sugli oggetti pericolosi non verranno visualizzate nel rapporto e sarà impossibile elaborare i dati.
- ✓ **Concedi risorse ad altri applicazioni** – sospende la scansione antivirus in corso se il processore è occupato con altre applicazioni.

## 14.4.6. Configurazione delle impostazioni di scansione globali per tutte le attività

Ogni operazione di scansione è eseguita in base alle proprie impostazioni. La modalità di scansione che si crea all'atto dell'installazione del programma utilizza le impostazioni predefinite raccomandate da Kaspersky Lab.

È possibile definire delle impostazioni globali valide per tutte le operazioni di scansione, in qualsiasi modalità. Come termine di riferimento si utilizza un gruppo di proprietà applicabili alla scansione anti-virus di un singolo oggetto.

*Per assegnare impostazioni di scansione globali:*

1. Selezionare la sezione **Scansione** nella parte sinistra della finestra principale del programma e fare clic su Impostazioni.
2. Configurare, nella finestra che appare, le impostazioni di scansione: Selezionare il livello di sicurezza (vedere 14.4.1 a pag. 207), configurare le impostazioni di livello avanzato, e selezionare un'azione (vedere 14.4.4 a pag. 212) per gli oggetti.
3. Per applicare queste nuove impostazioni a tutte le operazioni, fare clic sul pulsante **Applica** nella sezione **Altre impostazioni attività**. Confermare le impostazioni globali selezionate nella successiva finestra di dialogo.



---

# CAPITOLO 15. TESTARE LE FUNZIONI DI KASPERSKY ANTI-VIRUS

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

## 15.1. Test del virus EICAR e delle sue varianti

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

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

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

Il virus di prova può essere scaricato dal sito web ufficiale dell'organizzazione **EICAR**: [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm).

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

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

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

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

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

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

## 15.2. Testare File Anti-Virus

*Per testare la funzionalità di File Anti-Virus:*

1. Creare una cartella su un disco e copiare in essa il virus di prova scaricato dal sito Web ufficiale dell'organizzazione (vedere 15.1 a pag. 217), nonché le modifiche del virus di prova create dall'utente.
2. Lasciare che tutti gli eventi vengano registrati, in modo che il file rapporto conservi i dati sugli oggetti corrotti e quelli non esaminati a causa di errori. A tal fine, selezionare  **Registra eventi non critici** nella finestra di impostazione dei rapporti.
3. Lanciare il virus di prova o una sua variante.

File Anti-Virus blocca il tentativo di accesso al file, lo esamina e comunica all'utente di aver rilevato un oggetto nocivo:



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

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

## 15.3. Testare le attività di scansione anti-virus

*Per testare le attività di scansione anti-virus:*

1. Creare una cartella su un disco e copiare in essa il virus di prova scaricato dal sito Web ufficiale dell'organizzazione (vedere 15.1 a pag. 217), nonché le modifiche del virus di prova create dall'utente.
2. Creare una nuova attività di scansione anti-virus (vedere 14.3 a pag. 205) e selezionare la cartella contenente il gruppo di virus di prova quale oggetto da esaminare (vedere 14.2 a pag. 204).
3. Lasciare che tutti gli eventi vengano registrati, in modo che il file rapporto conservi i dati sugli oggetti corrotti e quelli non esaminati a causa di errori. A tal fine, selezionare  **Registra eventi non critici** nella finestra di impostazione dei rapporti.
4. Programmare una serie di scansioni antivirus (vedere 14.1 a pag. 203).

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



In questo modo, selezionando diverse opzioni di azione, è possibile testare le reazioni di Kaspersky Anti-Virus al rilevamento di diversi tipi di oggetti.

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

---

# CAPITOLO 16. AGGIORNAMENTI DEL PROGRAMMA

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

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

- **Elenchi delle minacce, elenchi degli attacchi di rete, driver di rete**

Le informazioni sul computer vengono protette tramite un database contenente gli elenchi delle minacce e i profili degli attacchi di rete, che vengono utilizzati dai componenti del programma che forniscono la protezione per rilevare e disinfettare oggetti dannosi eventualmente presenti. Le firme vengono aggiunte di ora in ora con la registrazione di nuove minacce e dei metodi per debellarle. Pertanto, si raccomanda di aggiornarli regolarmente.

Oltre agli elenchi delle minacce ad al database degli attacchi di rete, vengono aggiornati i driver di rete che consentono ai componenti di protezione di intercettare il traffico di rete.

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

- **Moduli applicazione**

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

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

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

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

Gli aggiornamenti possono essere scaricati secondo una delle seguenti modalità:

- *Automaticamente.* Kaspersky Anti-Virus verifica ad intervalli specificati la disponibilità di nuovi aggiornamenti presso la relativa sorgente. Durante le epidemie, la frequenza di verifica può aumentare, diminuendo al loro scemare. Se trova nuovi aggiornamenti, il programma li scarica e li installa sul computer. È la modalità predefinita.
- *Come pianificato.* L'avvio dell'aggiornamento è pianificato ad una certa ora.
- *Manualmente.* Con questa opzione, la procedura di aggiornamento viene avviata manualmente.

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

Prima di aggiornare gli elenchi dei virus, Kaspersky Anti-Virus for Windows Workstations ne crea una copia di backup, che può essere utilizzata se fosse necessario tornare alla versione precedente (vedere 16.2 a pag. 224). Se, per esempio, il processo di aggiornamento corrompe gli elenchi delle minacce rendendoli inutilizzabili, è possibile tornare con facilità alla versione precedente e ritentare l'aggiornamento in seguito.

È possibile distribuire gli aggiornamenti ad una sorgente locale contemporaneamente all'aggiornamento dell'applicazione (vedere 16.4.4 a pag. 233). Questa funzione consente di aggiornare i database ed i moduli utilizzati dalle applicazioni della versione 6.0 su computer collegati in rete, in modo da risparmiare larghezza di banda.

## 16.1. Avvio della procedura di aggiornamento

È possibile iniziare l'aggiornamento in qualsiasi momento. Il processo opererà dall'origine dell'aggiornamento selezionata dall'utente (vedere 16.4.1 a pag. 227).

La procedura di aggiornamento può essere avviata da:

- il menù contestuale (vedere 4.2 a pag. 53)
- la finestra principale del programma (vedere 4.3 a pag. 55)

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

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

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

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

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

Si noti che gli aggiornamenti vengono distribuiti alla sorgente locale durante il processo di aggiornamento, sempre che il servizio sia abilitato (vedere 16.4.4 a pag. 233).

## 16.2. Ripristino dell'aggiornamento precedente

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



*Per ripristinare la versione precedente degli elenchi delle minacce:*

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

## 16.3. Creazione delle attività di aggiornamento

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

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

*Per creare un'attività di aggiornamento avanzata:*

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

### Attenzione!

**Kaspersky Anti-Virus pone un limite al numero di attività di aggiornamento che l'utente può creare. Possono essere create due attività al massimo.**

La nuova attività eredita tutte le proprietà di quella sulla quale è basata, tranne per le impostazioni di pianificazione. L'impostazione di scansione automatica predefinita per la nuova attività è disabilitata.

Una volta creata l'attività, configurare le impostazioni avanzate: specificare l'origine dell'aggiornamento (vedere 16.4.1 a pag. 226), le impostazioni della connessione di rete (vedere 16.4.3 a pag. 231), e, se necessario, abilitare le attività con un altro profilo (vedere 6.4 a pag. 88) e configurare una pianificazione (vedere 6.5 a pag. 89).

*Per cambiare nome a un'attività:*

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

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

*Per eliminare un'attività:*

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

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

**Attenzione!**

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

## 16.4. Configurazione delle impostazioni di aggiornamento

Le impostazioni di aggiornamento specificano i seguenti parametri:

- La sorgente da cui l'aggiornamento viene scaricato e installato (vedere 16.4.1 a pag. 227).
- La modalità di esecuzione dell'aggiornamento dell'applicazione e i specifici componenti aggiornati (vedere 16.4.2 a pag. 229).
- Frequenza degli aggiornamento se gli aggiornamento vengono eseguiti puntualmente (vedere 6.5 a pag. 89).
- Account sotto il quale l'aggiornamento verrà eseguito (vedere 6.4 a pag. 88).
- Il requisito di copiare gli aggiornamenti scaricati in una directory locale (vedere 16.4.4 a pag. 233).
- Le azioni da compiere al termine dell'aggiornamento (vedere 16.4.5 a pag. 234).

Le seguenti sezioni esaminano in dettaglio questi aspetti.

## 16.4.1. Selezione di un'origine per l'aggiornamento

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

È possibile utilizzare quanto segue come origini degli aggiornamenti:

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

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

### Attenzione!

Per richiedere gli aggiornamenti salvati su un supporto, è necessario specificare se si desiderano anche gli aggiornamenti dei moduli dell'applicazione.

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

Selezionare la sorgente di aggiornamento dalla scheda **Origine aggiornamento** (vedere Figura 68).

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

*Per scaricare gli aggiornamenti da un altro sito FTP o HTTP:*

1. Fare clic su **Aggiungi**.

2. Nella finestra di dialogo **Seleziona origine aggiornamento**, selezionare il sito FTP o HTTP a cui si desidera connettersi, oppure specificare l'indirizzo IP, o l'URL del sito nel campo **Origine**. Quando si seleziona un sito ftp come sorgente di aggiornamento, è necessario inserire le impostazioni di autenticazione nell'URL del server in formato ftp://user:password@server.

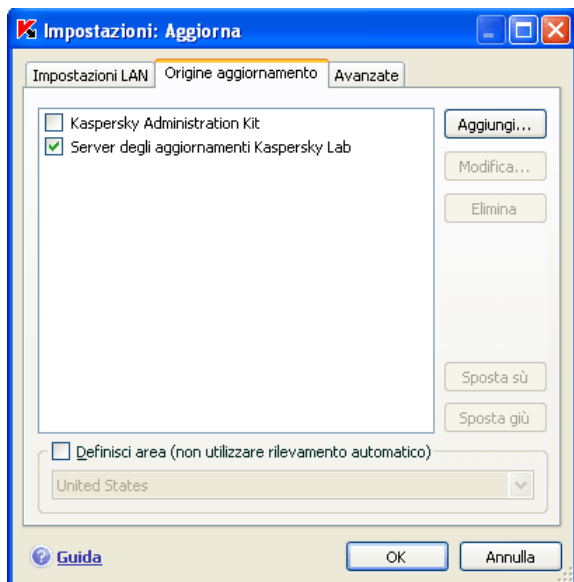


Figura 68. Selezione di una sorgente d'aggiornamento

### Attenzione!

Se si seleziona una risorsa esterna alla LAN per l'aggiornamento, è necessario disporre di una connessione Internet per recuperare gli aggiornamenti.

*Per scaricare l'aggiornamento da una cartella locale:*

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

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

Se sono state selezionate più risorse per l'aggiornamento, l'applicazione cerca di connettersi ad esse una dopo l'altra a partire da quella che occupa la prima posizione dell'elenco, e preleva gli aggiornamenti dalla prima disponibile. È possibile modificare l'ordine delle sorgenti nell'elenco tramite i pulsanti **Sposta su** e **Sposta giù**.

Per modificare la lista, utilizzare i pulsanti **Aggiungi**, **Modifica** e **Rimuovi**. L'unico tipo di sorgente che non può essere modificato né eliminato sono i server di aggiornamento di Kaspersky Lab.

Se si prelevano gli aggiornamenti dai server di Kaspersky Lab, è possibile selezionare la posizione ottimale del server da cui scaricare i file. Kaspersky Lab dispone di server in diversi paesi. La scelta del server di Kaspersky Lab più vicino aiuta a risparmiare tempo e ad accelerare il prelievo degli aggiornamenti.

Per scegliere il server più vicino, selezionare la casella  **Definisci area (non utilizzare rilevamento automatico)** e selezionare quindi dall'elenco a discesa il paese più vicino al proprio paese di residenza. Se si seleziona questa casella, gli aggiornamenti verranno eseguiti tenendo conto della regione selezionata nell'elenco. Questa casella di controllo è deselezionata per impostazione predefinita, e vengono utilizzate le informazioni sulla regione corrente tratte dal registro di sistema.

## 16.4.2. Selezione di un metodo di aggiornamento e degli oggetti da aggiornare

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

Gli oggetti dell'aggiornamento (vedere Figura 69) sono i componenti che verranno aggiornati:

- elenco delle minacce
- driver di rete che consentono ai componenti di protezione di intercettare il traffico di rete
- database degli attacchi di rete utilizzato da Anti-Hacker
- moduli del programma

I database dell'applicazione, i driver di rete ed i database degli attacchi di rete vengono sempre aggiornati, mentre i moduli dell'applicazione vengono aggiornati solo se è selezionata la relativa modalità.

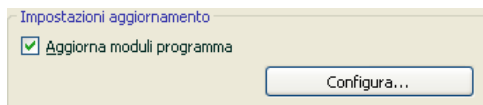


Figura 69. Selezione di un oggetto da aggiornare

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

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

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

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

Il Metodo di aggiornamento (vedere Figura 70) definisce le modalità di avvio del programma di aggiornamento. La sezione **Modalità esecuzione** consente di selezionare uno dei seguenti metodi:

**Automaticamente**. Kaspersky Anti-Virus verifica ad intervalli specificati la disponibilità di nuovi aggiornamenti presso la relativa sorgente. Se trova nuovi aggiornamenti, il programma li scarica e li installa sul computer. Questa modalità è selezionata per impostazione predefinita.

Se è specificata una risorsa di rete come origine di aggiornamento, Kaspersky Anti-Virus for Windows Workstations cerca di avviare l'aggiornamento dopo un certo periodo, secondo quanto specificato nel precedente pacchetto di aggiornamento. Se come sorgente di aggiornamento è specificata una cartella locale, l'applicazione cerca di scaricare gli aggiornamenti dalla cartella locale alla frequenza stabilita nel pacchetto scaricato durante l'ultimo aggiornamento. Questa opzione consente a Kaspersky Lab di regolare la frequenza di aggiornamento in caso di pandemie di virus e altre situazioni potenzialmente pericolose. L'applicazione riceve gli ultimi aggiornamenti relativi ad elenchi dei virus e moduli software in modo tempestivo, escludendo così la possibilità che eventuali software nocivi possano penetrare nel computer.

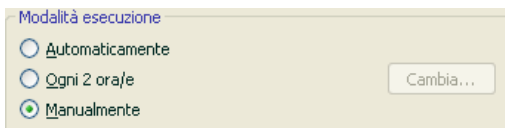


Figura 70. Selezione di una modalità di esecuzione degli aggiornamenti

- **Come pianificato.** L'avvio dell'aggiornamento è pianificato ad una certa ora. Per impostazione predefinita, gli aggiornamenti pianificati hanno cadenza di 2 ore. Per modificare la pianificazione predefinita, fare clic sul pulsante **Cambia...** accanto al nome della modalità e apportare le modifiche necessarie nella finestra che si apre (per ulteriori dettagli, vedere 6.5 a pag. 89).
- **Manualmente.** Questa opzione consente di avviare Updater manualmente. Kaspersky Anti-Virus for Windows Workstations notifica quando è necessario un aggiornamento:
  - Sopra all'icona dell'applicazione nell'area di notifica compare un messaggio pop-up che informa l'utente che è il momento di effettuare l'aggiornamento (se le notifiche sono abilitate; vedere 17.11.1 a pag. 275)
  - Il secondo indicatore nella finestra principale del programma informa che il computer non è aggiornato (vedere 5.1.1 a pag. 60)
  - Nella sezione messaggi della finestra principale del programma viene visualizzata la raccomandazione di aggiornare l'applicazione (vedere 4.3 a pag. 55)

### 16.4.3. Configurazione delle impostazioni di connessione

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

Tutte le impostazioni sono raggruppate in una scheda particolare – **Impostazioni LAN** (vedere Figura 71).

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

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

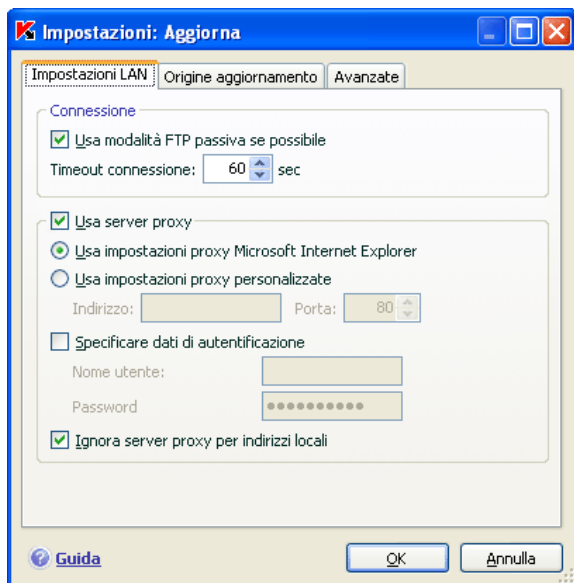


Figura 71. Configurazione delle impostazioni di aggiornamento

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

- Selezionare le impostazioni del server proxy da utilizzare durante l'aggiornamento:
  - ◉ **Usa impostazioni proxy Microsoft Internet Explorer.** Se si seleziona questa opzione, le impostazioni del server proxy vengono rilevate automaticamente utilizzando il protocollo WPAD (Web Proxy Auto Discovery Protocol). Se questo protocollo non è in grado di rilevare l'indirizzo, Kaspersky Anti-Virus utilizzerà le impostazioni del server proxy utilizzate in Microsoft Internet Explorer.
  - ◉ **Usa impostazioni proxy personalizzate** – per utilizzare un proxy diverso da quello specificato nelle impostazioni di connessione del browser. Nel campo **Indirizzo**, immettere l'indirizzo IP o il nome simbolico del server proxy e specificare il numero di porta proxy nel campo **Porta**.
- Specificare se è richiesta l'autenticazione sul server proxy. L'*autenticazione* è il processo di verifica dei dati di registrazione dell'utente ai fini di controllo dell'accesso.



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

Se questa casella di controllo non è selezionata o se i dati non vengono immessi, l'autenticazione NLTM verrà tentata utilizzando l'account utente per avviare l'aggiornamento (vedere 6.4 a pag. 88).

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

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

Questa funzione non è disponibile in Windows 9X/NT 4.0. Tuttavia, per impostazione predefinita, il server proxy non è utilizzato per gli indirizzi locali.

## 16.4.4. Aggiornamento della cartella di distribuzione

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

1. Uno dei computer della rete recupera un pacchetto di aggiornamento dell'applicazione e degli elenchi dei virus dai server Web di Kaspersky Lab, oppure da un'altra risorsa di rete che ospita un insieme di aggiornamenti. Gli aggiornamenti recuperati vengono salvati in una cartella ad accesso pubblico.
2. Gli altri computer della rete accedono alla cartella ad accesso pubblico per recuperare gli aggiornamenti all'applicazione.

Per abilitare la distribuzione degli aggiornamenti, selezionare la casella di controllo  **Aggiornare cartella di distribuzione** nella scheda **Avanzate** (vedere Figura 72), quindi specificare la cartella condivisa dove verranno salvati gli aggiornamenti nel campo sottostante. È possibile immettere il percorso manualmente o selezionarlo nella finestra che si apre facendo clic su **Sfoggia**. Se la casella di controllo è selezionata, gli aggiornamenti verranno copiati in questa cartella quando vengono recuperati.

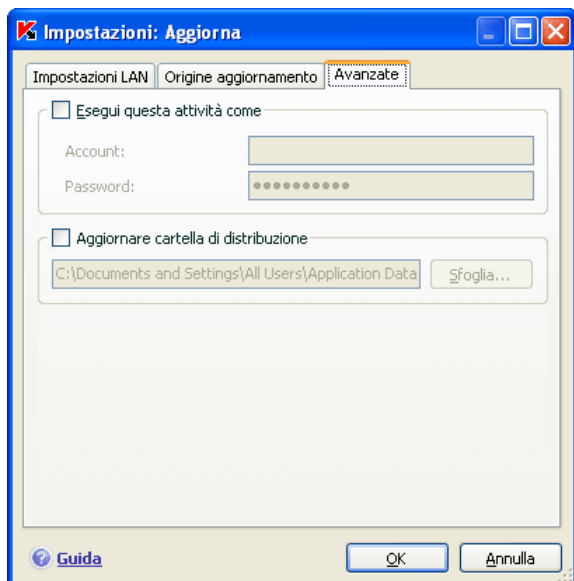


Figura 72. Impostazioni dello strumento di copia degli aggiornamenti

Si noti che Kaspersky Anti-Virus 6.0 recupera dai server di aggiornamento di Kaspersky Lab esclusivamente i pacchetti di aggiornamento relativi alle applicazioni v. 6.0. Si consiglia di copiare gli aggiornamenti per le altre applicazioni di Kaspersky Lab tramite Kaspersky Administration Kit.

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

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

## 16.4.5. Azioni successive all'aggiornamento del programma

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

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

Perché è necessario esaminare questi oggetti?

L'area di quarantena contiene oggetti che il programma ha catalogato come sospetti o potenzialmente infetti (vedere 17.1 a pag. 237). Utilizzando la versione più recente degli elenchi dei virus, Kaspersky Anti-Virus for Windows Workstations può essere in grado di identificare la minaccia e di eliminarla.

Per impostazione predefinita, l'applicazione esamina gli oggetti in quarantena dopo ogni aggiornamento degli elenchi delle minacce. Si consiglia inoltre di controllare periodicamente gli oggetti in questa cartella in quanto il loro stato può cambiare dopo varie scansioni. Alcuni oggetti possono quindi essere ripristinati nelle loro posizioni originarie per continuare ad utilizzarli.

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

Gli oggetti di avvio sono di importanza vitale per la sicurezza del computer. Se uno di essi è infetto da un'applicazione nociva, potrebbe verificarsi un errore di avvio del sistema operativo. Kaspersky Anti-Virus for Windows Workstations è dotato di un'attività di scansione degli oggetti all'avvio per quest'area (vedere Capitolo 14 a pag. 202). Si raccomanda di pianificare un calendario di esecuzione per questa attività in modo da avviarlo automaticamente ad ogni aggiornamento degli elenchi delle minacce (vedere 6.5 a pag. 89).

---

# CAPITOLO 17. OPZIONI AVANZATE

Kaspersky Anti-Virus for Windows Workstations è dotato di altre funzioni che ne espandono la funzionalità.

Il programma colloca alcuni oggetti in apposite aree di archiviazione, al fine di garantire la massima protezione dei dati riducendo al minimo le perdite.

- La cartella Backup contiene copie degli oggetti modificati o eliminati da Kaspersky Anti-Virus for Windows Workstations (vedere 17.2 a pag. 241). Se un oggetto conteneva informazioni importanti e non è stato possibile recuperarlo completamente durante l'elaborazione antivirus, è possibile ripristinare l'oggetto dalla copia di backup.
- La Quarantena contiene oggetti potenzialmente infetti che non è stato possibile elaborare con le firme correnti (vedere 17.1 a pag. 237).

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

Le opzioni avanzate comprendono diverse utili funzioni. Per esempio:

- Il servizio di supporto tecnico offre un'assistenza completa per Kaspersky Anti-Virus for Windows Workstations (vedere 17.6 a pag. 263). Kaspersky offre diversi canali di supporto, tra cui il supporto on-line ed un forum di domande e risposte per gli utenti del programma.
- La funzione di Notifica serve per configurare le notifiche agli utenti relative a eventi chiave di Kaspersky Anti-Virus for Windows Workstations (vedere 17.11.1 a pag. 275). Può trattarsi di eventi di natura informativa, o di errori critici che devono essere risolti immediatamente.
- La funzione di Auto-Difesa protegge i file del programma da qualsiasi modifica o danno perpetrati dagli hacker, blocca l'uso delle funzioni del programma da parte di amministrazioni remote e limita i diritti degli altri utenti sul computer in uso in relazione all'esecuzione di certe azioni in Kaspersky Anti-Virus for Windows Workstations (vedere 17.11.1.2 a pag. 277). Per esempio, la modifica del livello di protezione può influire considerevolmente sulla sicurezza del computer.
- La Gestione chiavi di licenza è in grado di ottenere informazioni dettagliate sulla licenza utilizzata, attivare la copia del programma, e gestire i file delle chiavi di licenza (vedere 17.5 a pag. 261).

Il programma offre anche una sezione di Guida (vedere 17.4 a pag. 260) e rapporti dettagliati (vedere 17.3 a pag. 243) sul funzionamento di tutti i componenti di protezione e le attività di scansione antivirus.

La creazione dell'elenco di porte monitorate può regolare quali moduli di Kaspersky Anti-Virus for Windows Workstations controllano i dati trasferiti sulle porte selezionate (vedere 17.7 a pag. 264).

Il disco di emergenza consente di ripristinare la funzionalità del computer dopo un'infezione (vedere 17.10 a pag. 270). Si tratta di una funzione particolarmente utile quando non si riesce ad avviare il sistema operativo del computer in seguito al danneggiamento dei file di sistema da parte di un codice nocivo.

È possibile inoltre modificare l'aspetto di Kaspersky Anti-Virus for Windows Workstations e personalizzare l'interfaccia del programma (vedere 17.9 a pag. 268).

Le seguenti sezioni esaminano in dettaglio queste funzioni.

## 17.1. Quarantena per gli oggetti potenzialmente infetti

La **Quarantena** è una speciale area di archiviazione che contiene gli oggetti potenzialmente infetti.

Gli **oggetti potenzialmente infetti** sono oggetti di cui si sospetta l'infezione da virus o virus modificati.

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

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

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

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

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

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

Un oggetto potenzialmente infetto può essere intercettato e trasferito in Quarantena da File Anti-Virus, Anti-Virus posta, Difesa proattiva o nel corso di una scansione antivirus.

Per mettere un oggetto in quarantena è sufficiente fare clic sul pulsante **Quarantena** nella notifica visualizzata al rilevamento di un oggetto potenzialmente infetto.

Quando un oggetto viene messo in Quarantena, esso non viene copiato ma trasferito. L'oggetto viene eliminato dal disco o dall'e-mail e salvato nella cartella di Quarantena. I file in Quarantena vengono salvati in uno speciale formato e pertanto non sono pericolosi.

## 17.1.1. Azioni da eseguire sugli oggetti in Quarantena

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

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

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

*Per accedere agli oggetti in Quarantena:*

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

La scheda **Quarantena** consente di eseguire le seguenti azioni (vedere Figura 73):

- Trasferire in Quarantena un file sospettato di contenere un'infezione che il programma non ha rilevato. A tal fine, fare clic sul pulsante **Aggiungi** e scegliere il file nella finestra standard di selezione. Il file viene aggiunto all'elenco con lo status *aggiunto dall'utente*.

Se un file viene messo in quarantena manualmente e si rivela non infetto dopo una scansione successiva, lo stato dopo la scansione non verrà modificato immediatamente in *OK*. Ciò succederà solo se la scansione ha avuto luogo dopo un certo tempo (almeno tre giorni) dalla messa in quarantena del file.

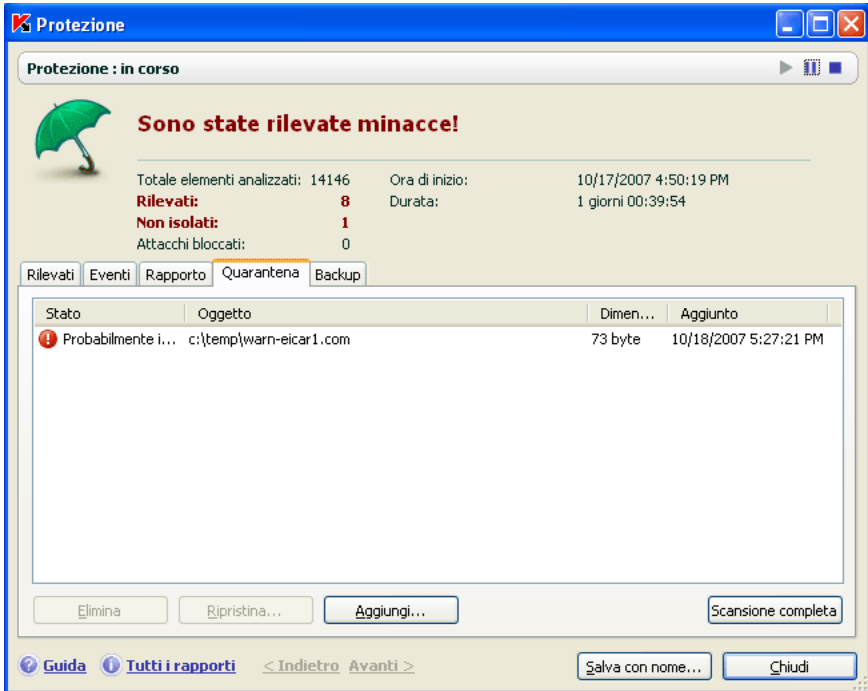


Figura 73. Elenco degli oggetti in quarantena

- Esaminare e disinfettare tutti gli oggetti potenzialmente infetti in Quarantena per mezzo di elenchi delle minacce correnti facendo clic su **Scansione completa**.

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

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

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

- Ripristinare i file in una cartella selezionata dall'utente o nella cartella in cui si trovavano prima della Quarantena (impostazione predefinita). Per ripristinare un oggetto, selezionarlo dall'elenco e fare clic su **Ripristina**. Durante il ripristino di oggetti da archivi, database di posta e file in formato posta trasferiti in quarantena, è necessario selezionare anche la directory in cui ripristinarli.

**Suggerimento:**

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

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

## 17.1.2. Configurazione della Quarantena

È possibile configurare le impostazioni di layout e funzionamento della Quarantena, in particolare:

- Impostare scansioni automatiche di oggetti in Quarantena dopo ogni aggiornamento degli elenchi delle minacce (per ulteriori informazioni, vedere 16.4.4 a pag. 233).

**Attenzione!**

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

- Impostare la durata massima della conservazione degli oggetti in Quarantena.

La durata predefinita è di 30 giorni, allo scadere dei quali gli oggetti vengono eliminati. È possibile modificare la durata di conservazione nella Quarantena o disabilitare del tutto questa limitazione

Per fare ciò:

1. Aprire la finestra delle impostazioni di Kaspersky Anti-Virus for Windows Workstations facendo clic su Impostazioni nella finestra principale del programma.
2. Selezionare **File dati** dalla struttura ad albero delle impostazioni.
3. Nella sezione **Quarantena e Backup** (vedere Figura 74), digitare il tempo massimo allo scadere del quale gli oggetti in quarantena saranno



automaticamente eliminati. In alternativa, deselezionare la casella di controllo per disabilitare la cancellazione automatica

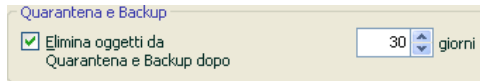


Figura 74. Configurazione del periodo di conservazione degli oggetti in Quarantena

## 17.2. Copie di backup di oggetti pericolosi

A volte, in seguito alla riparazione, gli oggetti perdono la propria integrità. Se un file riparato contiene informazioni importanti e risulta parzialmente o completamente corrotto, si può tentare di ripristinare l'oggetto originario da una copia di backup.

Una **copia di backup** è una copia dell'oggetto pericoloso creata prima di riparare o eliminare l'originale. Le copie di backup vengono salvate nella cartella Backup.

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

### 17.2.1. Azioni da eseguire sulle copie di backup

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

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

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

*Per accedere alle copie di oggetti pericolosi:*

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

Nella scheda Backup viene visualizzato un elenco delle copie di backup (vedere Figura 75). Per ogni copia sono fornite le seguenti informazioni: il nome ed il percorso dell'oggetto, lo stato dell'oggetto assegnato dalla scansione e le sue dimensioni.

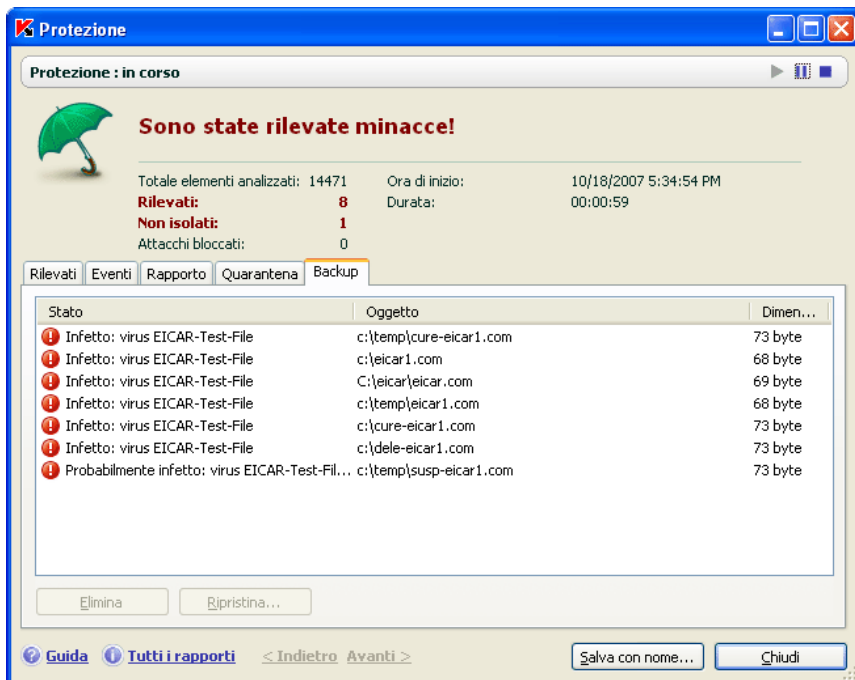


Figura 75. Elenco di oggetti dei quali esiste una copia di backup

Le copie selezionate possono essere ripristinate tramite il pulsante **Ripristina**. L'oggetto viene così ripristinato dalla cartella Backup con lo stesso nome dell'originale prima della riparazione.

Se esiste già un oggetto con quel nome nella posizione originaria (ciò è possibile se prima della disinfezione è stata creata una copia dell'oggetto che si desidera ripristinare), viene visualizzato un apposito messaggio. È possibile cambiare posizione all'oggetto ripristinato oppure rinominarlo.

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

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

Si consiglia di esaminare periodicamente l'area di backup e di svuotarla tramite il pulsante **Elimina**. È possibile inoltre configurare il programma in modo da eliminare automaticamente dal Backup le copie di più vecchia data (vedere 17.2.2 a pag. 243).

## 17.2.2. Configurazione delle impostazioni del Backup

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

La durata predefinita è di 30 giorni, allo scadere dei quali le copie di backup vengono eliminate. È possibile inoltre modificare la durata di conservazione o disabilitare del tutto questa limitazione procedendo come segue: Per fare ciò:

1. Aprire la finestra delle impostazioni di Kaspersky Anti-Virus for Windows Workstations facendo clic su Impostazioni nella finestra principale del programma.
2. Selezionare **File dati** dalla struttura ad albero delle impostazioni.
3. Impostare la durata della conservazione delle copie di backup nella sezione **Quarantena e Backup** (vedere Figura 74) nella parte destra della finestra. In alternativa, deselezionare la casella di controllo per disabilitare la cancellazione automatica.

## 17.3. Rapporti

Le attività dei componenti di Kaspersky Anti-Virus for Windows Workstations, le scansioni antivirus e le attività di aggiornamento sono tutte registrate in appositi rapporti.

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

*Per visualizzare i rapporti:*

Fare clic ovunque nel riquadro *Rapporto* per aprire la finestra Protezione, che riassume la protezione offerta dall'applicazione. Si apre una finestra contenente, tra le altre, la scheda **Rapporto** (vedere Figura 76).

La scheda Rapporto elenca gli ultimi rapporti su tutti i componenti e le attività di scansione anti-virus ed aggiornamento eseguite durante la sessione corrente di Kaspersky Anti-Virus for Windows Workstations. Lo stato viene elencato accanto

a ciascun componente o attività, ad esempio *fermato* o *completato*. Per vedere la cronologia completa della creazione dei rapporti per la sessione corrente del programma, selezionare  **Mostra cronologia rapporto**.

Per consultare tutti gli eventi registrati nel rapporto di un componente o di un'attività:

Selezionare il nome del componente o dell'attività nella scheda **Rapporto** e fare clic sul pulsante **Dettagli**.

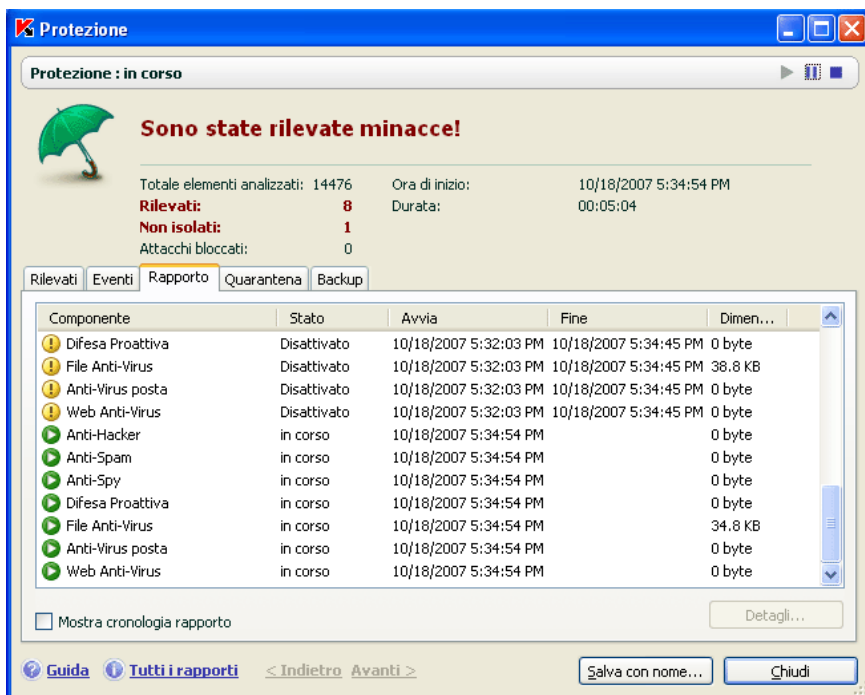


Figura 76. Rapporto sul funzionamento dei componenti

Si apre una finestra contenente informazioni dettagliate sulle prestazioni del componente o attività selezionati. Le statistiche sulle prestazioni sono visualizzate nella parte superiore della finestra, mentre le informazioni dettagliate sono riportate nelle schede. Le schede sono diverse a seconda del componente o attività:

- La scheda **Rilevati** contiene un elenco di oggetti pericolosi individuati da un componente o da un'attività di scansione antivirus.
- La scheda **Eventi** visualizza gli eventi relativi al componente o attività.

- La scheda **Statistiche** contiene statistiche dettagliate per tutti gli oggetti esaminati.
- La scheda **Impostazioni** visualizza una serie di impostazioni utilizzate dai componenti di protezione, dalle scansioni anti-virus o dagli aggiornamenti all'elenco dei virus.
- Le schede **Macro** e **Registro** sono presenti solo nel rapporto di Difesa Proattiva e contengono informazioni su tutte le macro che si è cercato di eseguire sul computer, nonché su tutti i tentativi di modificare il registro del sistema operativo.
- Le schede **Phishing**, **Popup**, **Banner** e **Composizione automatica numeri nascoste** sono presenti solo nel rapporto di Anti-Spy. Esse contengono informazioni su tutti gli attacchi di phishing intercettati e su tutti i popup, i banner e i tentativi di connessione dialer bloccati durante la sessione.
- Le schede **Attacchi provenienti dalla rete**, **Computer esclusi**, **Attività applicazione** e **Filtri pacchetti** sono presenti solo nel rapporto di Anti-Hacker. Esse contengono informazioni su tutti i tentativi di attacco di rete al computer e sui computer esclusi in seguito ad attacchi, le descrizioni delle attività di rete delle applicazioni che corrispondono alle regole di attività esistenti, e tutti i pacchetti dati che corrispondono alle regole di filtro pacchetti di Anti-Hacker.
- Le schede **Connessioni stabilite**, **Porte aperte** e **Traffico** coprono inoltre l'attività di rete del computer, visualizzando le connessioni correnti, le porte aperte e la quantità di traffico inviato e ricevuto dal computer.

I rapporti possono essere interamente esportati in formato testo. Questa funzione è utile quando si è verificato un errore impossibile da eliminare autonomamente, per il quale si necessita di assistenza tecnica. In tali casi è necessario inviare il rapporto in formato .txt al servizio di Assistenza tecnica per consentire ai nostri specialisti di studiare approfonditamente il problema e risolverlo nel più breve tempo possibile.

*Per esportare un rapporto in formato testo:*

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

Una volta completate le operazioni sul rapporto, fare clic su **Chiudi**.

Esiste un pulsante **Azioni** su tutte le schede (ad eccezione di **Impostazioni** e **Statistiche**), che può essere utilizzato per definire le reazioni agli oggetti presenti nell'elenco. Facendo clic su di esso, si apre un menu di scelta rapida con alcune di queste voci di menu (il menu è diverso a seconda del componente; di seguito sono elencate tutte le opzioni possibili):

**Disinfetta** – il programma cerca di riparare l'oggetto pericoloso. Se la riparazione non va a buon fine, è possibile lasciare l'oggetto nell'elenco per esaminarlo in seguito con gli elenchi delle minacce aggiornati oppure eliminarlo. Questa azione può essere applicata ad un oggetto nell'elenco o a diversi oggetti selezionati.

**Elimina** – elimina la voce relativa al rilevamento dell'oggetto dal rapporto.

**Aggiungi a zona attendibile** – esclude l'oggetto dalla protezione. Si apre una finestra con una regola di esclusione per l'oggetto.

**Vai al file** – si apre la cartella in cui è stato salvato l'oggetto in Windows Explorer.

**Isola tutto** – neutralizza tutti gli oggetti nella lista. Kaspersky Anti-Virus for Windows Workstations tenta di elaborare gli oggetti utilizzando l'elenco dei virus.

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

**Cerca** [www.viruslist.com](http://www.viruslist.com) – viene visualizzata una descrizione dell'oggetto nella Virus Encyclopedia sul sito web di Kaspersky Lab.

**Cerca** [www.google.com](http://www.google.com) – trova informazioni sull'oggetto utilizzando questo motore di ricerca.

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

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

## 17.3.1. Configurazione delle impostazioni dei rapporti

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

1. Aprire la finestra delle impostazioni di Kaspersky Anti-Virus for Windows Workstations facendo clic su Impostazioni nella finestra principale del programma.
2. Selezionare **File dati** dalla struttura ad albero delle impostazioni.
3. Modificare le impostazioni del riquadro **Rapporto** (vedere Figura 77) come segue:
  - Consentire o disabilitare la registrazione di eventi informativi. Questi eventi di solito non sono rilevati ai fini della sicurezza. Per registrare gli eventi, selezionare la casella  **Registra eventi non critici**.

- Scegliere di salvare nel rapporto solo gli eventi verificatisi successivamente all'ultima esecuzione dell'attività. Questa impostazione consente di salvare spazio su disco riducendo le dimensioni del rapporto. Se è selezionata l'opzione  **Mantieni solo eventi recenti**, le informazioni nel rapporto vengono aggiornate ogni volta che si riavvia l'attività. Tuttavia saranno sovrascritte solo le informazioni non critiche.
- Impostare la durata della conservazione dei rapporti. La durata predefinita è di 30 giorni, allo scadere dei quali i rapporti vengono eliminati. È possibile modificare la durata massima di conservazione o disabilitare del tutto questa limitazione.



Figura 77. Configurazione delle impostazioni del rapporto

### 17.3.2. La scheda *Rilevati*

Questa scheda (vedere Figura 78) contiene un elenco di oggetti pericolosi rilevati da Kaspersky Anti-Virus for Windows Workstations. Per ogni oggetto è indicato il nome ed il percorso completi, accompagnato dallo stato assegnato ad esso dal programma in seguito alla scansione o all'elaborazione.

Se si desidera che l'elenco contenga sia gli oggetti pericolosi sia quelli neutralizzati con successo, selezionare la casella  **Mostra oggetti isolati**.

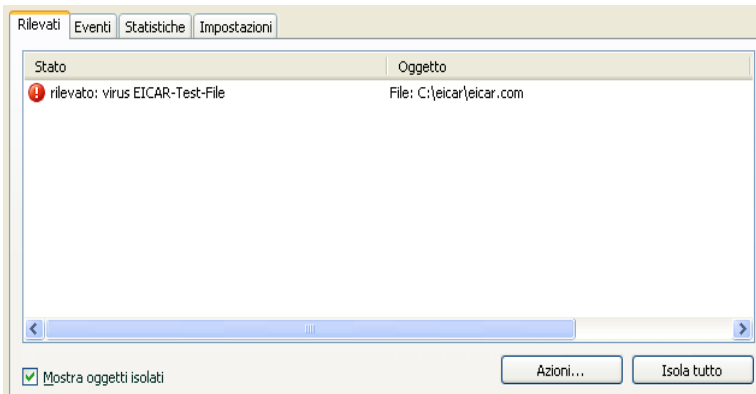


Figura 78. Elenco degli oggetti pericolosi rilevati

Per trattare gli oggetti pericolosi rilevati da Kaspersky Anti-Virus, scegliere **Isola** (per un oggetto o un gruppo di oggetti) o **Isola tutto** (per trattare tutti gli oggetti nella lista). Dopo aver trattato ciascun oggetto, viene visualizzato un messaggio sullo schermo. Sarà a questo punto necessario decidere cosa fare.

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

### 17.3.3. La scheda *Eventi*

Questa scheda (vedere Figura 79) contiene un elenco completo degli eventi importanti verificatisi durante il funzionamento di un componente di protezione, una scansione antivirus e gli aggiornamenti degli elenchi delle minacce non ignorati da una regola di controllo delle attività (vedere 10.1.1 a pag. 131).

Questi eventi possono essere:

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

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

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

**Mostra tutti gli eventi**.

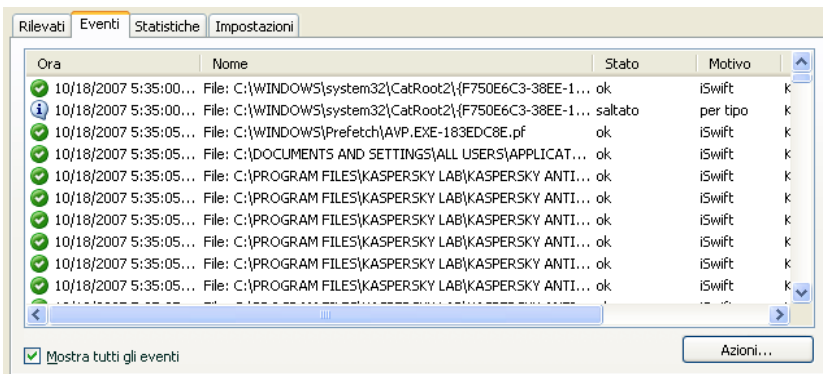


Figura 79. Eventi che si verificano durante il funzionamento di un componente



Il formato di visualizzazione degli eventi nel registro può variare in base al componente o all'attività. Per ogni attività di aggiornamento sono riportate le seguenti informazioni:

- Nome dell'evento
- Nome dell'oggetto interessato dall'evento
- L'ora in cui si è verificato l'evento
- Le dimensioni del file caricato

Per le attività di scansione antivirus, il registro degli eventi contiene il nome dell'oggetto esaminato e lo status assegnatogli in seguito alla scansione/elaborazione.

È possibile inoltre addestrare Anti-Spam durante la visualizzazione del rapporto per mezzo dell'apposito menu di scelta rapida. A tal fine, selezionare il nome del messaggio di posta e aprire il menu di scelta rapida facendo clic con il tasto destro del mouse e selezionare **Segna come spam** se il messaggio è indesiderato, o **Segna come non spam** se è valido. Inoltre, in base alle informazioni ottenute analizzando il messaggio, è possibile aggiungerlo alle liste bianche o alle liste nere di Anti-Spam. A tal fine, utilizzare le voci corrispondenti sul menu di scelta rapida.

### 17.3.4. La scheda *Statistiche*

Questa scheda (vedere Figura 80) contiene le statistiche dettagliate sui componenti e le attività di scansione antivirus. Da questa finestra risulta:

- Quanti oggetti sono stati esaminati in cerca di tratti pericolosi nella sessione corrente di un componente o dopo il completamento di un'attività. Il numero degli archivi, dei file compressi e degli oggetti protetti da password e corrotti esaminati.
- Quanti oggetti pericolosi sono stati rilevati, non disinfettati, eliminati o trasferiti in Quarantena.



| Oggetto           | Esaminati | Rilevato | Non isolati | Eliminati | Spostato in Quarantena | Archivi | Fi |
|-------------------|-----------|----------|-------------|-----------|------------------------|---------|----|
| Tutti gli oggetti | 2146      | 1        | 1           | 0         | 0                      | 0       | 0  |
| Local Disk (C:)   | 2146      | 1        | 1           | 0         | 0                      | 0       | 0  |

Figura 80. Statistiche dei componenti

### 17.3.5. La scheda *Impostazioni*

La scheda **Impostazioni** (vedere Figura 81) visualizza l'elenco completo delle impostazioni dei componenti di protezione, delle scansioni antivirus e degli aggiornamenti del programma. È possibile vedere il livello di protezione di un componente o di una scansione antivirus, le azioni compiute sugli oggetti pericolosi o le impostazioni in uso per gli aggiornamenti del programma. Utilizzare il collegamento [Modifica impostazioni](#) per configurare il componente.

È possibile configurare impostazioni avanzate per le scansioni antivirus:

- Stabilire la priorità delle attività di scansione in caso di sovraccarico sul processore. La casella di controllo  **Concedi risorse ad altre applicazioni** è selezionata per impostazione predefinita. Con questa funzione, il programma individua il carico sul processore e sui sottosistemi disco per l'attività di altre applicazioni. Se il carico sul processore aumenta considerevolmente e impedisce alle applicazioni dell'utente di funzionare normalmente, il programma riduce l'attività di scansione. In tal modo si aumenta la durata della scansione ma si liberano risorse per le applicazioni dell'utente.

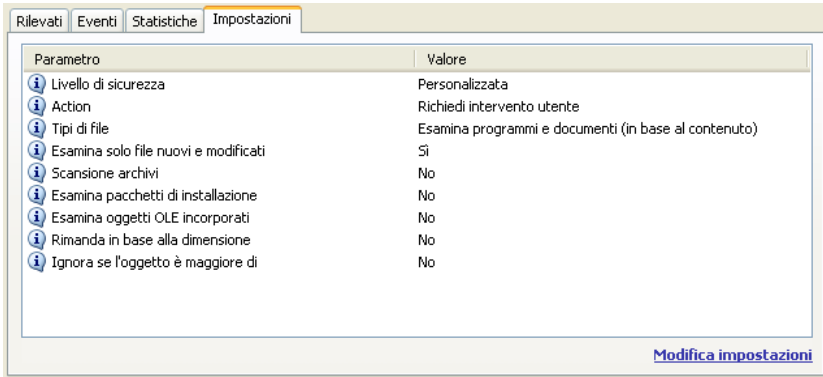


Figura 81. Impostazioni dei componenti

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

Questa funzione può risultare utile se, per esempio, si avvia una scansione antivirus al termine della giornata lavorativa e non si desidera aspettarne la conclusione.

Tuttavia, per poter utilizzare questa funzione è necessario eseguire i seguenti passaggi supplementari: prima di lanciare la scansione, è necessario disabilitare le richieste di password per gli oggetti esaminati, se abilitata, e abilitare l'elaborazione automatica degli oggetti pericolosi, per disabilitare le funzioni interattive del programma.

### 17.3.6. La scheda *Macro*

Tutte le macro di cui è stata tentata l'esecuzione durante la sessione corrente di Kaspersky Anti-Virus for Windows Workstations sono elencate nella scheda **Macro** (vedere Figura 82). Essa contiene il nome completo di ogni macro, l'ora in cui è stata eseguita e lo stato ottenuto dopo l'elaborazione.

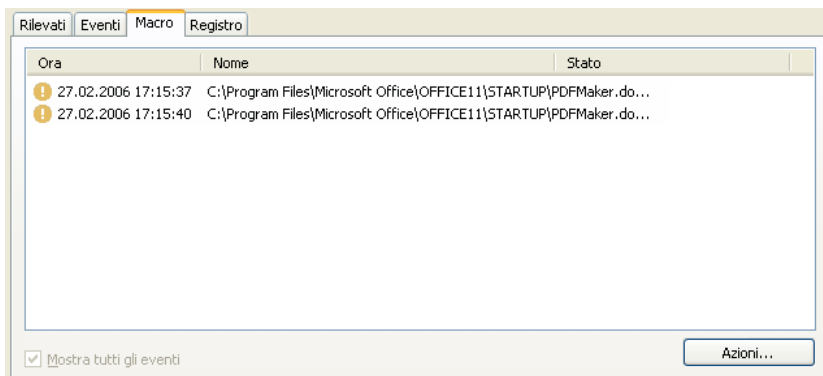


Figura 82. Rilevamento di una macro pericolosa

È possibile scegliere una modalità di visualizzazione per questa scheda. Se non si desidera visualizzare gli eventi informativi, deselezionare  **Mostra tutti gli eventi**.

### 17.3.7. La scheda *Registro*

Il programma registra le operazioni con le chiavi di registro che sono state tentate dall'avvio del programma nella scheda **Registro** (vedere Figura 83), a meno che non fossero proibite da una regola (vedere 10.1.3.2 a pag. 139).

La scheda riporta il nome completo della chiave, il suo valore, il tipo di dati e le informazioni relative all'operazione che ha avuto luogo: l'azione tentata, l'ora e l'eventuale autorizzazione.

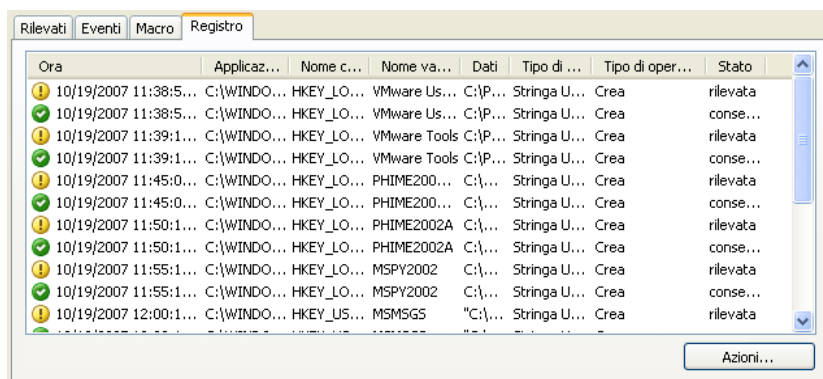


Figura 83. Lettura e modifica degli eventi del registro di sistema

### 17.3.8. La scheda *Phishing*

Questa scheda del rapporto (vedere Figura 84) visualizza tutti i tentativi di phishing eseguiti durante la sessione corrente di Kaspersky Anti-Virus for Windows Workstations. Il rapporto contiene un link al sito di phishing rilevato nel messaggio (o altrove), la data e l'ora di intercettazione dell'attacco e lo stato dell'attacco (se è stato bloccato oppure no).

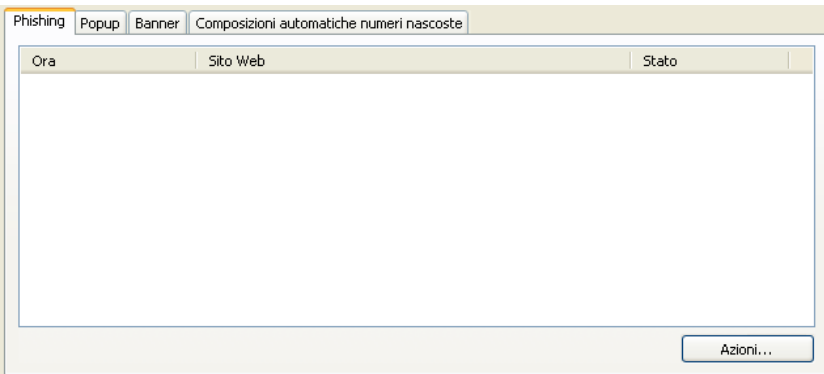


Figura 84. Attacchi di phishing bloccati

### 17.3.9. La scheda *Popup*

Questa scheda di rapporto (vedere Figura 85) elenca gli indirizzi di tutti le finestre pop-up bloccate da Anti-Spy. Questa finestra si apre generalmente dai siti web.

Per ognuno di essi sono registrati l'indirizzo e la data in cui Blocco Popup ha bloccato la finestra.

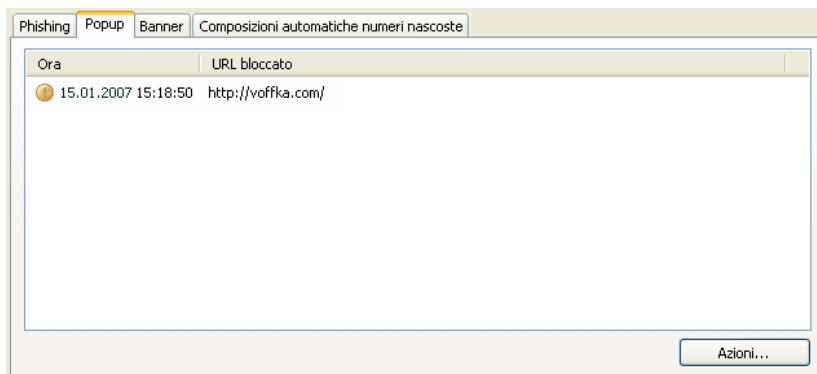


Figura 85. Elenco delle finestre popup bloccate

### 17.3.10. La scheda *Banner*

Questa scheda del rapporto (vedere Figura 86) contiene gli indirizzi dei banner pubblicitari che Kaspersky Anti-Virus for Windows Workstations ha rilevato nella sessione corrente. Per ogni banner è riportato l'indirizzo web accompagnato dallo status di elaborazione (banner bloccato o visualizzato).

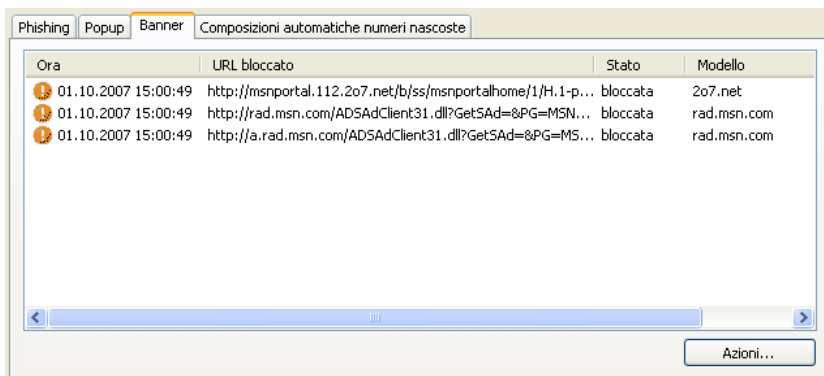
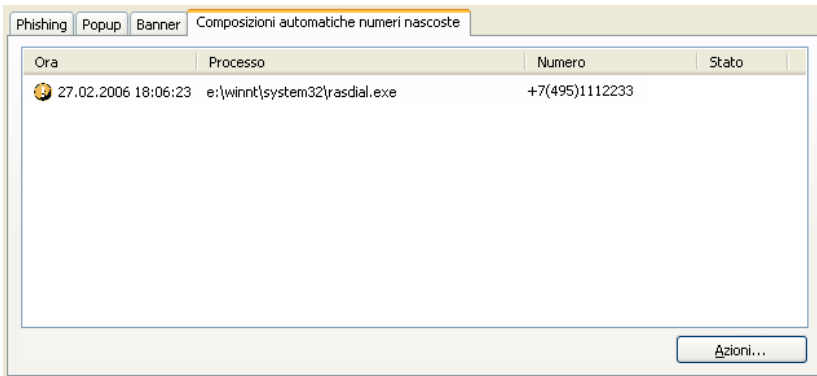


Figura 86. Elenco dei banner pubblicitari bloccati

È anche possibile decidere di visualizzare i banner bloccati. A tal fine, selezionare l'oggetto desiderato dalla lista e fare clic su **Azioni** → **Autorizza**.

### 17.3.11. La scheda *Composizioni automatiche numeri nascoste*

Questa scheda (vedere Figura 87) visualizza tutti i tentativi di connessione furtiva ai siti a pagamento. Tali tentativi sono generalmente effettuati da programmi nocivi installati sul computer.



The screenshot shows a window titled 'Composizioni automatiche numeri nascoste' with tabs for 'Phishing', 'Popup', and 'Banner'. The main area contains a table with the following data:

| Ora                 | Processo                      | Numero         | Stato |
|---------------------|-------------------------------|----------------|-------|
| 27.02.2006 18:06:23 | e:\winnt\system32\rasdial.exe | +7(495)1112233 |       |

An 'Azioni...' button is located at the bottom right of the window.

Figura 87. Elenco dei tentativi di connessione

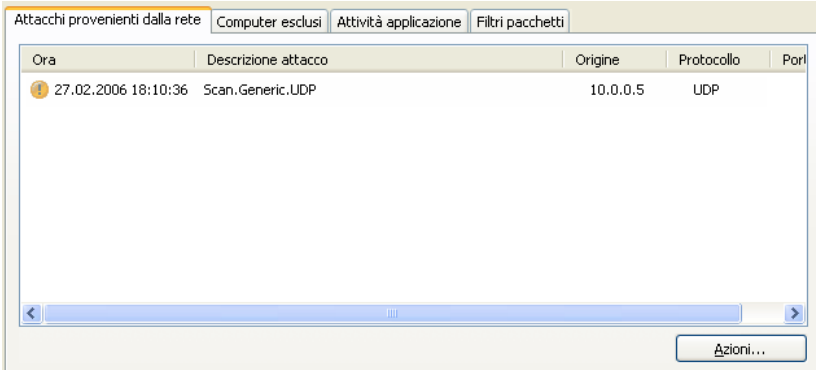
Il rapporto specifica quale programma ha tentato di comporre il numero per connettersi a Internet e se il tentativo è stato bloccato o consentito.

### 17.3.12. La scheda *Attacchi provenienti dalla rete*

Questa scheda (vedere Figura 88) visualizza una breve panoramica degli attacchi di rete sul computer. Questa informazione viene registrata se è stato abilitato il Sistema di rilevamento intrusioni, che monitora tutti i tentativi di attacco perpetrati al computer.

La scheda **Attacchi provenienti dalla rete** elenca le seguenti informazioni sugli attacchi:

- Provenienza dell'attacco. Può essere un indirizzo IP, un host, ecc.
- Porta locale sul quale è stato tentato l'attacco al computer.
- Una breve descrizione dell'attacco.
- L'ora in cui l'attacco è stato tentato.



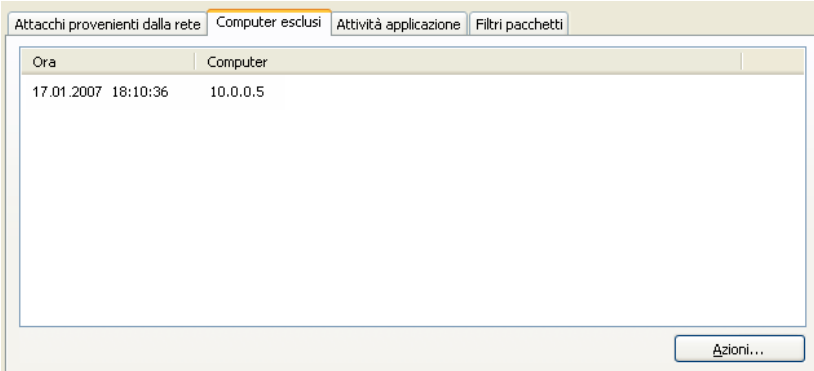
| Ora                 | Descrizione attacco | Origine  | Protocollo | Porta |
|---------------------|---------------------|----------|------------|-------|
| 27.02.2006 18:10:36 | Scan.Generic.UDP    | 10.0.0.5 | UDP        |       |

Figura 88. Elenco degli attacchi di rete intercettati

### 17.3.13. La scheda *Computer esclusi*

Tutti gli host bloccati dopo l'intercettazione di un attacco da parte del Sistema di rilevamento intrusioni sono elencati in questa scheda di rapporto (vedere Figura 89).

Sono indicati il nome di ciascun host e l'ora in cui è stato bloccato. Da questa scheda è possibile sbloccare gli host. A tal fine, selezionare l'host sulla lista e fare clic sul pulsante **Azioni** → **Sblocca**.



| Ora                 | Computer |
|---------------------|----------|
| 17.01.2007 18:10:36 | 10.0.0.5 |

Figura 89. Elenco degli host bloccati



### 17.3.14. La scheda *Attività applicazione*

Tutte le applicazioni la cui attività corrisponde alle regole dell'applicazione ed è stata registrata dal modulo *Firewall* durante la sessione corrente di Anti-Hacker, sono elencate nella scheda **Attività applicazione**. (vedere Figura 90).

L'attività è registrata solo se nella regola è selezionata l'opzione  **Registra evento**. Per impostazione predefinita, tale opzione è deselezionata nelle regole per le applicazioni incluse in Kaspersky Anti-Virus for Windows Workstations.

Questa scheda visualizza le proprietà di base di ogni applicazione (nome, PID, nome della regola) e un breve riepilogo della sua attività (protocollo, direzione pacchetti, ecc.). È specificato anche se l'attività dell'applicazione è stata bloccata.

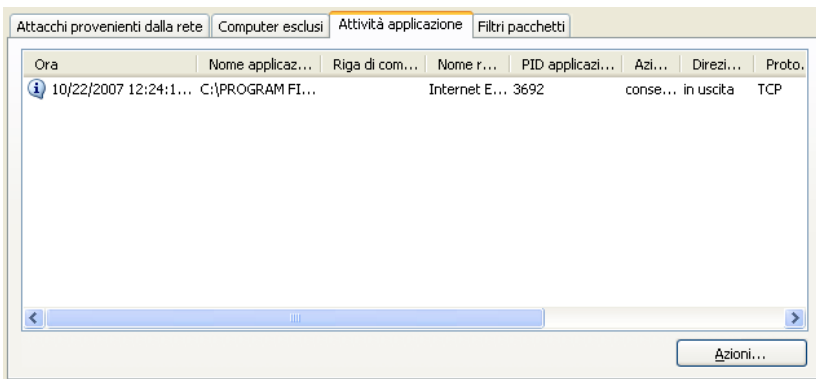


Figura 90. Attività dell'applicazione monitorata

### 17.3.15. La scheda *Filtri pacchetti*

La scheda **Filtri pacchetti** contiene informazioni sull'invio e la ricezione di pacchetti corrispondenti alle regole di filtraggio e registrati durante la sessione corrente dell'applicazione (vedere Figura 91).

L'attività è registrata solo se nella regola è selezionata l'opzione  **Registra evento**. Per impostazione predefinita, tale opzione è deselezionata nelle regole di filtro pacchetti incluse in Kaspersky Anti-Virus for Windows Workstations.

Per ogni pacchetto sono indicati il risultato dell'operazione di filtraggio (ovvero se il pacchetto sia stato bloccato o no), la direzione del pacchetto, il protocollo e altre impostazioni della connessione di rete per l'invio e la ricezione di pacchetti.

| Or                     | Nome r...   | Azi...   | Direzi...  | Proto... | Computer...   | Porta rem... | Compu...    | Pr |
|------------------------|-------------|----------|------------|----------|---------------|--------------|-------------|----|
| 10/22/2007 12:06:35 PM | ICMP Typ... | conse... | in uscita  | ICMP     | 10.10.0.100   |              | 999.99.9... |    |
| 10/22/2007 12:06:37 PM | ICMP Typ... | conse... | in uscita  | ICMP     | 10.10.0.100   |              | 999.99.9... |    |
| 10/22/2007 12:06:50 PM | ICMP Typ... | conse... | in uscita  | ICMP     | 10.10.0.100   |              | 999.99.9... |    |
| 10/22/2007 12:06:50 PM | ICMP Typ... | conse... | in entrata | ICMP     | 10.10.0.100   |              | 999.99.9... |    |
| 10/22/2007 12:06:52 PM | ICMP Typ... | conse... | in uscita  | ICMP     | 10.10.0.100   |              | 999.99.9... |    |
| 10/22/2007 12:06:52 PM | ICMP Typ... | conse... | in entrata | ICMP     | 10.10.0.100   |              | 999.99.9... |    |
| 10/22/2007 12:07:06 PM | ICMP Typ... | conse... | in uscita  | ICMP     | 99.999.99.99  |              | 999.99.9... |    |
| 10/22/2007 12:07:06 PM | ICMP Typ... | conse... | in entrata | ICMP     | 99.999.99.99  |              | 999.99.9... |    |
| 10/22/2007 12:07:06 PM | ICMP Typ... | conse... | in uscita  | ICMP     | 99.999.99.99  |              | 999.99.9... |    |
| 10/22/2007 12:07:06 PM | ICMP Typ... | conse... | in entrata | ICMP     | 99.999.99.99  |              | 999.99.9... |    |
| 10/22/2007 12:07:06 PM | ICMP Typ... | conse... | in uscita  | ICMP     | 999.999.99.99 |              | 999.99.9... |    |
| 10/22/2007 12:07:06 PM | ICMP Typ... | conse... | in uscita  | ICMP     | 999.999.99.99 |              | 999.99.9... |    |
| 10/22/2007 12:07:06 PM | ICMP Typ... | conse... | in uscita  | ICMP     | 999.999.99.99 |              | 999.99.9... |    |
| 10/22/2007 12:07:06 PM | ICMP Typ... | conse... | in uscita  | ICMP     | 999.999.99.99 |              | 999.99.9... |    |

Figura 91. Pacchetti dati monitorati

## 17.3.16. La scheda *Connessioni stabilite*

Tutte le connessioni di rete attive correntemente stabilite sul computer sono elencate nella scheda **Connessioni stabilite** (vedere Figura 92). Questa scheda riporta il nome dell'applicazione che ha iniziato la connessione, il protocollo usato, la direzione della connessione (in entrata o in uscita) e le impostazioni di connessione (porte locali e remote e indirizzi IP). Inoltre è possibile vedere per quanto tempo una connessione è stata attiva e il volume dei dati inviati e ricevuti. È possibile creare o eliminare le regole di connessione. A tal fine, utilizzare le opzioni appropriate sul menu di scelta rapida.

| Applicazione | Riga di comando | Protoc... | Direzione  | Indirizzo IP l... | Po  |
|--------------|-----------------|-----------|------------|-------------------|-----|
| System       |                 | TCP       | in entrata | 177.17.7.77       | 177 |

Figura 92. Elenco di connessioni stabilite

### 17.3.17. La scheda *Porte aperte*

Tutte le porte correntemente aperte sul computer per le connessioni di rete sono elencate nella scheda *Porte aperte* (vedere Figura 93). Essa elenca per ciascuna porta il numero, il protocollo di trasferimento dati, il nome dell'applicazione che la usa e per quanto tempo la porta è rimasta aperta.

| Porta I... | Protoc... | Applicazione  | Riga di comando  | Indirizzo IP I... |    |
|------------|-----------|---------------|------------------|-------------------|----|
| 445        | UDP       | System        |                  | 9.9.9.9           | 02 |
| 445        | TCP       | System        |                  | 999.99.9.99       | 02 |
| 138        | UDP       | System        |                  | 999.99.9.99       | 02 |
| 137        | UDP       | System        |                  | 999.99.9.99       | 02 |
| 139        | TCP       | System        |                  | 999.99.9.99       | 02 |
| 1162       | TCP       | System        |                  | 0.0.0.0           | 01 |
| 135        | TCP       | SVCHOST.EXE   | -K RPCSS         | 0.0.0.0           | 02 |
| 1025       | UDP       | SVCHOST.EXE   | -K NETWORKSER... | 0.0.0.0           | 02 |
| 1026       | UDP       | SVCHOST.EXE   | -K NETWORKSER... | 0.0.0.0           | 02 |
| 1353       | UDP       | SVCHOST.EXE   | -K NETWORKSER... | 0.0.0.0           | 00 |
| 1027       | UDP       | LSASS.EXE     |                  | 999.99.9.99       | 02 |
| 500        | UDP       | LSASS.EXE     |                  | 0.0.0.0           | 02 |
| 4500       | UDP       | LSASS.EXE     |                  | 0.0.0.0           | 02 |
| 123        | UDP       | SVCHOST.EXE   | -K NETSVCS       | 999.99.9.99       | 02 |
| 123        | UDP       | SVCHOST.EXE   | -K NETSVCS       | 999.99.9.99       | 02 |
| 1433       | TCP       | SQLSERVER.EXE | -SMSSQLSERVER    | 0.0.0.0           | 02 |

Figura 93. Elenco delle porte aperte del computer

Queste informazioni possono essere utili durante le pandemie virali e gli attacchi di rete se si sa con esattezza quale porta sia vulnerabile. Si può scoprire se quella porta sia aperta sul computer e prendere le misure necessarie per proteggere il computer (per esempio, abilitare Intrusion Detector, chiudere la porta vulnerabile, o creare una regola per tale porta).

### 17.3.18. La scheda *Traffico*

Questa scheda (vedere Figura 94) contiene informazioni su tutte le connessioni in entrata e in uscita stabilite tra il computer dell'utente e altri computer, inclusi web server, server di posta, ecc. Per ogni connessione sono fornite le seguenti informazioni: nome e indirizzo IP dell'host con cui è stabilita la connessione e volume di traffico inviato e ricevuto.

| Computer                  | Indirizzo IP   | Rice...  | Inviati  |
|---------------------------|----------------|----------|----------|
| ak-170-2k-srv2            | 999.99.9.99    | 5,2 KB   | 4,2 KB   |
| f601.avp.ru               | 999.99.9.99    | 525 byte | 0 byte   |
| voitenko.avp.ru           | 999.99.9.99    | 3,1 KB   | 1,9 KB   |
| ak-installtest.ak.ak20... | 999.99.9.99    | 5,2 KB   | 4,2 KB   |
| samsonov.avp.ru           | 999.99.9.99    | 1,5 KB   | 0 byte   |
| moscow3.avp.ru            | 999.99.9.99    | 51,9 KB  | 38,6 KB  |
| samson-vm.avp.ru          | 999.99.9.99    | 700 byte | 0 byte   |
| moscow4.avp.ru            | 999.99.9.99    | 312,9 KB | 340,7 KB |
| moscow2.avp.ru            | 999.99.9.99    | 43 KB    | 52 KB    |
| 91.103.64.7               | 999.99.9.99    | 4,1 KB   | 4,2 KB   |
| monastyrsky.avp.ru        | 777.77.777.777 | 525 byte | 0 byte   |
| s50-70-xp                 | 999.99.9.99    | 3 KB     | 0 byte   |
| tl-wmware-xpp             | 777.77.777.777 | 31,0 KB  | 0 byte   |
| volkovan.avp.ru           | 999.99.9.99    | 0 byte   | 186 byte |
| balesteros                | 999.99.9.99    | 525 byte | 0 byte   |
| uliss-xp.avp.ru           | 999.99.9.99    | 10,5 KB  | 6,8 KB   |
| petrov.avp.ru             | 999.99.9.99    | 1 KB     | 0 byte   |
| lebedev-a.avp.ru          | 999.99.9.99    | 525 byte | 0 byte   |
| tl-vmx-v64u2.avp.ru       | 777.77.777.777 | 3,4 KB   | 0 byte   |
| vmware-xp-nl              | 999.99.9.99    | 3 KB     | 0 byte   |
| windowsupdates.kas...     | 77.777.77.77   | 125 KB   | 210,5 KB |

Figura 94. Traffico sulle connessioni di rete stabilite

## 17.4. Informazioni generali sul programma

Le informazioni generali sul programma sono riportate nella sezione **Servizio** della finestra principale (vedere Figura 95).

Tutte le informazioni sono suddivise in tre sezioni:

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

Tutte queste informazioni sono necessarie qualora ci si rivolga al servizio di assistenza tecnica di Kaspersky Lab (vedere 17.6 a pag. 263).

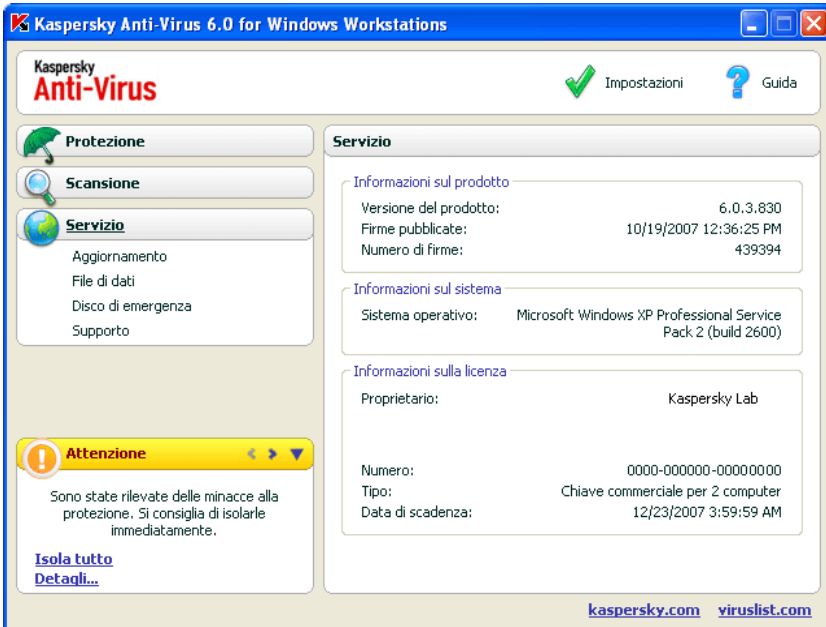


Figura 95. Informazioni sul programma, la licenza ed il sistema sul quale è installato.

## 17.5. Gestione delle licenze

Per funzionare, Kaspersky Anti-Virus for Windows Workstations richiede una *chiave di licenza*. La chiave, fornita all'acquisto del programma, dà diritto all'uso del programma dal giorno di installazione della chiave stessa.

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

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

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

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

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

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

*oppure:*

Acquistare una chiave di licenza o un codice di attivazione direttamente da Kaspersky Lab facendo clic sul collegamento **Acquista licenza** (vedere Figura 96). Compilare il modulo nella pagina Web che si apre. Dopo il pagamento, verrà inviato all'indirizzo di posta elettronica specificato nel modulo d'ordine un collegamento. Esso consentirà di scaricare una chiave di licenza o di ottenere un codice di attivazione per l'applicazione.

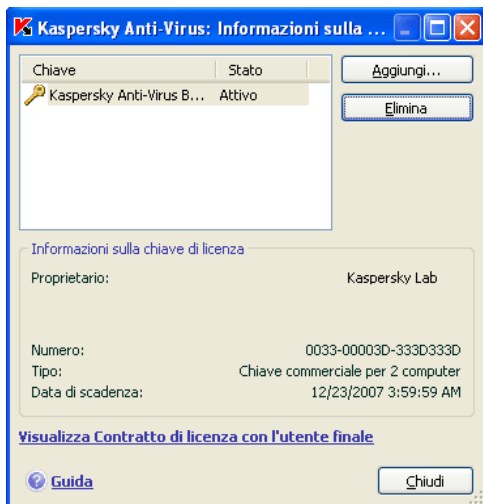


Figura 96. Informazioni sulla licenza

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

Le informazioni sulla chiave di licenza corrente sono disponibili nel riquadro **Informazioni sulla licenza** nella sezione **Servizio** della finestra principale dell'applicazione. Per raggiungere la finestra di gestione delle licenze, fare clic

ovunque nel riquadro. La finestra che si apre (vedere Figura 96) consente di visualizzare le informazioni sulla chiave di licenza corrente, o di eliminarne una.

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

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

## 17.6. Supporto tecnico

Kaspersky Anti-Virus for Windows Workstations offre una vasta gamma di opzioni per porgere domande e risolvere problemi relativi al funzionamento del programma. Queste risposte sono fornite sotto **Supporto** (vedere Figura 97) nella sezione **Servizio**.

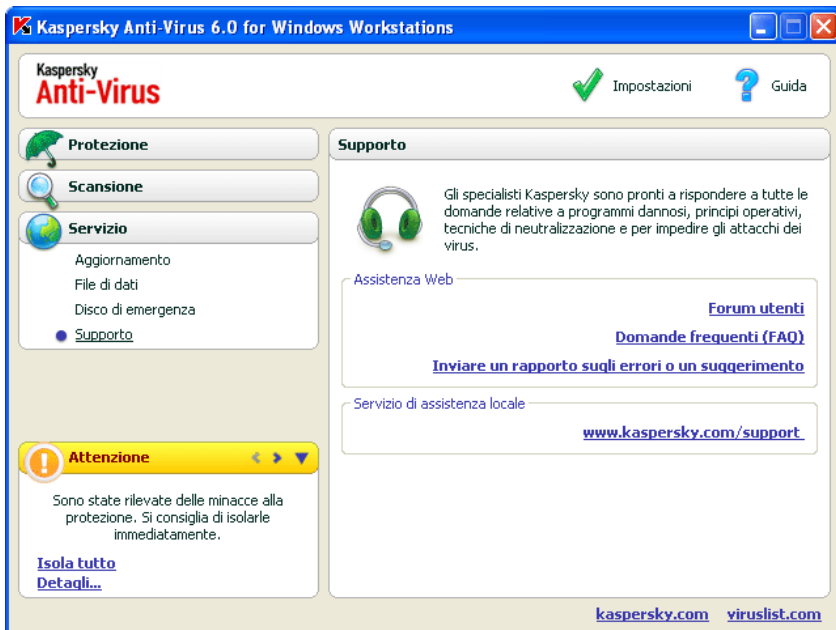


Figura 97. Informazioni sul servizio di assistenza tecnica

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

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

Per accedere a questa risorsa, utilizzare il collegamento [Forum utenti](#).

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

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

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

Per andare al modulo dei commenti, utilizzare il collegamento [Inviare un rapporto sugli errori o un suggerimento](#).

**Assistenza tecnica.** Se si necessita di assistenza tecnica durante l'utilizzo di Kaspersky Anti-Virus, fare clic sul collegamento ubicato nel riquadro **Servizio di assistenza locale**. Si aprirà il sito Web di Kaspersky Anti-Virus con informazioni su come contattare i nostri esperti.

## 17.7. Creazione di un elenco delle porte monitorate

I componenti di protezione come Anti-Virus posta, Web Anti-Virus, Anti-Spy e Anti-Spam, monitorano i flussi di dati trasmessi utilizzando determinati protocolli e che passano attraverso determinate porte del computer. Così, per esempio, Anti-Virus posta analizza le informazioni trasmesse per mezzo del protocollo SMTP mentre Web Anti-Virus analizza quelle trasmesse mediante HTTP.



Il pacchetto del programma include un elenco delle porte standard più utilizzate per la trasmissione della posta e del traffico HTTP. È possibile aggiungere una nuova porta o disabilitare il monitoraggio di una esistente disabilitando in tal modo il rilevamento di oggetti pericolosi nel traffico che passa attraverso la porta in questione.

*Per modificare l'elenco delle porte monitorate procedere come segue:*

1. Aprire la finestra delle impostazioni di Kaspersky Anti-Virus for Windows Workstations facendo clic sul collegamento Impostazioni nella finestra principale.
2. Selezionare **Impostazioni di rete** nella sezione **Servizio** della struttura ad albero delle impostazioni del programma.
3. Nella parte destra della finestra delle impostazioni, fare clic su **Impostazioni porta**.
4. Modificare la lista delle porte monitorate nella finestra che si apre (vedere Figura 98).



Figura 98. Elenco delle porte monitorate

Questa finestra offre un elenco delle porte monitorate da Kaspersky Anti-Virus. Per esaminare tutti i flussi di dati in entrata su tutte le porte di rete aperte, selezionare l'opzione  **Controlla tutte le porte**. Per modificare l'elenco di porte monitorate manualmente, selezionare  **Controlla solo le porte selezionate**.

È sconsigliabile selezionare l'opzione **Controlla tutte le porte** quando si amministra Kaspersky Anti-Virus 6.0 tramite Kaspersky Administration Kit, se installato su un computer che esegue Microsoft Windows 98. In caso contrario, potrebbero esserci problemi nell'accedere alle risorse di rete e ad Internet.

Per aggiungere una nuova porta all'elenco delle porte monitorate:

1. Fare clic sul pulsante **Aggiungi** nella finestra **Impostazioni porta**.
2. Immettere il numero della porta e una descrizione nei relativi campi nella finestra **Nuova porta**.

Per esempio, potrebbe esserci una porta non standard sul computer attraverso la quale vengono scambiati i dati con un computer remoto utilizzando il protocollo HTTP, che viene monitorata da Web Anti-Virus. Per analizzare questo traffico in cerca di codici nocivi, è possibile aggiungere la porta a un elenco di porte controllate.

All'avvio di qualsiasi dei suoi componenti, Kaspersky Anti-Virus for Windows Workstations apre la porta 1110 come una porta di ascolto per tutte le connessioni in entrata. Se in quel momento la porta è occupata, seleziona le porte 1111, 1112, ecc.

Se si usa Kaspersky Anti-Virus for Windows Workstations e il firewall di un altro produttore contemporaneamente, occorre configurare il firewall in modo da autorizzare il processo *avp.exe* (processo interno di Kaspersky Anti-Virus for Windows Workstations ) ad accedere a tutte le porte sopra elencate.

Per esempio, supponiamo che il firewall contenga una regola per *iexplorer.exe* che autorizza quel processo per stabilire le connessioni sulla porta 80.

Tuttavia, quando Kaspersky Anti-Virus for Windows Workstations intercetta la richiesta di connessione lanciata da *iexplorer.exe* sulla porta 80, la trasferisce a *avp.exe*, che a sua volta cerca di connettersi alla pagina web in modo indipendente. Se non esiste una regola di autorizzazione di *avp.exe*, la firewall blocca quella richiesta. L'utente a questo punto non potrà accedere alla pagina web.

## 17.8. Controllo delle connessioni crittografate

Le connessioni effettuate con il protocollo SSL proteggono lo scambio di dati tramite Internet. Il protocollo SSL è in grado di identificare le parti che si scambiano dati tramite certificati elettronici, crittografare i dati trasferiti e garantirne l'integrità durante il trasferimento.

Queste funzioni del protocollo vengono utilizzate dai pirati informatici per diffondere programmi nocivi, poiché quasi tutti i programmi antivirus non esaminano il traffico SSL.

Kaspersky Anti-Virus 6.0 offre l'opzione di esaminare il traffico SSL alla ricerca di virus. In caso di tentativo di connessione protetta ad una risorsa Web, verrà visualizzata una notifica sullo schermo (vedere Figura 99) che richiede l'intervento dell'utente.

Essa contiene informazioni sul programma che ha avviato la connessione protetta, unitamente all'indirizzo remoto ed alla porta remota. Il programma chiede di decidere se la connessione debba essere esaminata alla ricerca di virus:

- **Processa** – esamina il traffico alla ricerca di virus in caso di connessione protetta ad un sito Web.

Si consiglia di esaminare sempre il traffico SSL se ci si sta collegando ad un sito Web sospetto o se parte un trasferimento SSL quando si passa alla pagina successiva. È assai probabile che ciò segnali il trasferimento di un programma nocivo sul protocollo protetto.

- **Salta** – continua la connessione protetta senza esaminare il traffico alla ricerca di virus.

Per applicare l'azione selezionata a tutti i futuri tentativi di stabilire una connessione SSL, selezionare  **Applica a tutti**.

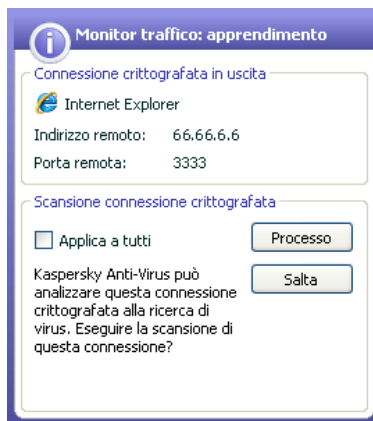


Figura 99. Notifica su rilevamento di una connessione SSL

Per esaminare le connessioni crittografate, Kaspersky Anti-Virus sostituisce il certificato di sicurezza richiesto con un certificato firmato dall'applicazione stessa. In alcuni casi, i programmi che stabiliscono la connessione non

accetteranno questo certificato e la connessione non può essere stabilita. Si consiglia di disattivare la scansione del traffico SSL nei seguenti casi:

- Durante il collegamento ad una risorsa Web attendibile, ad esempio la pagina Web della propria banca, dal quale gestire il proprio conto corrente. In questo caso, è importante che l'autenticità del certificato della banca venga confermata.
- Se il programma che stabilisce la connessione verifica il certificato del sito web al quale si accede. Ad esempio, MSN Messenger verifica l'autenticità della firma digitale di Microsoft Corporation quando stabilisce una connessione al server.

È possibile configurare le impostazioni della scansione SSL dalla sezione **Connessioni crittografate** (SSL/TLS) della finestra delle impostazioni del programma:

**Controlla tutte le connessioni crittografate** – esamina tutto il traffico in entrata tramite protocollo SSL alla ricerca di virus.

**Richiedi all'utente quando viene rilevata una nuova connessione crittografata** – visualizza un messaggio che richiede l'intervento dell'utente ogniqualvolta viene stabilita una connessione SSL.

**Non controllare connessioni crittografate** – non esamina il traffico in entrata tramite protocollo SSL alla ricerca di virus.

## 17.9. Configurazione dell'interfaccia di Kaspersky Anti-Virus for Windows Workstations

Kaspersky Anti-Virus for Windows Workstations offre la possibilità di modificare l'aspetto del programma creando e utilizzando nuovi stili. È possibile inoltre configurare l'uso degli elementi di interfaccia attiva come l'icona della barra delle applicazioni e i messaggi pop-up.

*Per configurare l'interfaccia del programma procedere come segue:*

1. Aprire la finestra delle impostazioni di Kaspersky Anti-Virus for Windows Workstations facendo clic sul collegamento Impostazioni nella finestra principale.
2. Selezionare **Aspetto** nella sezione **Servizio** della struttura ad albero delle impostazioni del programma (vedere Figura 100).

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

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

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

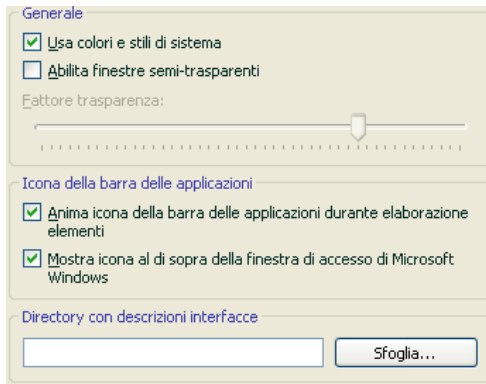


Figura 100. Configurazione dell'aspetto dell'interfaccia del programma

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

A seconda dell'operazione eseguita dal programma, l'icona dell'area di notifica cambia. Per esempio, durante la scansione di uno script compare sullo sfondo dell'icona l'immagine miniaturizzata di uno script, mentre durante la scansione di un messaggio di posta compare una busta. L'animazione dell'icona è abilitata per impostazione predefinita. Per disabilitare l'animazione, deselezionare  **Anima icona della barra delle applicazioni durante elaborazione elementi.** Da quel momento in poi l'icona rappresenta solo lo stato di protezione del computer: se la protezione è abilitata l'icona è a colori, mentre se la protezione è sospesa o disabilitata l'icona diventa grigia.

- Grado di trasparenza dei messaggi a comparsa.

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

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

Questa funzione non è disponibile in Windows 98/NT 4.0/ME.

- Applicare stili personalizzati all'interfaccia del programma.

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

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

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

## 17.10. Disco di emergenza

Kaspersky Anti-Virus for Windows Workstations dispone di uno strumento per creare un disco di emergenza.

Il disco di emergenza è progettato per consentire il ripristino della funzionalità del sistema dopo un attacco virale che ha danneggiato i file di sistema rendendo impossibile l'avvio del sistema operativo. Il disco include:

- File di sistema di Microsoft Windows XP Service Pack 2
- Una serie di utilità diagnostiche per il sistema operativo
- I file di programma di Kaspersky Anti-Virus for Windows Workstations
- I file contenenti gli elenchi delle minacce

*Per creare un disco di emergenza:*

1. Aprire la finestra principale del programma e selezionare **Disco di emergenza** nella sezione **Servizio**.
2. Fare clic sul pulsante **Avvia procedura guidata** per avviare la creazione del disco.

Il disco di emergenza viene creato per il computer sul quale è stato creato. L'utilizzo del disco su altri computer può determinare conseguenze imprevedibili, poiché contiene informazioni sui parametri relativi ad un computer specifico (le informazioni sui settori di boot, ad esempio).

La creazione di un disco di emergenza è possibile solo con Windows XP e Microsoft Windows Vista. Non è possibile creare dischi di emergenza sui computer che eseguono Microsoft Windows XP Professional x64 Edition o Microsoft Windows Vista x64.

## 17.10.1. Creazione di un disco di emergenza

**Attenzione!** Per creare un disco di emergenza occorre disporre del disco di installazione di Microsoft Windows XP Service Pack 2.

Per creare il disco di emergenza, occorre il programma **PE Builder**.

**È necessario installare PE Builder sul computer prima di creare un disco tramite il programma.**

La creazione del disco di emergenza è agevolata da un'apposita procedura guidata che consiste in una serie di finestre/passaggi fra i quali navigare servendosi dei pulsanti **Indietro** e **Avanti**. Per completare la procedura guidata fare clic su **Fine**. Per uscire dalla procedura in qualsiasi momento, fare clic su **Annulla**.

### Passaggio 1. La scrittura del disco

Per creare un disco di emergenza, specificare il percorso alle seguenti cartelle:

- Cartella del programma PE Builder
- Cartella in cui vengono salvati i file del disco di emergenza prima di masterizzare il CD

Se non è la prima volta che si crea un disco di emergenza, questa cartella contiene già una serie di file creati la volta precedente. Per usare i file salvati in precedenza, selezionare la cartella corrispondente.

Si noti che la versione precedente dei file del disco di emergenza conterrà elenchi delle minacce obsoleti. Per eseguire la scansione antivirus del computer e ripristinare il sistema in maniera ottimale, si raccomanda di aggiornare gli elenchi delle minacce e di creare una nuova versione del disco di emergenza.

- Il CD di installazione di Microsoft Windows XP Service Pack 2

Per creare un disco di ripristino in grado di avviare il sistema operativo su un computer remoto ed esaminare e trattare il codice nocivo utilizzando Kaspersky Anti-Virus, selezionare  **Abilita amministrazione remota del computer ripristinato.**

Si noti che, per utilizzare questa funzione, il computer remoto deve supportare Intel® vPro™ o Intel® Active Management Technology (iAMT). Queste tecnologie consentono agli amministratori di accedere in remoto a tutti computer della rete, compresi quelli spenti o che hanno dischi o sistemi operativi compromessi.

Dopo aver immesso i percorsi alle cartelle necessarie, fare clic su **Avanti**. PE Builder si avvia e ha inizio il processo di creazione del disco di emergenza. Attendere il completamento del processo. L'operazione potrebbe richiedere diversi minuti.

## Passaggio 2. Creazione di un file .iso

Dopo che PE Builder ha completato la creazione dei file del disco di emergenza, si apre la finestra **Crea file .iso**.

Il file .iso è un'immagine su CD del disco salvata come archivio. La maggior parte dei programmi di masterizzazione CD è in grado di riconoscere correttamente i file .iso (Nero, per esempio).

Se non è la prima volta che si crea un disco di emergenza, è possibile selezionare il file .iso dal disco precedente. A tal fine, selezionare **File ISO esistente**.

## Passaggio 3. Masterizzazione del disco

La finestra della procedura guidata chiede all'utente se masterizzare i file del disco di emergenza su CD ora o più tardi.

Se si decide di masterizzare immediatamente il disco, specificare se si desidera formattare il disco prima di procedere, selezionando la casella corrispondente. Questa opzione è disponibile solo se si usano dischi CD-RW.

Per avviare la masterizzazione del CD fare clic sul pulsante **Avanti**. Attendere il completamento del processo. L'operazione potrebbe richiedere diversi minuti.



## Passaggio 4. Completamento del disco di emergenza

La finestra della procedura guidata informa l'utente che la creazione del disco di emergenza è stata completata con esito positivo.

### 17.10.2. Uso del disco di emergenza

Osservare che Kaspersky Anti-Virus funziona in modalità provvisoria solo se la finestra principale è aperta. Chiudendo la finestra principale si chiude anche il programma.

Bart PE, il programma predefinito, non supporta i file .chm o i browser di Internet, pertanto in modalità provvisoria non è possibile visualizzare la Guida di Kaspersky Anti-Virus o i link dell'interfaccia del programma.

Se in seguito a un attacco di virus è impossibile caricare il sistema operativo, procedere come segue:

1. Creare un disco di boot di emergenza utilizzando Kaspersky Anti-Virus for Windows Workstations su un computer non infetto.
2. Inserire il disco di emergenza nell'unità disco del computer infetto e riavviare. Microsoft Windows XP SP2 si avvia con l'interfaccia Bart PE. Bart PE presenta un supporto di rete incorporato per l'utilizzo della LAN. All'avvio del programma, viene richiesto se si desidera abilitarlo. Autorizzare l'abilitazione del supporto di rete se si prevede di aggiornare l'elenco dei virus dalla LAN prima di eseguire la scansione del computer. Se non è necessario aggiornare i file, disabilitare il supporto di rete.
3. Per aprire Kaspersky Anti-Virus, fare clic su **Start**→**Tutti i programmi**→**Kaspersky Anti-Virus 6.0 for Windows Workstations**→**Avvio**.

Si apre la finestra principale di Kaspersky Anti-Virus for Windows Workstations. In modalità provvisoria è possibile accedere solo alle scansioni antivirus e agli aggiornamenti degli elenchi delle minacce dalla LAN (se era stato abilitato il supporto di rete in Bart PE).

4. Avviare la scansione antivirus.

Si noti che per impostazione predefinita vengono utilizzati gli elenchi delle minacce risalenti alla data in cui è stato creato il disco di emergenza. Per questa ragione, si consiglia di aggiornare gli elenchi prima di avviare la scansione.

Si noti inoltre che l'applicazione utilizzerà esclusivamente gli elenchi delle minacce aggiornati durante la sessione corrente col disco di ripristino, prima di riavviare il computer.

### Attenzione!

Se durante la scansione del computer sono stati rilevati oggetti infetti o potenzialmente infetti che sono stati trattati e poi spostati in quarantena o nella memoria di backup, si consiglia di completare il trattamento di tali oggetti durante la sessione corrente col disco di emergenza.

In caso contrario, tali oggetti andranno persi al riavvio del computer.

## 17.11. Utilizzo di servizi supplementari

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

- Notifiche di determinati eventi che si verificano nel programma.
- Autodifesa di Kaspersky Anti-Virus for Windows Workstations dalla disattivazione, eliminazione o modifica dei moduli, nonché protezione del programma tramite password.
- Risoluzione dei conflitti tra Kaspersky Anti-Virus 6.0 e altre applicazioni.

*Per configurare queste funzioni:*

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

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

## 17.11.1. Notifica eventi di Kaspersky Anti-Virus for Windows Workstations

Durante l'uso di Kaspersky Anti-Virus for Windows Workstations si verificano diversi tipi di eventi. Le notifiche corrispondenti possono essere informative o contenere dati importanti. Per esempio, un messaggio può informare dell'avvenuto aggiornamento del programma oppure registrare l'errore di un componente da risolvere immediatamente.

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

Le notifiche possono essere trasmesse in vari modi:

- In forma di messaggi a comparsa sopra l'icona del programma nella barra delle applicazioni
- Con segnali acustici
- Messaggi di posta elettronica
- Registrare tutti gli eventi nel registro eventi

*Per usare questa funzione procedere come segue:*

1. Selezionare  **Abilita notifiche** nella casella **Interazione con l'utente** (vedere Figura 101).

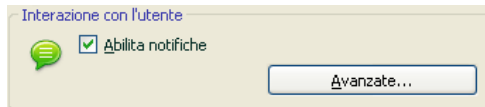


Figura 101. Abilitazione delle notifiche

2. Definire i tipi di eventi di Kaspersky Anti-Virus for Windows Workstations per i quali si desidera essere informati e il metodo di notifica (vedere 17.11.1.1 a pag. 275).
3. Configurare le impostazioni di consegna delle notifiche via posta elettronica, se questo è il metodo utilizzato (vedere 17.11.1.2 a pag. 277).

### 17.11.1.1. Tipi di eventi e metodo di notifica

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

**Notifiche critiche** – eventi di importanza cruciale. Si raccomanda di abilitare gli avvisi, poiché questo tipo di eventi segnala la presenza di problemi di funzionamento del programma o di vulnerabilità della protezione del computer. Per esempio, *il danneggiamento dell'elenco dei virus o il fatto che la licenza è scaduta*.

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

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

**Notifiche minori** – messaggi di riferimento che di solito non contengono informazioni rilevanti. Per esempio, *comunicano quali sono tutti gli oggetti pericolosi puliti*.

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

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

È possibile configurare i seguenti metodi di notifica per gli eventi sopra elencati nella finestra **Impostazioni notifica** che si apre (vedere Figura 102):

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

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

- *Segnale acustico*

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

- *Notifica via posta elettronica*

Per utilizzare questo tipo di notifica, selezionare la colonna  **Email** opposta all'evento di cui si desidera essere informati e configurare le impostazioni per l'invio delle notifiche (vedere 17.11.1.2 a pag. 277).

- *Registrazione di tutti gli eventi nel registro eventi*

Per registrare nel log le informazioni su qualsiasi evento verificatosi, selezionare  nella colonna **Registro** e configurare le impostazioni del registro eventi (vedere 17.11.1.3 a pag. 278).

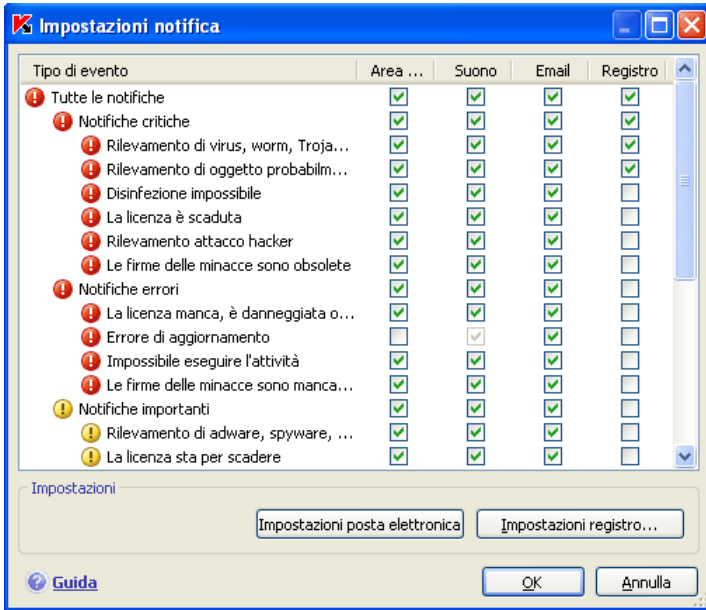


Figura 102. Eventi del programma e metodi di notifica eventi

### 17.11.1.2. Configurazione delle notifiche via posta elettronica

Dopo aver selezionato gli eventi (vedere 17.11.1.1 a pag. 275) dei quali si desidera essere informati per e-mail, è necessario configurare la consegna dell'avviso. Per fare ciò:

1. Aprire la finestra delle impostazioni del programma con il collegamento **Impostazioni** nella finestra principale.
2. Selezionare **Servizio** dalla struttura ad albero delle impostazioni.
3. Fare clic su **Avanzate** nel riquadro **Interazione con l'utente** nella parte destra dello schermo.
4. Nella scheda **Impostazioni di notifica** (vedere Figura 102), selezionare la casella di controllo  nella colonna **Email** per gli eventi che prevedono l'invio di un messaggio di posta elettronica.
5. Nella finestra che si apre facendo clic su **Impostazioni posta elettronica**, configurare le seguenti impostazioni per l'invio di notifiche via posta elettronica:

- Impostare la notifica di invio in **Da – Indirizzo e-mail**.
- Specificare l'indirizzo e-mail a cui inviare gli avvisi in **A – Indirizzo e-mail**.
- Impostare il metodo di avviso per e-mail in **Modalità invio**. Se si desidera che il programma invii il messaggio non appena l'evento si verifica, selezionare  **Immediatamente quando l'evento si verifica**. Per la notifica di eventi entro un determinato periodo di tempo, impostare il calendario di invio dei messaggi informativi facendo clic su **Cambia**. Gli invii quotidiani sono l'impostazione predefinita.

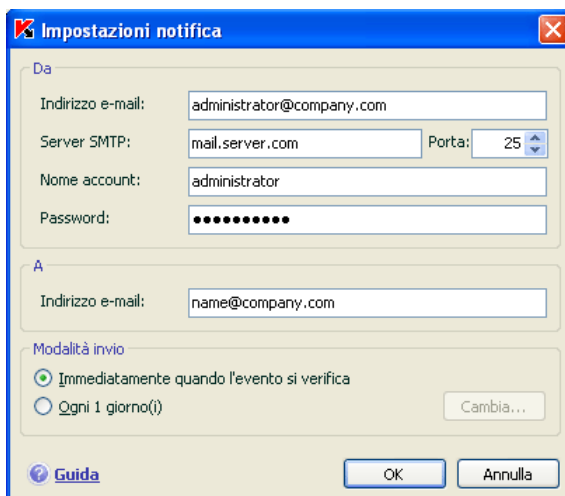


Figura 103. Configurazione delle notifiche via posta elettronica

### 17.11.1.3. Configurazione delle impostazioni del registro eventi

*Configurare le impostazioni del registro eventi:*

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

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

Kaspersky Anti-Virus offre l'opzione di registrare le informazioni sugli eventi che si verificano mentre il programma è in esecuzione, sia nel registro eventi generale di MS Windows (**Applicazione**) che nel registro eventi dedicato di Kaspersky Anti-Virus (**Registro eventi Kaspersky**).

In Microsoft Windows 98/ME, è impossibile registrare gli eventi nel registro eventi. In Microsoft Windows NT 4.0, è impossibile registrare gli eventi nel **Registro eventi Kaspersky**.

Tali limiti sono dovuti alle caratteristiche di questi sistemi operativi.

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

## 17.11.2. Protezione automatica e limitazioni d'accesso

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

Inoltre è possibile che più utenti si servano dello stesso PC, con diversi gradi di competenza nel suo utilizzo. Lasciare libero accesso al programma e alle sue impostazioni, pertanto, riduce considerevolmente la sicurezza del computer.

Per garantire la stabilità del sistema operativo, il programma è stato dotato di meccanismi di protezione automatica, protezione dall'accesso remoto e protezione mediante password.

Questa opzione non è disponibile se si sta eseguendo Kaspersky Anti-Virus in Microsoft Windows 98/ME.

Nei computer che utilizzano sistemi operativi a 64 bit e Microsoft Windows Vista, l'autodifesa è disponibile solo per impedire la modifica o l'eliminazione dei file del programma sui dischi locali e le relative voci del registro di sistema.

*Per abilitare la protezione automatica:*

1. Aprire la finestra delle impostazioni del programma tramite il collegamento Impostazioni della finestra principale.

2. Selezionare **Servizio** dalla struttura ad albero delle impostazioni.
3. Effettuare le seguenti configurazioni nella sezione **Auto-difesa** (vedere Figura 104):

- Abilita Auto-Difesa.** Se questa casella è selezionata, il programma protegge i propri file, processi di memoria e voci del registro di sistema dalla cancellazione o dalla modifica.
- Disabilita controllo servizio esterno.** Se questa casella è selezionata, qualsiasi tentativo di uso del programma da parte di amministrazioni remote viene bloccato.

In presenza di qualsiasi azione tra quelle sopra elencate, viene visualizzato un messaggio sopra l'icona del programma nell'area di notifica (se il servizio di notifica non è stato disabilitato dall'utente).

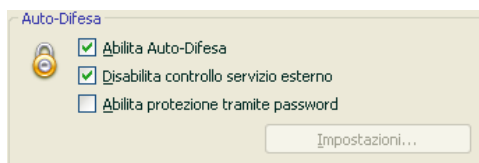


Figura 104. Configurazione della protezione automatica

Per proteggere il programma mediante password, selezionare la casella  **Abilita protezione tramite password**. Fare clic sul pulsante **Impostazioni** per aprire la finestra **Protezione tramite password** ed immettere la password e l'area coperta dalla restrizione di accesso (vedere Figura 105). È possibile bloccare qualsiasi operazione del programma, ad eccezione della notifica di rilevamento di oggetti pericolosi, o impedire l'esecuzione di qualsiasi tra le seguenti azioni:

- Modifica delle impostazioni del programma
- Chiudere Kaspersky Anti-Virus for Windows Workstations
- Disattivazione o sospensione della protezione del computer

Ognuna di queste azioni riduce il livello di protezione del computer, pertanto si consiglia di stabilire quali utenti del computer si ritiene affidabili al punto da autorizzarli a compiere tali azioni.

Selezionando questa opzione, ogni volta che un utente del computer cerca di eseguire le azioni selezionate, il programma richiede sempre una password.



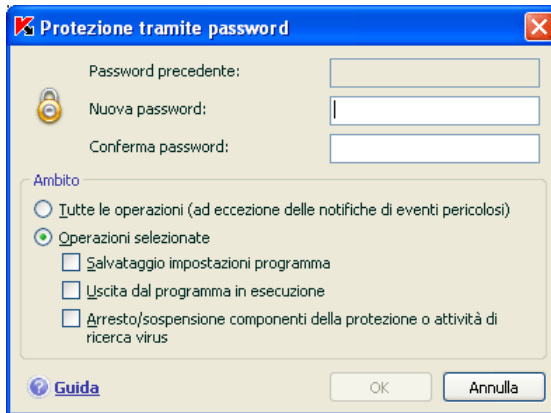


Figura 105. Impostazioni di protezione del programma tramite password

### 17.11.3. Risoluzione dei conflitti con altre applicazioni

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

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

**Se Kaspersky Anti-Virus viene installato su un computer che esegue Microsoft Windows Vista o Microsoft Windows Vista x64, non è possibile risolvere i problemi di compatibilità con altre applicazioni.**

Tuttavia, si tenga presente che abilitando questa casella di controllo, alcune funzioni di Kaspersky Anti-Virus come Office Guard e Anti-Dialer non saranno disponibili. Se si abilita uno di questi componenti, la compatibilità con l'autodifesa dell'applicazione verrà automaticamente disattivata. Una volta attivati, questi componenti inizieranno ad operare solo dopo il riavvio del computer.

## 17.12. Importazione ed esportazione delle impostazioni di Kaspersky Anti-Virus for Windows Workstations

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

Questa funzione risulta utile nei casi in cui, per esempio, il programma è installato sia nel computer di casa sia in quello dell'ufficio. È possibile configurare le impostazioni preferite del programma sul computer di casa, salvare queste impostazioni su un disco e, servendosi della funzione di importazione, caricarle sul computer in ufficio. Le impostazioni vengono salvate in uno speciale file di configurazione.

*Per esportare le impostazioni correnti del programma:*

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

*Per importare le impostazioni da un file di configurazione:*

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

## 17.13. Ripristino delle impostazioni predefinite

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

*Per ripristinare le impostazioni di protezione:*

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

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

La finestra elenca i componenti del programma le cui impostazioni sono state modificate dall'utente, o configurate man mano dal programma stesso durante l'autoapprendimento (Anti-Hacker o Anti-Spam). Qualora fossero state create impostazioni speciali per uno o più componenti, anch'esse saranno visualizzate nell'elenco.

Esempi di impostazioni speciali sono le liste bianche e nere di espressioni e indirizzi utilizzati da Anti-Spam, elenchi di indirizzi e di numeri di ISP affidabili utilizzati da Web Anti-Virus e Anti-Spy, regole di esclusione create per componenti del programma, regole di applicazioni e filtraggio di pacchetti per Anti-Hacker, e regole di applicazioni per Difesa proattiva.

Questi elenchi vengono solitamente creati man mano che si utilizza il programma, in base alle attività individuali e ai requisiti di sicurezza; la loro creazione richiede spesso un certo tempo. Pertanto, si consiglia di salvarle prima di resettare le impostazioni del programma.

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

Dopo aver configurato le impostazioni, fare clic sul pulsante **Avanti**. Si apre la procedura guidata di configurazione iniziale (vedere 3.2 a pag. 38). Seguire le istruzioni.

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

---

# CAPITOLO 18. USO DEL PROGRAMMA DA RIGA DI COMANDO

Kaspersky Anti-Virus può essere utilizzato da riga di comando eseguendo le seguenti operazioni:

- Avvio, arresto, sospensione e ripristino dell'attività dei componenti dell'applicazione
- Avvio, arresto, pausa e ripristino delle scansioni antivirus
- Ottenimento di informazioni sullo status corrente di componenti, attività e statistiche
- Scansione degli oggetti selezionati
- Aggiornamento degli elenchi delle minacce e dei moduli del programma
- Accesso alla Guida per consultare la sintassi dei prompt di comando
- Accesso alla Guida per consultare la sintassi dei comandi

La sintassi da riga di comando è la seguente:

```
avp.com <command> [settings]
```

È necessario accedere al programma dalla riga di comando dalla cartella d'installazione del programma o specificando il percorso completo a `avp.com`

Quando segue può essere utilizzato come `<commands>`:

|                 |   |
|-----------------|---|
| <b>ADDKEY</b>   | Attiva l'applicazione utilizzando una chiave di licenza (il comando può essere eseguito solo inserendo la password assegnata tramite l'interfaccia del programma) |
| <b>ACTIVATE</b> | Attiva l'applicazione on-line utilizzando il codice di attivazione.   |
| <b>START</b>    | Avvia un componente o attività  |

|                   |  |
|-------------------|--|
| <b>PAUSE</b>      | Sospende un componente o un'attività (il comando può essere eseguito solo inserendo la password assegnata tramite l'interfaccia del programma)                                     |
| <b>RESUME</b>     | Ripristina l'uso di un componente o un'attività  |
| <b>STOP</b>       | Arresta un componente o un'attività (il comando può essere eseguito solo inserendo la password assegnata tramite l'interfaccia del programma)                                      |
| <b>STATUS</b>     | Visualizza lo status del componente o attività correnti  |
| <b>STATISTICS</b> | Visualizza le statistiche del componente o attività  |
| <b>HELP</b>       | Fornisce indicazioni sulla sintassi dei comandi e sull'elenco dei comandi  |
| <b>SCAN</b>       | Esegue la scansione antivirus di oggetti   |
| <b>UPDATE</b>     | Avvia l'aggiornamento del programma  |
| <b>ROLLBACK</b>   | Ripristina la versione precedente dopo un aggiornamento (il comando può essere eseguito solo inserendo la password assegnata tramite l'interfaccia del programma)                  |
| <b>EXIT</b>       | Chiude il programma (è possibile eseguire questo comando solo con la password impostata nell'interfaccia del programma)  |
| <b>IMPORT</b>     | Importa le impostazioni di Kaspersky Anti-Virus for Windows Workstations (il comando può essere eseguito solo inserendo la password assegnata tramite l'interfaccia del programma) |
| <b>EXPORT</b>     | Esporta le impostazioni di Kaspersky Anti-Virus for Windows Workstations   |

Ogni comando utilizza le proprie impostazioni specifiche per il particolare componente di Kaspersky Anti-Virus for Windows Workstations.

## 18.1. Attivazione dell'applicazione

Due sono i metodi per attivare l'applicazione:

- on-line utilizzando un codice di attivazione (comando ACTIVATE)
- utilizzando un file chiave di licenza (comando ADDKEY).

Sintassi del comando:

```
ACTIVATE <activation_code>
ADDKEY <file_name> /password=<your_password>
```

Descrizione dei parametri:

|   |   |
|---|---|
| <b>&lt;file_name&gt;</b>  | Nome del file chiave di licenza con estensione <i>.key</i> .                            |
| <b>&lt;activation_code&gt;</b>  | Codice di attivazione dell'applicazione fornito all'acquisto.                           |
| <b>&lt;password&gt;</b>   | La password di accesso a Kaspersky Anti-Virus assegnata nell'interfaccia del programma. |
| Osservare che non è possibile eseguire questo comando senza digitare la password. |   |

Esempio:

```
avp.com ACTIVATE 11AA1-11AAA-1AA11-1A111
avp.com ADDKEY 1AA111A1.key /password=<your_password>
```

## 18.2. Gestione dei componenti e delle attività del programma

Sintassi del comando:

```
avp.com <command> <profile|task_name>
[/R[A]:<log_file>]
avp.com STOP|PAUSE <profile|task_name>
/password=<your_password> [/R[A]:<report_file>]
```

Parametri:

|   |   |
|---|---|
| <p><b>&lt;command&gt;</b></p>           | <p>Kaspersky Anti-Virus consente la gestione dell'attività del componente dalla riga di comando utilizzando i seguenti comandi:</p> <p><b>START</b> – avvia un componente o un'attività di protezione in tempo reale.</p> <p><b>STOP</b> – arresta un componente o un'attività di protezione in tempo reale.</p> <p><b>PAUSE</b> – sospende un componente o un'attività di protezione in tempo reale.</p> <p><b>RESUME</b> – ripristina un componente o un'attività di protezione in tempo reale.</p> <p><b>STATUS</b> – visualizza lo stato corrente di un componente o un'attività di protezione in tempo reale.</p> <p><b>STATISTICS</b> – visualizza le statistiche di esecuzione di un componente o un'attività di protezione in tempo reale.</p> <p>Si noti che i comandi PAUSE e STOP sono protetti da password.</p> |
| <p><b>&lt;profile task_name&gt;</b></p> | <p>Al parametro <b>&lt;profile&gt;</b> può essere assegnato come valore qualsiasi componente di protezione dell'applicazione in tempo reale o qualsiasi modulo di componente, come anche qualsiasi attività di scansione manuale o di aggiornamento (i valori standard utilizzati dall'applicazione sono mostrati di seguito).</p> <p>I valori validi per il parametro <b>&lt;task_name&gt;</b> possono includere il nome di qualsiasi attività di scansione manuale o di aggiornamento definita dall'utente.</p>   |
| <p><b>&lt;your_password&gt;</b></p>     | <p>Password di Kaspersky Anti-Virus impostata tramite l'interfaccia del programma.</p>  |
| <p><b>/R[A]:&lt;report_file&gt;</b></p> | <p><b>R:&lt;report_file&gt;</b>: registra solo eventi importanti;</p> <p><b>/RA:&lt;report_file&gt;</b>: registra tutti gli eventi.</p> <p>È possibile utilizzare un percorso assoluto o</p>  |

|  |   |
|--|---|
|  | relativo ad un file. Se il parametro non è definito, i risultati di scansione vengono visualizzati sullo schermo, insieme a tutti gli eventi. |
|--|---|

Uno dei seguenti valori è assegnato a **<profile>**:

|            |   |
|------------|---|
| <b>RTP</b> | <p>Tutti i componenti della protezione</p> <p>Il comando <code>avp.com START RTP</code> avvia tutti i componenti di protezione in tempo reale se la protezione è completamente disabilitata (vedere 6.1.2 a pag. 74) o sospesa (vedere 6.1.1 a pag. 73). Questo comando avvia inoltre qualsiasi componente di protezione in tempo reale che sia stato sospeso tramite il pulsante <b>II</b> dall'interfaccia utente o il comando <code>PAUSE</code> dalla riga di comando.</p> <p>Se il componente è stato disabilitato utilizzando il pulsante dall'interfaccia utente o tramite il comando <b>■ STOP</b> da riga di comando, il comando <code>avp.com START RTP</code> non lo riavvia. Per avviarlo, è necessario eseguire il comando <code>avp.com START &lt;profile&gt;</code>, immettendo per <code>&lt;profile&gt;</code> il valore per lo specifico componente di protezione. Ad esempio, <code>avp.com START FM</code>.</p> |
| <b>FM</b>  | File Anti-Virus   |
| <b>EM</b>  | Anti-Virus posta  |
| <b>WM</b>  | <p>Web Anti-Virus</p> <p>Valori per i subcomponenti di Web Anti-Virus:</p> <p><code>httpscan</code> – esamina il traffico http</p> <p><code>sc</code> – esamina gli script</p>  |
| <b>BM</b>  | <p>Difesa proattiva</p> <p>Valori per i subcomponenti di Difesa proattiva:</p> <p><code>og</code> – scansione delle macro di Microsoft Office</p> <p><code>pdm</code> – analisi dell'attività delle applicazioni</p>  |



|  |   |
|--|---|
| <b>ASPY</b>  | Anti-Spy<br>Valori per i subcomponenti di Anti-Spy:<br><b>AdBlocker</b> – AdBlocker<br><b>antidial</b> – Anti-Dialer<br><b>antiphishing</b> – Anti-Phishing<br><b>popupchk</b> – Blocco popup |
| <b>AH</b>  | Anti-Hacker<br>Valori per i subcomponenti di Anti-Hacker:<br><b>fw</b> – Firewall<br><b>ids</b> – Sistema di rilevamento intrusioni   |
| <b>AS</b>  | Anti-Spam   |
| <b>UPDATER</b>   | Aggiornamento   |
| <b>RetranslationCfg</b>  | Distribuzione degli aggiornamenti ad una sorgente locale  |
| <b>Rollback</b>  | Ripristini all'aggiornamento precedente   |
| <b>SCAN_OBJECTS</b>  | Attività di scansione antivirus   |
| <b>SCAN_MY_COMPUTER</b>  | Attività Risorse del computer   |
| <b>SCAN_CRITICAL_AREAS</b>   | Attività aree critiche  |
| <b>SCAN_STARTUP</b>  | Attività oggetti ad esecuzione automatica   |
| <b>SCAN_QUARANTINE</b>   | Esamina gli oggetti in quarantena   |
| I componenti e le attività avviati da riga di comando vengono eseguiti con le impostazioni configurate dall'interfaccia del programma. |   |

**Esempi:**

Per abilitare File Anti-Virus, digitare la seguente stringa nella riga di comando:

```
avp.com START FM
```

Per visualizzare lo status corrente di Difesa proattiva sul computer, digitare il testo seguente nella riga di comando:

```
avp.com STATUS BM
```

Per terminare un'attività di scansione di Risorse del computer da riga di comando, digitare:

```
avp.com STOP SCAN_MY_COMPUTER
/password=<your_password>
```

## 18.3. Scansioni antivirus

La sintassi per avviare una scansione anti-virus di una determinata area ed elaborare gli oggetti nocivi dalla riga di comando generalmente ha questo aspetto:

```
avp.com SCAN [<object scanned>] [<action>] [<file
types>] [<exclusions>] [<configuration file>]
[<report settings>] [<advanced settings>]
```

Per eseguire la scansione di oggetti, è possibile anche avviare una delle attività create in Kaspersky Anti-Virus for Windows Workstations dalla riga di comando (vedere 18.1 a pag. 286). L'attività viene eseguita con le impostazioni specificate nell'interfaccia del programma.

### Descrizione del parametro.

**<object scanned>** - questo parametro fornisce l'elenco di oggetti che saranno sottoposti a scansione per evidenziare eventuali codici nocivi.

Può includere diversi valori dall'elenco seguente, separati da uno spazio.

|                      |   |
|----------------------|---|
| <b>&lt;files&gt;</b> | <p>Lista dei percorsi ai file e/o cartelle da sottoporre a scansione.<br/>È possibile inserire percorsi assoluti o relativi. Gli elementi nell'elenco sono separati da uno spazio.</p> <p>Note:</p> <ul style="list-style-type: none"> <li>• Se il nome dell'oggetto contiene uno spazio, esso deve essere incluso tra virgolette.</li> <li>• Se si seleziona una cartella specifica, saranno sottoposti a scansione antivirus tutti i file in essa contenuti.</li> </ul> |
| <b>/MEMORY</b>       | Oggetti della memoria di sistema.   |

|  |   |
|--|---|
| <b>/STARTUP</b>  | Oggetti di avvio.   |
| <b>/MAIL</b>   | Database di posta.  |
| <b>/REMDRIVES</b>  | Tutte le unità estraibili.  |
| <b>/FIXDRIVES</b>  | Tutte le unità interne.   |
| <b>/NETDRIVES</b>  | Tutte le unità di rete.   |
| <b>/QUARANTINE</b>   | Oggetti in quarantena.  |
| <b>/ALL</b>  | Scansione completa.   |
| <b>/@:&lt;filelist.lst&gt;</b>   | <p>Percorso al file contenente un elenco di oggetti e cartelle da includere nella scansione. Il file deve essere in formato testo e ogni oggetto della scansione deve iniziare una nuova riga.</p> <p>È possibile immettere un percorso assoluto o relativo al file. Il percorso deve essere scritto tra virgolette se contiene uno spazio.</p> |
| <p><b>&lt;action&gt;</b> -questo parametro imposta le reazioni agli oggetti nocivi rilevati durante la scansione. Se questo parametro non viene definito, il valore predefinito è /i8.</p> |   |
| <b>/i0</b>   | nessuna azione sull'oggetto; semplice registrazione delle informazioni nel rapporto.  |
| <b>/i1</b>   | Trattare gli oggetti infetti e, se la riparazione non riesce, ignorare.   |
| <b>/i2</b>   | Trattare gli oggetti infetti e, se la disinfezione non riesce, eliminarli. Eccezioni: non eliminare gli oggetti infetti dagli oggetti compositi; eliminare gli oggetti compositi con intestazioni eseguibili, ad esempio gli archivi .sfx (impostazione predefinita).   |
| <b>/i3</b>   | Trattare gli oggetti infetti e, se la disinfezione non riesce, eliminarli. Inoltre, eliminare completamente tutti gli oggetti compositi se i contenuti infetti non possono essere eliminati.  |

|  |   |
|--|---|
| /i4  | Disinfettare gli oggetti infetti e, se la disinfezione non riesce, eliminarli. Inoltre, eliminare completamente tutti gli oggetti composti se i contenuti infetti non possono essere eliminati. |
| /i8  | Richiedere l'intervento dell'utente se viene rilevato un oggetto infetto.   |
| /i9  | Richiedere l'intervento dell'utente al termine della scansione.   |
| <p>&lt;file types&gt; - questo parametro definisce quali tipi di file saranno sottoposti alla scansione anti-virus. Se questo parametro non viene definito, il valore predefinito è /i8.</p> |   |
| /fe  | Esaminare solo i file potenzialmente infetti in base all'estensione.  |
| /fi  | Esaminare solo i file potenzialmente infetti in base ai contenuti (impostazione predefinita).   |
| /fa  | Esaminare tutti i file.   |
| <p>&lt;exclusions&gt; - questo parametro definisce quali oggetti sono esclusi dalla scansione.</p> <p>Può includere diversi valori dall'elenco fornito, separati da uno spazio.</p>          |   |
| -e:a   | Non esaminare archivi.  |
| -e:b   | Non esaminare database di posta.  |
| -e:m   | Le e-mail con testo semplice non vengono esaminate.   |
| -e:<filemask>  | Non esaminare oggetti in base alle maschere.  |
| -e:<seconds>   | Vengono ignorati gli oggetti la cui scansione richiede un intervallo di tempo superiore a quello specificato nel parametro <seconds>.   |
| -es:<size>   | Ignorare gli oggetti di dimensione (in MB) superiore a quella specificata nel parametro <size>.   |

|   |   |
|---|---|
| <p><b>&lt;configuration file&gt;</b> - definisce il percorso al file di configurazione che contiene le impostazioni di scansione del programma.</p> <p>Il file di configurazione è un file in formato testo contenente l'insieme di parametri da riga di comando per le scansioni antivirus.</p> <p>È possibile immettere un percorso assoluto o relativo al file. Se questo parametro non è definito, vengono utilizzati i valori impostati nell'interfaccia di Kaspersky Anti-Virus for Windows Workstations.</p> |   |
| <code>/C:&lt;file_name&gt;</code>   | Utilizzare i valori di impostazione assegnati nel file di configurazione <code>&lt;file_name&gt;</code> |
| <p><b>&lt;report settings&gt;</b> - questo parametro determina il formato del rapporto sui risultati di scansione.</p> <p>È possibile immettere un percorso assoluto o relativo al file. Se il parametro non è definito, i risultati di scansione sono visualizzati sullo schermo, insieme a tutti gli eventi.</p>  |   |
| <code>/R:&lt;report_file&gt;</code>   | Registrare in questo file solo gli eventi importanti.   |
| <code>/RA:&lt;report_file&gt;</code>  | Registrare tutti gli eventi in questo file.   |
| <p><b>&lt;Advanced settings&gt;</b> - impostazioni che definiscono l'utilizzo delle tecnologie di scansione antivirus.</p>  |   |
| <code>/iChecker=&lt;on off&gt;</code>   | Abilita/disabilita iChecker   |
| <code>/iSwift=&lt;on off&gt;</code>   | Abilita/disabilita iSwift   |

### Esempi:

Avviare una scansione di RAM, programmi di avvio, database di posta elettronica, directory **Documenti e Programmi** e del file **test.exe**:

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and
Settings\All Users\My Documents" "C:\Program Files"
"C:\Downloads\test.exe"
```

Sospensione temporanea della scansione di oggetti selezionati e avvio di una scansione completa del computer, quindi proseguimento della scansione antivirus degli oggetti selezionati:

```
avp.com PAUSE SCAN_OBJECTS /password=<your_password>
avp.com START SCAN_MY_COMPUTER
avp.com RESUME SCAN_OBJECTS
```

Esaminare gli oggetti elencati nel file **object2scan.txt**. Utilizzare il file di configurazione **scan\_setting.txt**. Dopo la scansione, creazione di un rapporto con registrazione di tutti gli eventi:

```
avp.com SCAN /MEMORY /@:objects2scan.txt
/C:scan_Impostazioni.txt /RA:scan.log
```

File di configurazione esemplificativo:

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt
/RA:scan.log
```

## 18.4. Aggiornamenti del programma

La sintassi per l'aggiornamento dei moduli di programma di Kaspersky Anti-Virus for Windows Workstations e degli elenchi delle minacce dalla riga di comando è la seguente:

```
avp.com UPDATE [<path/URL>] [/R[A]:<report_file>]
[/C:<settings_file>] [/APP=<on|off>]
```

Descrizione dei parametri:

|                                  |  |
|----------------------------------|--|
| <b>&lt;update_source&gt;</b>     | Server HTTP o FTP o directory di rete per il download degli aggiornamenti. Il valore per il parametro può essere un percorso completo ad un'origine di aggiornamento o ad un URL. Se non viene selezionato un percorso, l'origine degli aggiornamenti sarà quella delle impostazioni di aggiornamento dell'applicazione.   |
| <b>/R[A]:&lt;report_file&gt;</b> | <p><b>/R:&lt;report_file&gt;</b> - registra solo gli eventi importanti nel rapporto.</p> <p><b>/R[A]:&lt;file_report&gt;</b> - registra tutti gli eventi nel rapporto.</p> <p>È possibile immettere un percorso assoluto o relativo al file. Se il parametro non è definito, i risultati di scansione sono visualizzati sullo schermo, insieme a tutti gli eventi.</p> |

|                                   |   |
|-----------------------------------|---|
| <code>/C:&lt;file_name&gt;</code> | <p>Percorso al file di configurazione con le impostazioni degli aggiornamenti del programma.</p> <p>Il file di configurazione è un file in formato testo contenente l'insieme di parametri da riga di comando per l'aggiornamento del programma.</p> <p>È possibile immettere un percorso assoluto o relativo al file. Se questo parametro non è definito, vengono utilizzati i valori impostati nell'interfaccia di Kaspersky Anti-Virus for Windows Workstations.</p> |
| <code>/APP=&lt;on off&gt;</code>  | <p>Abilita/disabilita gli aggiornamenti ai moduli del programma</p>   |

**Esempi:**

*Aggiornamento dell'elenco dei virus e registrazione di tutti gli eventi nel rapporto:*

```
avp.com UPDATE /RA:avbases_upd.txt
```

*Aggiornamento dei moduli di programma di Kaspersky Anti-Virus for Windows Workstations applicando le impostazioni nel file di configurazione **updateapp.ini**:*

```
avp.com UPDATE /APP=on /C:updateapp.ini
```

**File di configurazione esemplificativo:**

```
"ftp://my_server/kav updates" /RA:avbases_upd.txt
/app=on
```

## 18.5. Impostazioni di rollback

**Sintassi del comando:**

```
ROLLBACK
[/R[A]:<report_file>][/password=<your_password>]
```

|   |  |
|---|--|
| <code>/R[A]:&lt;report_file&gt;</code>                              | <p><code>/R:&lt;report_file&gt;</code> - registra solo gli eventi importanti nel rapporto.</p> <p><code>/R[A]:&lt;file_report&gt;</code> – registra tutti gli eventi nel rapporto.</p> <p>È possibile immettere un percorso assoluto o relativo al file. Se il parametro non è definito, i risultati di scansione sono visualizzati sullo schermo, insieme a tutti gli eventi.</p> |
| <code>&lt;your_password&gt;</code>                                  | La password di accesso a Kaspersky Anti-Virus assegnata nell'interfaccia del programma.  |
| <p>Si noti che questo comando non sarà accettato senza password</p> |  |

Esempio:

```
avp.com ROLLBACK /RA:rollback.txt
/password=<your_password>
```

## 18.6. Esportazione delle impostazioni

Sintassi del comando:

```
avp.com EXPORT <profile> <file_name>
```



Descrizione dei parametri:

|                         |  |
|-------------------------|--|
| <b>&lt;profile&gt;</b>  | Componente o attività le cui impostazioni vengono esportate.<br><br>È possibile utilizzare qualsiasi valore per <b>&lt;profile&gt;</b> , elencato 18.2 a pag. 286.   |
| <b>&lt;filename&gt;</b> | Il file di configurazione può essere salvato come file di testo. A tal fine, specificare l'estensione <i>.txt</i> nel nome del file. Questo file può inoltre essere salvato in qualsiasi formato binario.<br><br>Il file di configurazione viene salvato in formato binario ( <i>.dat</i> , a meno che non venga specificato un altro formato o il formato non sia assegnato, e può essere utilizzato successivamente per importare le impostazioni dell'applicazione su altri computer. Il file di configurazione può essere salvato come file di testo. A tal fine, specificare l'estensione <i>.txt</i> nel nome del file. Si noti che non è possibile importare le impostazioni di protezione da un file di testo. Questo file può essere utilizzato solo per specificare le impostazioni principali per il funzionamento del programma. |

Esempio:

```
avp.com EXPORT c:\settings.dat
```

## 18.7. Importazione delle impostazioni

Sintassi del comando:

```
avp.com IMPORT <filename> [/password=<your_password>]
```

|   |  |
|---|--|
| <b>&lt;filename&gt;</b>   | <p>Il file di configurazione può essere salvato come file di testo. A tal fine, specificare l'estensione <i>.dat</i> nel nome del file.</p> <p>Le impostazioni possono essere importate solo da file binari.</p> <p>Se si installa il programma in modalità nascosta dalla riga di comando o con il l'Editor Oggetti delle Regole di gruppo, il nome del file di configurazione deve essere <i>install.cfg</i>. In caso contrario il programma non lo riconoscerà.</p> |
| <b>&lt;your_password&gt;</b>  | La password di Kaspersky Anti-Virus impostata dall'interfaccia del programma.  |
| <b>Si noti che questo comando non sarà accettato senza password</b> |  |

Esempio:

```
avp.com IMPORT c:\settings.dat /password=<your_password>
```

## 18.8. Avvio del programma

Sintassi del comando:

```
avp.com
```

## 18.9. Arresto del programma

Sintassi del comando:

```
avp.com EXIT /password=<your_password>
```

|   |  |
|---|--|
| <b>&lt;your_password&gt;</b>  | La password di Kaspersky Anti-Virus for Windows Workstations impostata dall'interfaccia del programma. |
| <b>Si noti che questo comando non sarà accettato senza password</b> |  |

Osservare che non è possibile eseguire questo comando senza digitare la password.

## 18.10. Ottenere un file traccia

Potrebbe essere necessario un file traccia nel caso in cui ci siano problemi di runtime dell'applicazione, per consentire agli specialisti dell'assistenza tecnica di ricercare i problemi con maggiore precisione.

### Sintassi del comando:

```
avp.com TRACE [file] [on|off] [<trace_level>]
```

|   |   |
|---|---|
| <b>[on off]</b>   | Abilita/disabilita la creazione della traccia.  |
| <b>[file]</b>   | Ottenere una traccia e salvarla in un file.   |
| <b>&lt;trace_level&gt;</b>  | A questo parametro possono essere assegnati valori numerici compresi tra 0 (valore più basso, solo eventi critici) e 700 (valore più alto, tutti gli eventi).<br><br>Quando viene inviata una richiesta all'assistenza tecnica, un esperto deve definire il livello di traccia richiesto. Se non viene specificato, il livello richiesto è 500. |
| Prudenza! La generazione del file traccia deve essere abilitata solo per risolvere un determinato problema. Tenere sempre attivata la funzione traccia può ridurre le prestazioni del computer e fare sì che il disco rigidi diventi pieno. |   |

### Esempi:

*Disabilitare la traccia:*

```
avp.com TRACE file off
```

*Generare un file traccia per l'assistenza tecnica con un livello di traccia massimo pari a 500:*

```
avp.com TRACE file on 500
```

## 18.11. Visualizzazione della Guida

Questo comando è disponibile per visualizzare la Guida con la sintassi del prompt di comando:

```
avp.com [ /? | HELP ]
```

Per ricevere aiuto sulla sintassi di un comando specifico, è possibile usare uno dei seguenti comandi:

```
avp.com <command> /?  
avp.com HELP <command>
```

## 18.12. Codici restituiti dall'interfaccia a riga di comando

Questa sezione contiene un elenco di codici restituiti dalla riga di comando. I codici generali possono essere restituiti da qualsiasi comando dalla riga di comando. I codici restituiti comprendono i codici generali e quelli specifici per un'attività di tipo specifico.

| <b>Codici restituiti generali:</b>                             |   |
|--|---|
| 0  | Operazione completata con successo                |
| 1  | Valore non valido per l'impostazione              |
| 2  | Errore sconosciuto                                |
| 3  | Errore di completamento dell'attività             |
| 4  | Attività cancellata                               |
| <b>Codici restituiti dall'attività di scansione anti-virus</b> |   |
| 101  | Tutti gli oggetti pericolosi sono stati elaborati |
| 102  | Rilevati oggetti pericolosi                       |

---

# CAPITOLO 19. MODIFICA, RIPARAZIONE E DISINSTALLAZIONE DEL PROGRAMMA

L'applicazione può essere disinstallata in due modi:

- Tramite la procedura guidata d'installazione dell'applicazione (vedere 19.2 a pag. 304)
- Dalla riga di comando (vedere 19.2 a pag. 304)
- Tramite Kaspersky Administration Kit (vedere la Guida di distribuzione di Kaspersky Administration Kit)
- Tramite le regole di dominio di gruppo di Microsoft Windows Server 2000/2003 (vedere 3.4.3 a pag. 50).

## 19.1. Modifica, riparazione e rimozione del programma tramite la procedura guidata d'installazione

In caso di errori di funzionamento dovuto a un'errata configurazione o alla corruzione dei file può rendersi necessario riparare il programma.

La modifica del programma consente di installare componenti di Kaspersky Anti-Virus for Windows Workstations assenti o di eliminare quelli indesiderati.

*Per riparare o modificare i componenti assenti di Kaspersky Anti-Virus for Windows Workstations o disinstallare il programma:*

1. Uscire dal programma. facendo clic con il pulsante sinistro del mouse sull'icona del programma nella barra delle applicazioni e selezionare **Esci** dal menu di scelta rapida.

2. Inserire l'eventuale CD di installazione nell'unità CD-ROM (se utilizzato per installare il programma). Se Kaspersky Anti-Virus for Windows Workstations è stato installato da una diversa origine (cartella ad accesso pubblico, cartella nel disco fisso, ecc.), verificare che la cartella contenga il pacchetto di installazione e di potervi accedere.
3. Selezionare **Start** → **Tutti i programmi** → **Kaspersky Anti-Virus for Windows Workstations 6.0** → **Modifica, ripara o rimuovi**.

Si apre una procedura di installazione guidata del programma. Osserviamo in dettaglio i passaggi necessari per riparare, modificare o eliminare il programma.

## Passaggio 1. Finestra di avvio dell'installazione



Dopo aver eseguito tutti i passaggi sopra descritti, necessari per riparare o modificare il programma, si apre la finestra iniziale di installazione di Kaspersky Anti-Virus for Windows Workstations. Fare clic sul pulsante **Avanti** per continuare.

## Passaggio 2. Selezione di un'operazione

In questa fase viene richiesto di selezionare l'operazione che si desidera eseguire. È possibile modificare i componenti del programma, riparare quelli già installati, rimuoverli o disinstallare completamente il programma. Per eseguire l'operazione desiderata, fare clic sul pulsante appropriato. La reazione del programma dipende dall'operazione selezionata.

La modifica del programma è analoga all'installazione personalizzata (vedere Passaggio 7 a pag. 36), in cui è possibile specificare quali componenti si desidera installare e quali eliminare.

La riparazione del programma dipende dai componenti installati. Saranno riparati i file di tutti i componenti installati e per ciascuno di essi sarà impostato il livello di sicurezza Consigliato.

Se si rimuove il programma, è possibile selezionare quali dati creati e usati dal programma si desidera salvare sul computer. Per eliminare tutti i dati di Kaspersky Anti-Virus for Windows Workstations, selezionare  **Disinstallazione completa**. Per salvare i dati, selezionare  **Salva oggetti applicazione** e specificare quali oggetti non eliminare dall'elenco:

- *Dati di attivazione* – file chiave di licenza necessario per il funzionamento del programma.
- *Database delle minacce* – serie completa delle firme di programmi pericolosi, virus e altre minacce correnti all'ultimo aggiornamento.

- *Database di Anti-Spam* – database utilizzato per individuare la posta indesiderata. Questo database contiene informazioni dettagliate su quali messaggi costituiscono spam e quali no.
- *File di backup* – copie di backup di oggetti eliminati o disinfettati. Si consiglia di salvarli per poterli eventualmente ripristinare in un secondo momento.
- *File in Quarantena* – file potenzialmente infetti da virus o varianti di essi. Questi file contengono codici simili a quelli di virus noti ma è difficile stabilire se siano nocivi. Si consiglia di salvare questi file poiché potrebbero non essere effettivamente infetti, oppure essere riparati dopo l'aggiornamento degli elenchi delle minacce.
- *Impostazioni dell'applicazione* – configurazioni per tutti i componenti del programma.
- *Dati iSwift* – database con informazioni sugli oggetti esaminati nei file system NTFS, che può aumentare la velocità di scansione. Quando usa questo database, Kaspersky Anti-Virus for Windows Workstations esamina solo i file che hanno subito modifiche in seguito all'ultima scansione.

**Attenzione!**

Se trascorre un lungo periodo di tempo tra la disinstallazione di una versione di Kaspersky Anti-Virus for Windows Workstations e l'installazione di un'altra, si sconsiglia di utilizzare il database *iSwift* di un'installazione precedente. Un programma pericoloso potrebbe essere penetrato nel computer nel frattempo e i suoi effetti non sarebbero rilevati dal database, con conseguente rischio di infezione.

Per avviare l'operazione selezionata fare clic sul pulsante **Avanti**. Il programma inizia a copiare i file necessari sul computer o a eliminare i componenti e i dati selezionati.

### Passaggio 3. Completamento della modifica, riparazione o rimozione del programma

L'avanzamento del processo di modifica, riparazione o rimozione del programma viene seguito sullo schermo. Al termine l'utente viene informato del completamento dell'operazione.

La rimozione del programma richiede solitamente il riavvio del computer, necessario per applicare le modifiche al sistema. Il programma chiede quindi se si desidera riavviare il computer. Fare clic su **Sì** per riavviarlo subito. Per riavviarlo in un secondo momento, scegliere invece **No**.

## 19.2. Disinstallazione del programma da riga di comando

*Per disinstallare Kaspersky Anti-Virus 6.0 for Windows Workstations dalla riga di comando, digitare:*

```
msiexec /x <package_name>
```

Si apre la procedura di installazione guidata. Essa consente di disinstallare l'applicazione (vedere la Capitolo 19 a pag. 301).

*Per disinstallare l'applicazione in modalità non interattiva senza riavviare il computer, (il computer deve essere riavviato manualmente dopo la disinstallazione), digitare:*

```
msiexec /x <package_name> /qn
```

*Per disinstallare l'applicazione in modalità non interattiva e dopo riavviare il computer, digitare:*

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

Se durante l'installazione si è scelto di proteggere il programma dalla disinstallazione tramite una password, è necessario inserire tale password di protezione quando si disinstalla il programma. In caso contrario, sarà impossibile disinstallare il programma.

*Per rimuovere l'applicazione inserendo una password come dimostrazione dell'autorizzazione a disinstallare, inserire:*

```
msiexec /x <package_name> KLUNINSTPASSWD=***** – per  
rimuovere l'applicazione in modalità interattiva;
```

```
msiexec /x <package_name> KLUNINSTPASSWD=***** /qn –  
per rimuovere l'applicazione in modalità non interattiva.
```



---

# CAPITOLO 20. GESTIONE DELL'APPLICAZIONE PER MEZZO DI KASPERSKY ADMINISTRATION KIT

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

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

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

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

**Si noti quanto segue per quanto riguarda l'installazione di Kaspersky Anti-Virus tramite Kaspersky Administration Kit:**

Se i computer della rete hanno installato Kaspersky Anti-Virus 5.0, sono necessari i seguenti passaggi prima di eseguire l'upgrade alla versione 6.0 tramite Kaspersky Administration Kit:

- Innanzitutto, arrestare la versione precedente dell'applicazione (questo può essere fatto in remoto tramite Kaspersky Administration Kit);
- Chiudere tutte le altre applicazioni prima di iniziare l'installazione;
- Riavviare il sistema operativo sul computer remoto dopo aver completato l'installazione.

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

La *Console di amministrazione* (vedere Figura 106) consente di amministrare l'applicazione tramite Kaspersky Administration Kit. Si tratta di un'**interfaccia integrata nell'MMC**, che consente all'amministratore di eseguire le seguenti operazioni:

- installare Kaspersky Anti-Virus for Windows Workstations 6.0 e *Administration Agent* sui computer della rete
- configurare in remoto Kaspersky Anti-Virus sui computer della rete
- aggiornare l'elenco delle minacce ed i moduli di Kaspersky Anti-Virus
- gestire le licenze per l'applicazione sui computer della rete
- visualizzare le informazioni sul funzionamento del programma sui computer client

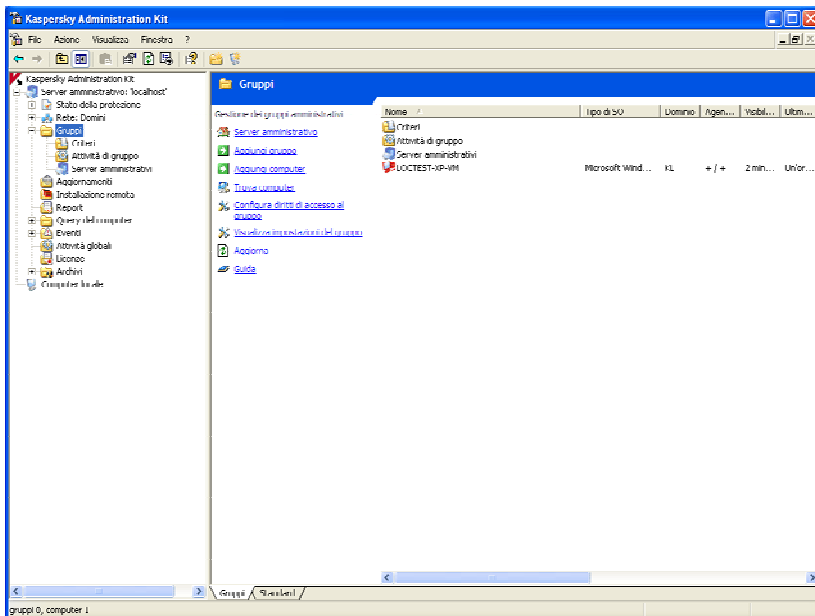


Figura 106. Console di amministrazione di Kaspersky Administration Kit

Quando si amministra il programma centralmente tramite Kaspersky Administration Kit, l'amministratore determina le impostazioni per le regole, le attività e l'applicazione. La protezione è progettata attorno a queste impostazioni.

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

Un'**Attività** è un'azione specifica eseguita dall'applicazione. Le attività di Kaspersky Anti-Virus 6.0 sono suddivise per tipo (attività di installazione della chiave, attività di scansione antivirus, attività di rollback di un aggiornamento precedente, attività di aggiornamento del database antivirus e dei moduli del programma). Ciascuna attività specifica prevede un insieme di impostazioni di Kaspersky Anti-Virus utilizzate in sede di esecuzione (*impostazioni dell'attività*).

La funzione chiave dell'amministrazione centralizzata è il raggruppamento dei computer e la gestione delle loro impostazioni creando e configurando regole di gruppo.

**Regola** si riferisce ad un insieme di impostazioni di funzionamento di Kaspersky Anti-Virus all'interno di un gruppo di rete. Una regola può comprendere restrizioni alla modifica delle configurazioni assegnate durante l'impostazione dell'applicazione o dell'attività.

Una regola consente di gestire la funzionalità completa dell'applicazione, poiché contiene sia le impostazioni dell'applicazione che le impostazioni per tutti i tipi di attività, tranne le impostazioni da configurare direttamente all'avvio di un'attività (ad esempio, la pianificazione delle attività).

## 20.1. Amministrazione dell'applicazione

Kaspersky Administration Kit consente di avviare e sospendere Kaspersky Anti-Virus in remoto sui computer client singoli, come anche di configurare le impostazioni generali dell'applicazione, ad esempio l'abilitazione o disabilitazione della protezione del computer, le impostazioni di backup e quarantena, e le impostazioni per la creazione dei rapporti.

*Per gestire le impostazioni dell'applicazione:*

1. Selezionare la cartella del gruppo che contiene il computer client nella cartella **Gruppi** (vedere Figura 106).
2. Nel riquadro dei risultati, selezionare il computer per il quale si desidera modificare le impostazioni dell'applicazione. Selezionare il comando **Applicazioni** dal menu di scelta rapida o dal menu **Azioni**.
3. La scheda **Applicazioni** sulla finestra delle proprietà del computer client (vedere Figura 107) visualizza un elenco completo delle applicazioni di Kaspersky Lab installate sul computer client. Selezionare **Kaspersky Anti-Virus 6.0 for Windows Workstations**.

I pulsanti sotto l'elenco consentono di:

- Visualizzare un elenco di eventi nel funzionamento dell'applicazione che si sono verificati sul server e sono stati registrati sul server di amministrazione
- Visualizzare informazioni statistiche sul funzionamento dell'applicazione
- Configurare le impostazioni dell'applicazione (vedere 20.1.2 a pag. 310)

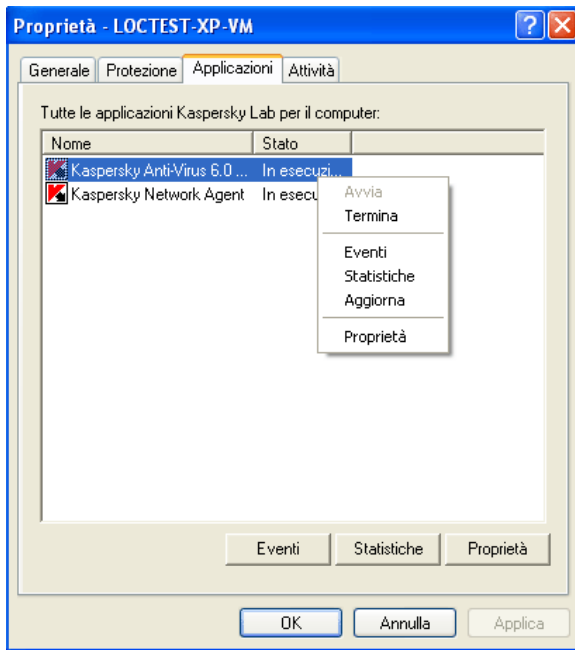


Figura 107. Elenco di applicazioni di Kaspersky Lab

## 20.1.1. Avvio/arresto dell'applicazione

È possibile avviare o sospendere Kaspersky Anti-Virus su un computer remoto tramite i comandi del menù contestuale nella finestra **Proprietà – Nome computer** (vedere Figura 107).

Ciò è possibile anche utilizzando i pulsanti **Avvia/Arresta** della finestra delle impostazioni sulla scheda **Generale** (vedere Figura 109).

La sezione superiore della finestra visualizza il nome dell'applicazione installata, la versione, la data dell'installazione, lo stato (se l'applicazione è in esecuzione oppure no sul computer locale) nonché le informazioni relative alle condizioni del database antivirus.

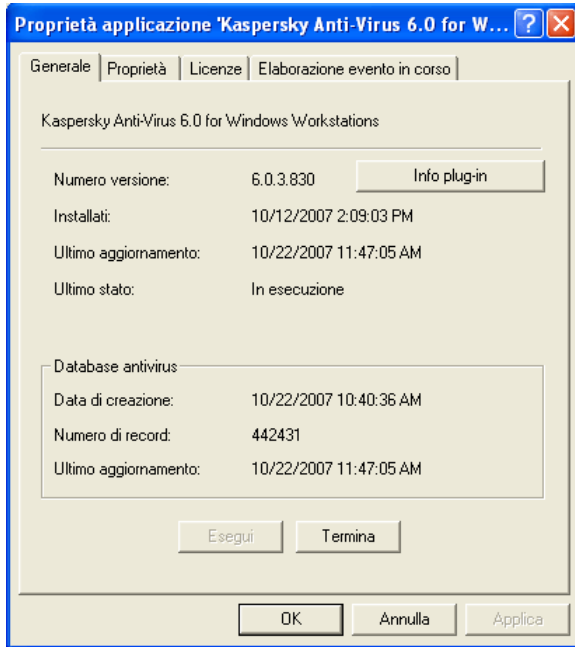


Figura 108. Configurazione delle impostazioni di Kaspersky Anti-Virus. Scheda **Generale**

## 20.1.2. Configurazione delle impostazioni dell'applicazione

*Per visualizzare o modificare le impostazioni dell'applicazione:*

1. Aprire la finestra delle proprietà per il computer client sulla scheda **Applicazione** (vedere Figura 107).
2. Selezionare **Kaspersky Anti-Virus 6.0 for Windows Workstations**. Fare clic sul pulsante **Proprietà** nella finestra delle impostazioni dell'applicazione (vedere Figura 109).

Tutte le schede (ad eccezione di **Proprietà**) sono standard di Kaspersky Administration Kit. Per ulteriori informazioni sulle schede standard, vedere la Guida dell'amministratore.

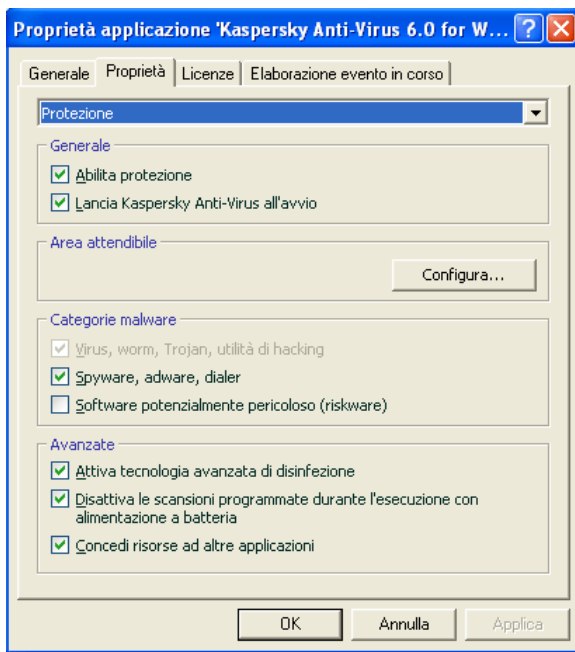


Figura 109. Configurazione delle impostazioni di Kaspersky Anti-Virus. La scheda **Proprietà**

Se è stata creata una regola per l'applicazione (vedere 20.3.1 a pag. 320) che impedisce la riconfigurazione di alcune impostazioni, esse non saranno modificabili quando si configura l'applicazione.

La scheda **Proprietà** consente di configurare le impostazioni generali di protezione, le impostazioni degli strumenti di protezione dell'applicazione e le impostazioni per creare e salvare rapporti statistici per l'applicazione. A tal fine, selezionare il valore desiderato dall'elenco a discesa nella parte superiore della finestra e configurare le impostazioni.

### Protezione

La scheda **Proprietà** nella sezione **Protezione** consente di:

- abilitare/disabilitare la protezione in tempo reale di un computer (vedere 6.1 a pag. 72);
- configurare l'avvio automatico dell'applicazione all'accensione del computer (vedere 6.1.5 a pag. 76);

- creare una zona affidabile o un elenco di esclusioni (vedere 6.3 a pag. 78);
- selezionare i tipi di programmi nocivi che verranno monitorati dall'applicazione (vedere 6.2 a pag. 77);
- configurare le impostazioni di produttività per l'applicazione e quelle per una configurazione multiprocessore (vedere 6.6 a pag. 91).

### Servizio

La scheda **Proprietà** nella sezione **Servizio** consente di:

- Configurare le notifiche per gli eventi che si verificano (vedere 17.11.1.2 a pag. 277)
- Gestire la funzione di autodifesa e le impostazioni di protezione con password dell'applicazione (vedere 17.11.1.3 a pag. 278)
- Configurare l'aspetto dell'applicazione (vedere 20.3.1 a pag. 320)
- Configurare le impostazioni di compatibilità tra Kaspersky Anti-Virus e altri programmi (vedere 17.11.1.3 a pag. 278)

### File di dati

Questa finestra consente di configurare le impostazioni per la generazione del rapporto statistico sul funzionamento dell'applicazione (vedere 17.3.1 a pag. 246) e di specificare per quanto tempo i file vengono conservati nell'area di backup (vedere 17.1.2 a pag. 240) e quarantena (vedere 17.2.2 a pag. 243).

### Impostazioni di rete

Questa finestra consente di modificare l'elenco di porte utilizzate da Kaspersky Anti-Virus per la scansione (vedere 17.7 a pag. 264) e abilitare/disabilitare la scansione SSL (vedere 17.8a pag. 266)

## 20.1.3. Configurazione delle impostazioni specifiche

Durante l'amministrazione di Kaspersky Anti-Virus tramite Kaspersky Administration Kit, è possibile abilitare o disabilitare l'interattività e modificare le informazioni di assistenza tecnica. Per fare ciò:



1. Aprire la finestra delle proprietà per il computer client sulla scheda **Applicazione** (vedere Figura 107). Selezionare **Kaspersky Anti-Virus for Windows Workstations 6.0** e fare clic sul pulsante **Proprietà**. Si aprirà una finestra delle impostazioni dell'applicazione.
2. Passare alla scheda **Impostazioni** (vedere Figura 108). Selezionare **Servizio** dal menù a discesa nella parte superiore della finestra.

La scheda **Servizio** della finestra **Aspetto** consente di abilitare o disabilitare l'interattività di Kaspersky Anti-Virus su un computer remoto: la visualizzazione dell'icona di Kaspersky Anti-Virus nell'area di notifica, l'invio di notifiche sugli eventi che si verificano nell'applicazione (ad esempio il rilevamento di un oggetto pericoloso).

Se è selezionato  **Consenti interattività**, un utente che lavori su un computer remoto potrà vedere l'icona di Anti-Virus ed i messaggi a comparsa, e sarà in grado di prendere decisioni sull'azione successiva nelle finestre di notifica riguardanti gli eventi che si verificano. Per disabilitare l'interattività dell'applicazione, deselegionare la casella di controllo.

La scheda **Informazioni di assistenza personali** nella finestra che si apre facendo clic sul pulsante **Impostazioni** consente di modificare le informazioni di assistenza tecnica utente che vengono visualizzate nella sezione **Servizio** della voce **Assistenza** (vedere Figura 97) di Kaspersky Anti-Virus.

Per modificare le informazioni del caso superiore, immettere il testo corrente nell'assistenza fornita. Nel campo sottostante, è possibile modificare i collegamenti ipertestuali che vengono visualizzati nella casella **Assistenza tecnica on-line**, che appare selezionando **Assistenza** nella sezione **Servizio**.

Per modificare l'elenco di fonti, utilizzare i pulsanti **Aggiungi**, **Modifica** ed **Elimina**. Kaspersky Anti-Virus aggiungerà un nuovo collegamento sulla parte superiore dell'elenco. Per modificare l'ordine dei collegamenti nell'elenco, utilizzare i pulsanti **Su** e **Giù**.

Se la finestra non contiene dati, le informazioni predefinite sull'assistenza tecnica non sono modificabili.

## 20.2. Gestione delle attività

Questa sezione include informazioni sulla gestione delle attività di Kaspersky Anti-Virus for Windows Workstations 6.0. Per ulteriori dettagli sul concetto di gestione delle attività tramite Kaspersky Administration Kit 6.0, si veda la Guida dell'amministratore per il programma.

Un insieme di attività di sistema viene creato per ciascun computer all'installazione dell'applicazione. Questo elenco (vedere Figura 110) comprende le attività di protezione in tempo reale (File Anti-Virus, Web Anti-Virus, Anti-Virus

posta, Difesa Proattiva, Anti-Spy e Anti-Hacker), le attività di scansione antivirus (Risorse del computer, Oggetti di avvio, Aree critiche), nonché le attività di aggiornamento (aggiornamento all'elenco dei virus ed ai moduli dell'applicazione, rollback di un aggiornamento).

È possibile avviare le attività di sistema, configurarne le impostazioni e pianificarle, ma non possono essere eliminate.

Inoltre, è possibile creare le proprie attività, ad esempio scansioni antivirus, aggiornamenti dell'applicazione e rollback dell'aggiornamento precedente, attività di installazione di una chiave di licenza (vedere 20.2.2 a pag. 315).

Per visualizzare un elenco delle attività create per un computer client:

1. Selezionare la cartella del gruppo che contiene il computer client nella cartella **Gruppi** (vedere Figura 106).

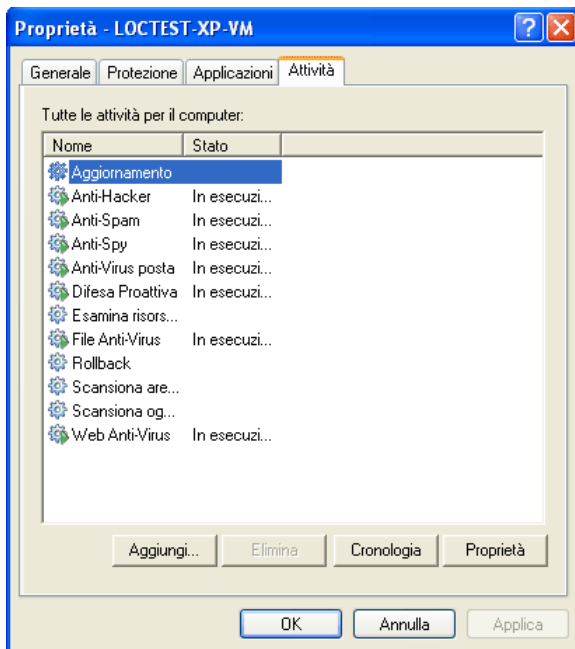


Figura 110. Elenco di attività dell'applicazione

2. Nel riquadro dei risultati, selezionare il computer per il quale si desidera visualizzare un elenco di attività locali. Selezionare il comando **Attività** dal menu di scelta rapida o dal menu **Azioni**. Nella finestra principale si aprirà un'altra finestra che visualizza le proprietà del computer client.

3. La scheda **Attività** (vedere Figura 110) visualizza un elenco completo di attività create per quel computer client.

## 20.2.1. Avvio e arresto delle attività

Le attività possono essere avviate sui computer client solo se la corrispondente applicazione è in esecuzione (vedere 20.1.1 a pag. 309). Se l'applicazione viene arrestata, tutte le attività avviate verranno arrestate.

Le attività vengono avviate e sospese automaticamente, in base ad una pianificazione, oppure manualmente utilizzando i comandi dal menù contestuale e dalla finestra di visualizzazione delle impostazioni dell'attività. È inoltre possibile sospendere un'attività e riavviarla.

*Per avviare/arrestare/sospendere/riprendere manualmente un'attività:*

Selezionare l'attività desiderata (di gruppo o globale) dal riquadro dei risultati, aprire il menu di scelta rapida e selezionare **Avvia/Arresta/Sospendi/Riprendi** nel menu stesso o nel menu **Azione**.

È possibile avviare le stesse operazioni per tutti i tipi di attività dalla finestra delle impostazioni dell'attività della scheda **Generale** (vedere Figura 111) utilizzando gli stessi pulsanti di comando.

## 20.2.2. Creazione delle attività

Quando si lavora con l'applicazione tramite Kaspersky Administration Kit, è possibile creare:

- Attività locali, configurate per i singoli computer
- Attività di gruppo, configurate per i computer uniti in un gruppo di rete
- Attività globali, configurate per qualsiasi insieme di computer da qualsiasi gruppo di rete

È possibile modificare le impostazioni delle attività, controllarne l'esecuzione, copiare e spostare attività da un gruppo all'altro, ed eliminarle tramite i comandi standard del menu di scelta rapida, come **Copia/Incolla**, **Taglia/Incolla** e **Cancella**, o tramite comandi analoghi nel menu **Azione**.

## 20.2.2.1. Creazione delle attività locali

Per creare un'attività locale, procedere come segue:

1. Aprire la finestra delle proprietà del client locale sulla scheda **Attività** (vedere Figura 110).
2. Fare clic su **Aggiungi** per aggiungere una nuova attività locale. Verrà avviata una procedura guidata di creazione dell'attività che consiste in una serie di finestre o passaggi fra i quali navigare servendosi dei pulsanti **Indietro** e **Avanti**. Per completare la procedura guidata fare clic su **Fine**. Per uscire dalla procedura in qualsiasi momento, fare clic su **Annulla**.

### Passaggio 1. Immissione delle informazioni generali sull'attività

La prima finestra principale ha una funzione introduttiva: digitare qui il nome dell'attività (campo **Nome**).

### Passaggio 2. Selezionare l'applicazione ed il tipo di attività

Durante questo passaggio, è necessario specificare l'applicazione per la quale viene creata l'attività (Kaspersky Anti-Virus for Windows Workstations 6.0). È inoltre necessario selezionare il tipo di attività. Le attività possibili per Kaspersky Anti-Virus 6.0 sono:

- *Scansione antivirus* – analizza l'area specificata dall'utente alla ricerca di virus
- *Aggiornamento* – recupera ed applica i pacchetti di aggiornamento per il programma
- *Rollback dell'aggiornamento* – ripristina l'aggiornamento precedente del programma
- *Installazione della chiave di licenza* – aggiunge una nuova chiave di licenza per l'utilizzo dell'applicazione

### Passaggio 3. Configurazione delle impostazioni per il tipo di attività selezionato

In funzione del tipo di attività selezionato durante il passo precedente, i contenuti delle seguenti finestre possono variare:

### SCANSIONE ANTIVIRUS

La finestra di configurazione dell'attività di scansione antivirus richiede di specificare l'azione che dovrà essere eseguita da Kaspersky Anti-Virus alla rilevamento di un oggetto pericoloso (vedere 14.4.4 a pag. 212). Sarà inoltre necessario creare un elenco di oggetti da esaminare (vedere 14.2 a pag. 204).

### AGGIORNAMENTO

Per le attività di aggiornamento dell'elenco delle minacce e dei moduli dell'applicazione, è necessario specificare la sorgente che verrà utilizzata per scaricare gli aggiornamenti (vedere 16.4.1 a pag. 227). L'origine di aggiornamento predefinita è costituita dal server di aggiornamento di Kaspersky Administration Kit.

### ROLLBACK DELL'AGGIORNAMENTO PRECEDENTE

L'attività di rollback degli aggiornamenti più recenti non prevede impostazioni specifiche.

### INSTALLAZIONE DELLA CHIAVE DI LICENZA

Per le attività di installazione delle chiavi di licenza, specificare il percorso al file chiave col pulsante **Sfoggia**. Per utilizzare una chiave aggiunta quale backup, selezionare  **Aggiungi come chiave di backup**. Essa sarà attivata alla scadenza della chiave corrente.

Le informazioni sulla chiave aggiunta (numero di licenza, tipo e data di scadenza) vengono visualizzate nel campo sottostante.

## **Passaggio 4. Selezione di un profilo utente**

In questa fase, viene richiesto di configurare le attività per l'avvio tramite un account utente con privilegi sufficienti a garantire l'accesso all'oggetto che viene esaminato, o all'origine degli aggiornamenti (per ulteriori dettagli, vedere 6.4 a pag. 88).

## **Passaggio 5. Pianificazione degli aggiornamenti**

Dopo avere configurato le impostazioni dell'attività, verrà richiesto di pianificare l'esecuzione automatica dell'attività.

A tal fine, selezionare la frequenza desiderata per l'esecuzione dell'attività dal menù a discesa, è regolare le impostazioni di pianificazione nella parte inferiore della finestra.

## Passaggio 6. Completare la creazione di un'attività

L'ultima finestra di dialogo della procedura guidata comunica all'utente che l'attività è stata creata con successo.

### 20.2.2.2. Creazione delle attività di gruppo

*Per creare un'attività di gruppo, procedere come segue:*

1. Selezionare il gruppo per il quale si desidera creare un'attività dall'albero della console.
2. Selezionare la cartella **Attività** (vedere Figura 106), aprire il menù contestuale e selezionare il comando **Crea**→ **attività**, oppure utilizzare lo stesso comando dal menù **Azione**. Partirà quindi la procedura di creazione guidata dell'attività, simile alla procedura guidata per la creazione delle attività locali (20.2.2.1 316). Seguire le istruzioni.

Una volta terminata la procedura guidata, l'attività verrà aggiunta alla cartella **Attività** di quel gruppo e di tutti i suoi sottogruppi, e visualizzata nel riquadro dei risultati.

### 20.2.2.3. Creazione delle attività globali

*Per creare un'attività globale, procedere come segue:*

1. Selezionare il nodo **Attività globali** dall'albero della console (vedere Figura 106), aprire il menù contestuale e selezionare il comando **Crea**→ **attività**, oppure utilizzare lo stesso comando dal menù **Azione**.
2. Partirà quindi la procedura di creazione guidata dell'attività, simile alla procedura guidata per la creazione delle attività locali (20.2.2.1 316). La differenza è che previsto il passaggio per la creazione di un elenco di computer client della rete per per i quali viene creata l'attività globale.
3. E selezionare dalla rete i computer che eseguiranno l'attività. È possibile selezionare computer da più cartelle o selezionare un'intera cartella (per ulteriori dettagli, consultare la guida dell'amministratore di Kaspersky Administration Kit 6.0).

Le attività globali vengono eseguite esclusivamente sui computer specificati. Se vengono aggiunti nuovi computer ad un gruppo contenente computer per i quali è stata creata un'attività di installazione remota, l'attività non verrà eseguita per essi. A tal fine sarà necessario creare una nuova attività o modificare di conseguenza quella esistente.

Una volta terminata la procedura guidata, una nuova attività globale sarà giunta al nodo **Attività globali** della struttura ad albero della console, e visualizzata nel riquadro dei risultati.

### 20.2.3. Configurazione di impostazioni specifiche dell'attività

*Per visualizzare o modificare le impostazioni dell'attività del computer client:*

1. Aprire la finestra delle proprietà per il computer client sulla scheda **Attività** (vedere Figura 110).
2. Selezionare l'attività desiderata dall'elenco e fare clic sul pulsante **Proprietà**. Si aprirà una finestra di impostazione dell'attività (vedere Figura 111).

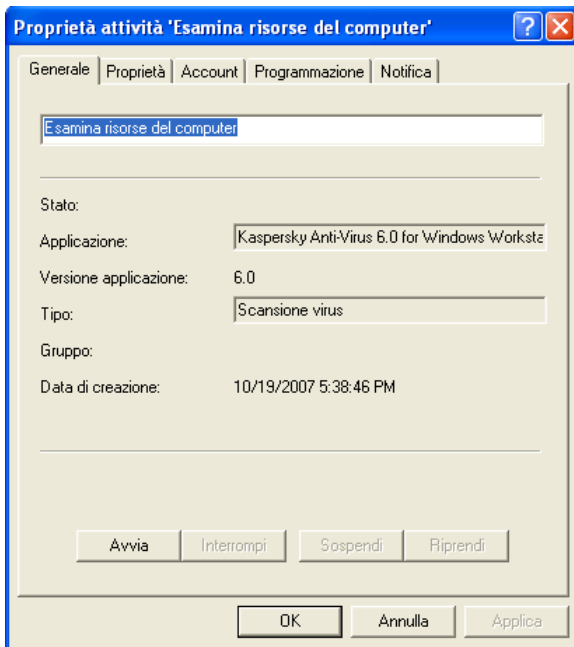


Figura 111. Configurazione delle impostazioni dell'attività

Tutte le schede (ad eccezione di **Impostazioni**) sono quelle standard di Kaspersky Administration Kit 6.0. Vengono trattate con maggiore dettaglio nella guida dell'amministratore. La scheda **Impostazioni** contiene impostazioni

specifiche per Kaspersky Anti-Virus. I contenuti di questa scheda variano in funzione del tipo di attività selezionata.

La configurazione delle impostazioni delle attività di programma tramite l'interfaccia di Kaspersky Administration Kit è analoga alla configurazione attraverso l'interfaccia locale di Kaspersky Anti-Virus, con la differenza che le impostazioni vengono configurate a livello individuale per ciascun utente, come ad esempio le liste bianche e nere di Anti-Spam. Vedere Capitolo 7 – Capitolo 16 a pag. 93 – 222 di questa guida utente per una descrizione più approfondita della configurazione delle impostazioni di un'attività.

Se è stata creata una regola per l'applicazione (vedere 20.3 a pag. 320) che impedisce la riconfigurazione di alcune impostazioni, esse non saranno modificabili quando si configurano le attività.

## 20.3. Gestione delle regole

L'impostazione di regole consente di applicare impostazioni universali per l'applicazione e le attività ai computer client appartenenti ad un singolo gruppo di rete.

Questa sezione include informazioni sulla creazione e gestione di regole per Kaspersky Anti-Virus for Windows Workstations 6.0. Per ulteriori dettagli sul concetto di gestione delle attività tramite Kaspersky Administration Kit 6.0, si veda la Guida dell'amministratore per il programma.


### 20.3.1. Creazione di regole

*Per creare una regola per Kaspersky Anti-Virus, procedere come segue:*

1. Nella cartella **Gruppi** (vedere Figura 106), selezionare il gruppo di computer per il quale si desidera creare una regola.
2. Selezionare la cartella **Regole** appartenente al gruppo selezionato, aprire il menù contestuale ed utilizzare il comando **Crea→ regola**. Verrà visualizzata una finestra Crea nuova regola.

Le regole vengono create tramite una procedura guidata di Windows che consiste in una serie di finestre o passaggi fra i quali navigare servendosi dei pulsanti **Indietro** e **Avanti**. Per completare la procedura guidata fare clic su **Fine**. Per uscire dalla procedura in qualsiasi momento, fare clic su **Annulla**.



Durante ciascuna fase di creazione di una regola, le impostazioni immesse possono essere bloccate con il pulsante . Se il lucchetto sul pulsante è chiuso, i valori assegnati in futuro dalla regola creata verranno utilizzati quando si utilizza la regola sui computer client.

## Passaggio 1. Immissione delle informazioni generali sulla regola

Il primo passaggio della procedura guidata ha una funzione introduttiva: Digitare nella prima finestra della procedura il nome dell'attività (campo **Nome**). Nel secondo, selezionare **Kaspersky Anti-Virus 6.0 for Windows Workstations** dal menu a discesa **Nome applicazione**. Se si desidera che le impostazioni della regola abbiano effetto immediato dopo averla creata, selezionare **Attiva regola**.

## Passaggio 2. Selezione di uno stato per una regola

Questa finestra richiede di specificare lo stato della regola. A tal fine, selezionare l'opzione desiderata: regola attiva o regola inattiva.

È possibile creare diverse regole in un gruppo per un'applicazione, ma solo una di esse può essere la regola corrente (attiva).

## Passaggio 3. Selezione configurazione dei componenti di protezione

Durante questa fase, è possibile abilitare, disabilitare e configurare i componenti di protezione che verranno utilizzati nella regola.

Tutti i componenti della protezione sono abilitati per impostazione predefinita. Per disabilitare un componente, deselegionare la casella di testo accanto al suo nome. Per configurare con maggiore precisione la protezione o File Anti-Virus, selezionarli dall'elenco e fare clic sul pulsante **Impostazioni**.

## Passaggio 4. Configurazione delle impostazioni di scansione antivirus

Durante questa fase, è possibile configurare le impostazioni che verranno utilizzate per le attività di scansione antivirus.

Nella sezione **Livello di sicurezza**, selezionare uno dei livelli di sicurezza preimpostati (vedere 14.4.1 a pag. 207). Per regolare con maggiore precisione il

livello selezionato, fare clic sul pulsante **Impostazioni**. Per ripristinare le impostazioni del livello **Consigliato**, utilizzare il pulsante **Predefinito**.

Nella sezione **Azioni**, specificare l'azione che dev'essere eseguita da Anti-Virus quando viene rilevato un oggetto pericoloso (vedere 14.4.4 a pag. 212).

## Passaggio 5. Configurazione delle impostazioni di aggiornamento

In questa finestra, configurare le impostazioni per la funzione di distribuzione degli aggiornamenti di Kaspersky Anti-Virus.

Nella sezione **Impostazioni di aggiornamento**, specificare cosa aggiornare (vedere 16.4.2 a pag. 229). Nella finestra che si apre facendo clic sul pulsante **Impostazioni**, assegnare le impostazioni locali della rete (vedere 16.4.3 a pag. 231) e specificare l'origine di aggiornamento (vedere 16.4.1 a pag. 226).

Nella sezione **Azioni successive all'aggiornamento**, abilitare o disabilitare la scansione della quarantena dopo aver ricevuto un nuovo pacchetto di aggiornamento (vedere 16.4.4 a pag. 233).


## Passaggio 6. Applicazione della regola

A questo punto, selezionare un metodo per la prima applicazione di una regola sui computer client del gruppo (per maggiori dettagli vedere la guida dell'amministratore di Kaspersky Administration Kit 6.0).

## Passaggio 7. Completare la creazione di una regola

La finestra finale della procedura guidata comunica all'utente che una nuova regola è stata creata con successo.

Al termine della procedura guidata, la regola di che Anti-Virus verrà aggiunta alla cartella **Regole** (vedere Figura 106) del gruppo corrispondente, e sarà visualizzata nel pannello dei risultati.

È possibile modificare le impostazioni della regola creata e stabilire delle restrizioni alla loro modifica utilizzando il pulsante  per ciascun gruppo di impostazioni. Un utente su un computer client non sarà in grado di modificare le impostazioni se vengono bloccate in questo modo. La regola verrà applicata ai computer client al momento della loro prima sincronizzazione con il server.

È possibile copiare e spostare le regole da un gruppo ad un altro oppure cancellarle, utilizzando i comandi standard del menu di scelta rapida, come **Copia/Incolla**, **Taglia/Incolla** e **Cancella**, o i comandi analoghi nel menu Azione.

## 20.3.2. Visualizzazione e modifica delle impostazioni delle regole

In fase di modifica, è possibile modificare la regola e bloccare la modifica delle impostazioni delle regole di gruppo nidificate e di quelle dell'applicazione e delle attività.

*Per visualizzare e modificare le impostazioni delle regole:*

1. Selezionare il gruppo di computer per il quale si desidera modificare le impostazioni dall'albero della console nella cartella **Gruppi**.
2. Selezionare la cartella **Regole** appartenente a quel gruppo (vedere Figura 106). A questo punto, il riquadro dei risultati visualizza tutte le regole create per il gruppo.
3. Selezionare la regola desiderata dall'elenco di regole per **Kaspersky Anti-Virus for Windows Workstations 6.0** (il nome dell'applicazione è specificato nel campo **Applicazione**).
4. Selezionare il comando **Proprietà** dal menu di scelta rapida per la regola selezionata. Si aprirà la finestra di impostazione delle regole per l'applicazione, contenete diverse schede (vedere Figura 112).

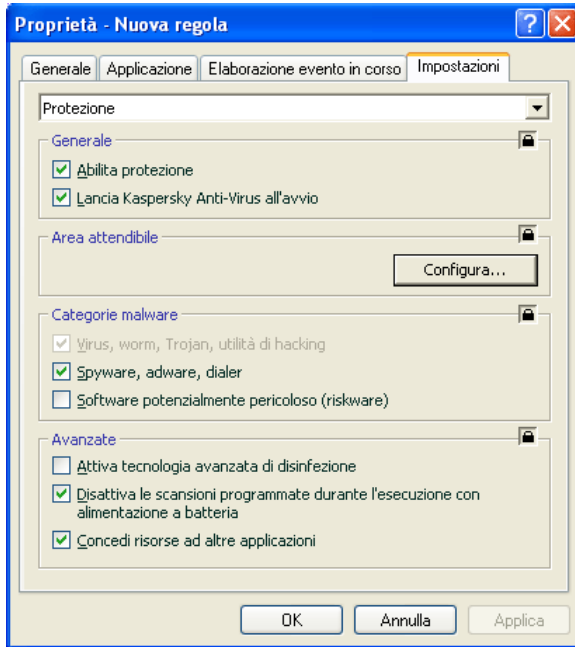


Figura 112. Configurazione delle impostazioni delle regole

Tutte le schede (ad eccezione di **Impostazioni**) sono quelle standard di Kaspersky Administration Kit (per maggiori dettagli, vedere la guida dell'amministratore per il programma).

La scheda **Impostazioni** contiene le impostazioni della regola per Kaspersky Anti-Virus 6.0. Le impostazioni della regola includono le impostazioni del programma (vedere 20.1.2 a pag. 310) e le impostazioni dell'attività (vedere 20.1.3 a pag. 312).

Per configurare le impostazioni, selezionare il valore desiderato dal menu a discesa e procedere.

---

# CAPITOLO 21. DOMANDE FREQUENTI

Il presente capitolo è dedicato alle domande frequenti poste dagli utenti in merito a installazione, configurazione e funzionamento di Kaspersky Anti-Virus for Windows Workstations; seguono risposte dettagliate a tali domande

Domanda: *E' possibile utilizzare Kaspersky Anti-Virus for Windows Workstations 6.0 con prodotti anti-virus di altri fabbricanti?*

No. Si raccomanda di disinstallare altri prodotti antivirus eventualmente presenti sul computer prima di installare Kaspersky Anti-Virus for Windows Workstations per evitare conflitti di software.

Domanda: *Kaspersky Anti-Virus for Windows Workstations non riesamina i file precedentemente sottoposti alla scansione. Perché?*

È vero. Kaspersky Anti-Virus for Windows Workstations non riesamina i file che non sono stati modificati dalla scansione precedente.

Questo è possibile grazie alle nuove tecnologie iChecker e iStream. La tecnologia è implementata nel programma utilizzando un database di checksum dei file e un metodo di archiviazione delle stesse nei flussi NTFS supplementari.

Domanda: *Perché mi occorre una chiave di licenza? Senza la chiave di licenza, Kaspersky Anti-Virus for Windows Workstations funziona?*

Kaspersky Anti-Virus for Windows Workstations non funziona senza una chiave di licenza e non è nemmeno possibile accedere all'Updater e al Supporto Tecnico.

Qualora l'utente non abbia ancora deciso se acquistare Kaspersky Anti-Virus for Windows Workstations, può richiedere una licenza di prova che funziona per due settimane o per un mese. Trascorso questo periodo, la chiave scade.

Domanda: *Dopo l'installazione di Kaspersky Anti-Virus for Windows Workstations il sistema operativo ha iniziato a "comportarsi" in maniera strana (schermo blu, riavvii frequenti, ecc.). Cosa devo fare?*

Sebbene si tratti di una circostanza rara, è possibile che Kaspersky Anti-Virus for Windows Workstations e altri software presenti sul computer siano in conflitto.

Per ripristinare la funzionalità del sistema operativo procedere come segue:

1. Premere ripetutamente il tasto **F8** non appena il computer inizia la fase di caricamento fino alla visualizzazione del menu di avvio.
2. Selezionare la **Modalità provvisoria** e caricare il sistema operativo.
3. Aprire Kaspersky Anti-Virus for Windows Workstations.
4. Utilizzare il collegamento Impostazioni nella finestra principale e selezionare la sezione **Protezione** nella finestra delle impostazioni del programma.
5. Deselezionare **Esegui Kaspersky Anti-Virus 6.0 all'avvio** e fare clic su **OK**.
6. Riavviare il sistema operativo in modalità normale.

Quindi rivolgersi al servizio di assistenza tecnica attraverso il sito web aziendale di Kaspersky Lab (**Services→Technical Support**). Descrivere dettagliatamente il problema e le circostanze in cui esso si è verificato.

Ricordare di allegare alla domanda un file contenente un'immagine completa della memoria del sistema operativo Microsoft Windows. Per creare questo file procedere come segue:


1. Fare clic con il tasto destro del mouse su **Risorse del computer** e selezionare la voce **Proprietà** nel menu di scelta rapida che si apre.
2. Selezionare la scheda **Avanzate** nella finestra **Proprietà di sistema** quindi premere il pulsante **Impostazioni** nella sezione **Avvio e ripristino**.
3. Selezionare l'opzione **Completa dump memoria** dalla lista a discesa nella sezione **Scrivi informazioni di debugging** della finestra **Avvio e ripristino**.
4. Come impostazione predefinita, il file dump sarà salvato nella cartella di sistema come *memory.dmp*. La cartella di memorizzazione del dump può essere modificata editando il nome della cartella nel campo corrispondente.
5. Riprodurre il problema collegato al funzionamento di Kaspersky Anti-Virus for Windows Workstations.
6. Accertarsi che l'immagine completa della memoria sia stata salvata correttamente.

---

# APPENDICE A. INFORMAZIONI DI RIFERIMENTO

Questa appendice contiene materiali di riferimento sui formati dei file e le maschere delle estensioni utilizzati nelle impostazioni di Kaspersky Anti-Virus for Windows Workstations, nonché informazioni sulle impostazioni del file setup.ini, utilizzato per installare l'applicazione in modalità nascosta.

## A.1. Elenco dei file esaminati in base all'estensione

Se si seleziona  **Programmi e documenti (per estensione)** come opzione di scansione per File Antivirus o per le attività di scansione antivirus, i file con le estensioni elencate di seguito verranno analizzati attentamente alla ricerca di virus. Questi tipi di file vengono esaminati anche da Anti-Virus posta, se è attivata la scansione degli allegati ai messaggi:

*com* - file eseguibile per un programma

*exe* - file eseguibile o archivio autoestraente

*sys* - driver di sistema

*prg* - testo programma per un programma dBase, Clipper o Microsoft Visual FoxPro, o WAVmaker

*bin* - file binario

*bat* - file batch

*cmd* - riga di comando per Microsoft Windows NT (simile a un file .bat per DOS), OS/2.

*dpl* - libreria compressa Borland Delphi

*dll* - libreria a caricamento dinamico

*scr* - splash screen di Microsoft Windows

*cpl* - modulo del pannello di controllo di Microsoft Windows

*ocx* - oggetto OLE Microsoft (Object Linking and Embedding)

*tsp* - programma che si esegue in modalità a ripartizione di tempo

*drv* - driver dispositivo

*vxd* - driver dispositivo virtuale Microsoft Windows

*pif* - file di informazione programma

*lnk* - file di collegamento Microsoft Windows

*reg* – file della chiave di registro del sistema di Microsoft Windows  
*ini* - file di inizializzazione  
*cla* - classe Java  
*vbs* - script Visual Basic  
*vbe* - estensione video BIOS  
*js, jse* - testo sorgente JavaScript  
*htm* - documento ipertestuale  
*htt* - intestazione ipertesto Microsoft Windows  
*hta* - programma di ipertesto per Microsoft Internet Explorer  
*asp* - script Active Server Pages  
*chm* - file HTML compilato  
*pht* - HTML con script PHP incorporati  
*php* - script incorporato in file HTML  
*wsh* - file di Windows Script Host  
*wsf* - script Microsoft Windows  
*the* - sfondo desktop Microsoft Windows 95  
*hlp* - file della guida di Windows  
*eml* - file di posta elettronica Microsoft Outlook Express  
*nws* - nuovo file di posta elettronica Microsoft Outlook Express  
*msg* - file di posta elettronica Microsoft Mail  
*plg* - posta elettronica  
*mbx* - estensione per messaggi di posta elettronica salvati in Microsoft Office Outlook  
*doc\** - un documento di Microsoft Word, come: *doc* – un documento di Microsoft Word , *docx* – un documento di Microsoft Word 2007 con supporto XML, *docm* – un documento di Microsoft Word 2007 con supporto alle macro  
*dot\** - un modello di documento Microsoft Word, come *dot* – un modello di documento Microsoft Word, *dotx* – un modello di documento Microsoft Word 2007, *dotm* – un modello di documento Microsoft Word 2007 con supporto alle macro  
*fpm* - programma di database, file di avvio di Microsoft Visual FoxPro  
*rtf* - documento in Rich Text Format  
*shs* - frammento di gestore di eventi oggetti Shell Scrap  
*dwg* - database blueprint AutoCAD  
*msi* - pacchetto di Microsoft Windows Installer  
*otm* - progetto VBA per Microsoft Office Outlook  
*pdf* - documento di Adobe Acrobat



*swf* - file di Shockwave Flash

*jpg, jpeg, png* - formato compresso delle immagini

*emf* - formato Enhanced Metafile, prossima generazione dei metafile del sistema operativo Microsoft Windows. I file EMF non sono supportati da Microsoft Windows a 16 bit.

*ico* - file icona

*ov?* – file eseguibili Microsoft DOC

*xl\** - documenti e file di Microsoft Office Excel, come: *xla* - estensione Microsoft Office Excel, *xlc* - diagramma, *xlt* - modelli di documento. *xlsx* – un documento di lavoro Microsoft Excel 2007, *xltm* – un documento di lavoro Microsoft Excel 2007 con supporto alle macro, *xlsb* – un documento Microsoft Excel 2007 in formato binario (non XML), *xltx* – un modello di documento Microsoft Excel 2007, *xlsm* – un modello di documento Microsoft Excel 2007 con supporto alle macro, *xlam* – un plug-in di Microsoft Excel 2007 con supporto alle macro.

*xl\** - documenti e file di Microsoft Office Excel, come: *xla* - estensione Microsoft Office Excel, *xlc* - diagramma, *xlt* - modelli di documento. *xlsx* – un documento di lavoro Microsoft Excel 2007, *xltm* – un documento di lavoro Microsoft Excel 2007 con supporto alle macro, *xlsb* – un documento Microsoft Excel 2007 in formato binario (non XML), *xltx* – un modello di documento Microsoft Excel 2007, *xlsm* – un modello di documento Microsoft Excel 2007 con supporto alle macro, *xlam* – un plug-in di Microsoft Excel 2007 con supporto alle macro.

*mda\** - Documenti e file di Microsoft Office Access, come: *mda* - Gruppo di lavoro, *mdb* - database, ecc. di Microsoft Office Access

*sldx* – una diapositiva di Microsoft PowerPoint 2007.

*sldm* – una diapositiva di Microsoft PowerPoint 2007 con supporto alle macro.

*thmx* – un tema di Microsoft Office 2007.

Si tenga presente che il formato effettivo di un file può non corrispondere al formato indicato dall'estensione.

## A.2. Maschere di esclusione file possibili

Osserviamo alcuni esempi delle maschere possibili per la creazione di elenchi di esclusione di file:

- Maschere senza percorso file:
  - **\*.exe** - tutti i file con estensione .exe
  - **\*.ex?** - tutti i file con estensione .ex?, dove ? può rappresentare qualsiasi carattere
  - **test-** tutti i file con estensione .test
- Maschere con percorso file assoluto:
  - **C:\dir\\*.\*** o **C:\dir\\*** o **C:\dir\** – tutti i file nella cartella C:\dir\
  - **C:\dir\\*.exe** - tutti i file con estensione exe nella cartella C:\dir\
  - **C:\dir\\*.ex?** – tutti i file con estensione .ex? nella cartella C:\dir\, dove ? può rappresentare qualsiasi carattere
  - **C:\dir\test** – solo il file C:\dir\test
- Se si desidera che il programma non esamini i file nelle sottocartelle di questa cartella, deselezionare **Includi sottocartelle** durante la creazione della maschera.
- Maschere con percorso file relativo:
  - **dir\\*.\*** o **dir\\*** o **dir\** - tutti i file in tutte le cartelle dir\
  - **dir\test** - tutti i file *prova* nelle cartelle dir\
  - **dir\\*.exe** - tutti i file con estensione exe in tutte le cartelle dir\
  - **dir\\*.ex?**– tutti i file con estensione .ex? in tutte le cartelle di C:\dir\, dove ? rappresenta qualsiasi carattere

Se si desidera che il programma non esamini i file nelle sottocartelle di questa cartella, deselezionare **Includi sottocartelle** durante la creazione della maschera.

#### Suggerimento:

Le maschere di esclusione \*.\* e \* possono essere usate esclusivamente se si assegna un'esclusione al verdetto come da Virus Encyclopedia. In caso contrario, la minaccia specificata non sarà rilevata in alcun oggetto. L'uso di queste maschere senza selezionare un verdetto disabilita il monitoraggio.

Si sconsiglia inoltre di selezionare un'unità virtuale creata sulla base di una directory di file system usando il comando *subst* come esclusione. Non avrebbe alcun senso farlo poiché, durante la scansione, il programma percepisce questa unità virtuale come cartella e di conseguenza la esamina.

## A.3. Maschere di esclusione minacce possibili

Durante l'aggiunta di minacce con un determinato verdetto dalla classificazione dell'enciclopedia dei virus come esclusioni, è possibile specificare:

- il nome completo della minaccia come indicata nella Virus Encyclopedia sul collegamento [www.viruslist.com](http://www.viruslist.com) (per esempio, **not-a-virus:RiskWare.RemoteAdmin.RA.311** o **Flooder.Win32.Fuxx**);
- nome della minaccia in base alla maschera. Per esempio:
  - **not-a-virus\*** – esclude dalla scansione potenziali programmi pericolosi e joke.
  - **\*Riskware.\*** - esclude il riskware dalla scansione.
  - **\*RemoteAdmin.\*** - esclude tutti i programmi di amministrazione remota dalla scansione.

## A.4. Panoramica delle impostazioni in *setup.ini*

Il file *setup.ini*, ubicato nella cartella d'installazione di Kaspersky Anti-Virus, viene utilizzato durante l'installazione del programma in modalità non interattiva dalla riga di comando (vedere 3.3 a pag. 48) o tramite l'Editor Oggetti delle Regole di gruppo (vedere 3.4 a pag. 49). Il file contiene le seguenti impostazioni:

**[Setup]** – impostazioni generali per l'installazione del programma.

**InstallDir**=<percorso alla cartella d'installazione del programma>.

**Reboot=yes|no** – stabilisce se riavviare o meno il computer al termine dell'installazione (non viene riavviato per impostazione predefinita).

**SelfProtection=yes|no** – stabilisce se Kaspersky Anti-Virus deve abilitare l'Autodifesa durante l'installazione (abilitata per impostazione predefinita).

**[Components]** – seleziona i componenti da installare. Se non sono specificati componenti, verranno installati tutti. Se vengono specificati componenti, tutti quelli non elencati non verranno installati.

**FileMonitor=yes|no** – installa File Anti-Virus

**MailMonitor=yes|no** – installa Anti-Virus posta

**WebMonitor=yes|no** – installa Web Anti-Virus

**ProactiveDefence=yes|no** – installa Proactive Defense

**AntiSpy=yes|no** – installa Anti-Spy

**AntiHacker=yes|no** – installa Anti-Hacker

**AntiSpam=yes|no** – installa Anti-Spam

**[Tasks]** – abilita le attività di Kaspersky Anti-Virus. Se non vengono specificate attività, dopo l'installazione verranno eseguite tutte. Se vengono specificate attività, tutte quelle non elencate saranno disabilitate.

**ScanMyComputer=yes|no** – attività che prevede la scansione completa del computer

**ScanStartup=yes|no** – attività di scansione degli oggetti di avvio

**ScanCritical=yes|no** – attività di scansione delle aree critiche

**Updater=yes|no** – attività di aggiornamento dell'elenco delle minacce e dei moduli del programma

Anziché il valore **yes**, è possibile utilizzare i valori **1**, **on**, **enable**, o **enabled**, e invece di **no** è possibile utilizzare – **0**, **off**, **disable**, o **disabled** .

---

## APPENDICE B. KASPERSKY LAB

Fondata nel 1997, Kaspersky Lab è ormai un leader indiscusso nel settore delle tecnologie per la sicurezza informatica. Produce un'ampia gamma di software per la sicurezza dei dati e fornisce soluzioni complete e ad elevate prestazioni per proteggere computer e reti da tutti i tipi di programmi nocivi, posta elettronica indesiderata e attacchi degli hacker.

Kaspersky Lab è un'azienda internazionale, con sede nella Federazione Russa e uffici di rappresentanza nel Regno Unito ed in Francia, Germania, Giappone, USA (CA), Benelux, Cina, Polonia e Romania. Recentemente è stato inaugurato un nuovo reparto, l'European Anti-Virus Research Centre, in Francia. Kaspersky Lab conta su una rete di partner costituita da oltre 500 aziende in tutto il mondo.

Oggi Kaspersky Lab si avvale di oltre 450 esperti, tutti specializzati in tecnologie antivirus, 10 dei quali in possesso di laurea in amministrazione aziendale, 16 di specializzazione postlaurea, e due appartenenti alla Computer Anti-Virus Researcher's Organization (CARO).

Kaspersky Lab offre soluzioni di sicurezza di alto livello, elaborate grazie a un'esperienza esclusiva accumulata in più di 14 anni di attività nel settore dei virus informatici. La scrupolosa analisi delle attività dei virus informatici consente all'azienda di offrire una protezione completa contro le minacce presenti e future. La resistenza agli attacchi futuri è la strategia di base implementata in tutti i prodotti Kaspersky Lab. L'azienda si trova costantemente all'avanguardia rispetto a numerosi altri produttori offrendo una protezione antivirus completa per utenti domestici e commerciali.

Anni di duro lavoro hanno fatto dell'azienda uno dei principali produttori di software per la sicurezza informatica. Kaspersky Lab è stata una delle prime aziende di questo tipo a sviluppare i più severi standard per la protezione antivirus. Il prodotto di punta dell'azienda, Kaspersky Anti-Virus, offre una protezione completa a tutti i livelli di una rete, inclusi workstation, file server, sistemi di posta elettronica, firewall, gateway Internet e palmari. I suoi strumenti di gestione, pratici e di facile utilizzo, garantiscono l'automazione avanzata per una sollecita protezione antivirus ad ogni livello dell'azienda. Numerose imprese di grande notorietà utilizzano Kaspersky Anti-Virus, tra cui Nokia ICG (USA), F-Secure (Finlandia), Aladdin (Israele), Sybari (USA), G Data (Germania), Deerfield (USA), Alt-N (USA), Microworld (India), BorderWare (Canada).

Gli utenti Kaspersky Lab possono usufruire di un'ampia gamma di servizi supplementari volti a garantire non solo un funzionamento stabile dei prodotti dell'azienda, ma anche la conformità a qualsiasi esigenza aziendale specifica. Il database antivirus di Kaspersky Lab viene aggiornato ogni ora. L'azienda offre ai propri clienti un servizio di assistenza tecnica 24 ore su 24, disponibile in diverse lingue per soddisfare le esigenze di una clientela internazionale.

## B.1. Altri prodotti Kaspersky Lab

### **Kaspersky Lab News Agent**

News Agent è progettato per comunicare tempestivamente le notizie pubblicate da Kaspersky Lab, per le notifiche relative allo status corrente dell'attività dei virus e per notizie fresche. Il programma legge l'elenco dei canali di news disponibili ed il loro contenuto dai news server di Kaspersky Lab ad intervalli specificati.

News Agent consente agli utenti di:

- Vedere le previsioni correnti in materia di virus nell'aria di notifica
- Iscrivere ai newsfeed ed annullare l'iscrizione
- Recuperare le notizie da ciascun canale selezionato agli intervalli specificati, e notifica la presenza di notizie fresche
- Rivedere le notizie sui canali specificati
- Rivedere l'elenco dei canali ed il loro stato
- Aprire l'intero testo dell'articolo nel browser

News Agent è un'applicazione autonoma di Microsoft Windows, che può essere utilizzata indipendentemente o in congiunzione con diverse soluzioni integrate offerte da Kaspersky Lab Ltd.

### **Kaspersky® OnLine Scanner**

Questo programma è un servizio gratuito offerto ai visitatori del sito web Kaspersky Lab. Esso consente di effettuare un'efficace scansione antivirus online del computer. Kaspersky OnLine Scanner viene eseguito direttamente dal browser. In questo modo, l'utente riceve una risposta rapida alle domande riguardanti potenziali infezioni del computer in uso. Questo servizio consente agli utenti di:

- Escludere gli archivi e i database di posta dalla scansione
- Selezionare il database standard/esteso per la scansione
- Salvare un rapporto sui risultati della scansione in formato .txt o .html

### **Kaspersky® OnLine Scanner Pro**

Questo programma è un servizio a pagamento offerto ai visitatori del sito web Kaspersky Lab. Esso consente di effettuare un'efficace scansione antivirus online del computer e di disinfettare i file pericolosi. Kaspersky OnLine Scanner Pro viene eseguito direttamente dal browser. Questo servizio consente agli utenti di:

- Escludere gli archivi e i database di posta dalla scansione
- Selezionare il database standard/esteso per la scansione
- Salvare un rapporto sui risultati della scansione in formato .txt o .html

### Kaspersky® Anti-Virus® 7.0

Kaspersky Anti-Virus 7.0 è progettato per proteggere i personal computer dal software nocivo grazie a una combinazione ottimale di metodi di protezione antivirus convenzionali e nuove tecnologie proattive.

Il programma offre complesse verifiche antivirus, fra cui:

- Scansione antivirus del traffico e-mail al livello del protocollo di trasmissione dati (POP3, IMAP e NNTP per la posta in arrivo, e SMTP per quella in uscita) indipendentemente dal client di posta usato, nonché riparazione dei database di posta.
- Scansione antivirus in tempo reale del traffico Internet trasferito mediante HTTP.
- Scansione antivirus di singoli file, cartelle o unità. Inoltre è possibile usare un'attività di scansione preimpostata per iniziare l'analisi antivirus esclusivamente delle aree critiche del sistema operativo e degli oggetti ad esecuzione automatica di Microsoft Windows.

La protezione proattiva offre le seguenti funzioni:

- **Controlla le modifiche nel file system.** Il programma consente agli utenti di creare un elenco di applicazioni che controllerà in base ai componenti. Aiuta a proteggere l'integrità delle applicazioni dall'influsso del software nocivo.
- **Monitora i processi nella RAM.** Kaspersky Anti-Virus 7.0 avvisa tempestivamente gli utenti ogni volta che rileva processi pericolosi, sospetti o nascosti, o nei casi in cui si siano verificate variazioni non autorizzate dei processi attivi.
- **Monitora le variazioni del registro del SO** grazie al controllo interno del registro di sistema.
- **Il controllo dei processi nascosti** favorisce la protezione dai codici nocivi nascosti nel sistema operativo tramite le tecnologie rootkit.
- **Analizzatore euristico.** Durante la scansione di un programma, l'analizzatore ne emula l'esecuzione e registra tutta l'attività sospetta, come l'apertura o la scrittura in un file, l'interruzione di intercettazioni vettoriali, ecc. La reazione viene presa in base a tale procedura in relazione a possibili infezioni del programma con un virus. L'emulazione ha luogo in un ambiente virtuale isolato, che protegge con affidabilità il computer dalle infezioni.

- **Ripristina il sistema** dopo attacchi da parte di software nocivi tenendo traccia di tutte le modifiche al registro ed al file system del computer, e le annulla a discrezione dell'utente.

## Kaspersky® Internet Security 7.0

Kaspersky Internet Security 7.0 è una soluzione integrata per la protezione dei personal computer dalle principali minacce alle informazioni (virus, hacker, spam e spyware). Una singola interfaccia consente agli utenti di configurare e gestire tutti i componenti del programma.

Le funzioni di protezione antivirus includono:

- **Scansione antivirus del traffico e-mail** al livello del protocollo di trasmissione dati (POP3, IMAP e NNTP per la posta in arrivo, e SMTP per quella in uscita) indipendentemente dal client di posta usato, nonché riparazione dei database di posta. Il programma include plug-in per i client di posta più utilizzati (come Microsoft Office Outlook, Microsoft Outlook Express (Windows Mail), e TheBat!) e supporta la disinfezione dei loro database di posta.
- **Scansione antivirus in tempo reale del traffico Internet** trasferito mediante HTTP.
- **Protezione del file system:** scansione antivirus di singoli file, cartelle o unità. Inoltre l'applicazione è in grado di eseguire l'analisi antivirus esclusivamente delle aree critiche del sistema operativo e degli oggetti di avvio di Microsoft Windows.
- **Difesa proattiva:** il programma monitora costantemente l'attività delle applicazioni e dei processi in esecuzione nella RAM, impedendo modifiche pericolose al file system ed al registro, e ripristina il sistema dopo gli effetti dei programmi nocivi.

**La protezione dalle frodi via Internet** è garantita grazie al riconoscimento degli attacchi di phishing, il che previene le perdite di dati riservati (innanzitutto, le password ed i numeri di di numero di conto bancario e di carta di credito) e blocca l'esecuzione di script pericolosi su pagine Web, finestre pop-up e banner pubblicitari. La funzione di **blocco autodialer** aiuta a identificare il software che cerca di utilizzare il modem per connessioni nascoste non autorizzate a servizi telefonici a pagamento ed impedisce tali attività. Il modulo *Privacy Control* protegge i dati riservati da accessi e trasmissioni non autorizzate. *Parental Control* è un componente di Kaspersky Internet Security che monitora l'accesso degli utenti a Internet.

Kaspersky Internet Security 7.0 **registra i tentativi di scansione delle porte del computer**, che spesso precedono gli attacchi di rete, e difende con successo dai tipici attacchi di rete. Il programma utilizza **regole definite come base** per il controllo di tutte le transazioni di rete, controllando **tutti i pacchetti di dati in entrata ed in uscita**. La **modalità Stealth** (basata sulla tecnologia



SmartStealth™) **impedisce il rilevamento del computer dall'esterno**. In modalità Stealth , il sistema blocca tutte le attività di rete tranne le poche transazioni autorizzate nelle regole definite dall'utente.

Il programma utilizza un approccio omnicomprensivo al filtraggio spam dei messaggi e-mail in entrata:

- Verifica a fronte di liste nere e bianche di destinatari (tra cui gli indirizzi dei siti di phishing)
- Ispezione delle frasi nel corpo del messaggio
- Analisi del testo del messaggio tramite un algoritmo ad apprendimento automatico
- Riconoscimento della spam inviata in file immagine

### **Kaspersky Anti-Virus Mobile**

Kaspersky® Anti-Virus Mobile garantisce la protezione antivirus ai dispositivi mobili che eseguono Symbian OS e Microsoft Windows Mobile. Il programma offre la scansione antivirus completa, che comprende:

- **Scansioni manuali** della memoria del dispositivo mobile, delle memory card e delle singole cartelle, oppure di file specifici; se viene rilevato un file infetto, esso viene spostato in quarantena o eliminato
- **Scansione in tempo reale** – tutti i file in entrata ed in uscita vengono esaminati automaticamente, come anche tutti i file ai quali si cerca di accedere
- **Protezione dallo spam via SMS**

### **Kaspersky Anti-Virus for File Servers**

Questo pacchetto software offre un'affidabile protezione ai file system dei server che utilizzano Microsoft Windows, Novell NetWare, Linux e Samba da tutti i tipi di software nocivo. La suite include le seguenti applicazioni di Kaspersky Lab:

- [Kaspersky Administration Kit](#).
- [Kaspersky Anti-Virus for Windows Server](#).
- [Kaspersky Anti-Virus for Linux File Server](#).
- [Kaspersky Anti-Virus for Novell Netware](#).
- [Kaspersky Anti-Virus for Samba Server](#).

Caratteristiche e funzionalità:

- *Protegge i file system dei server in tempo reale: Tutti i file del server vengono esaminati all'apertura o al salvataggio sul server*
- *Previene le pandemie di virus;*
- *Scansioni manuali dell'intero file system o di singoli file e singole unità e cartelle;*
- *Uso di tecnologie di ottimizzazione durante la scansione di oggetti nel file system del server;*
- *Ripristino del sistema dopo attacchi da parte di virus;*
- *Scalabilità del pacchetto software nell'ambito delle risorse di sistema disponibili;*
- *Monitoraggio dell'equilibrio del carico sul sistema;*
- *Creazione di un elenco di processi attendibili la cui attività sul server non è soggetta a controllo da parte del pacchetto software;*
- *Amministrazione remota del pacchetto software, compresa l'installazione, la configurazione e l'amministrazione centralizzata;*
- *Salvataggio delle copie di backup degli oggetti infetti ed eliminati per poterli ripristinare;*
- *Messa in quarantena degli oggetti sospetti;*
- *Invio di notifiche sugli eventi che si verificano nel programma all'amministratore;*
- *Registrazione di rapporto dettagliati;*
- *Aggiornamento automatico dei database del programma.*

### **Kaspersky Open Space Security**

Kaspersky Open Space Security è un pacchetto software con un approccio nuovo alla sicurezza per le reti aziendali moderne di qualsiasi dimensione, che offre la protezione centralizzata ai sistemi informati ed il supporto per gli uffici remoti e gli utenti mobili.

La suite comprende quattro programmi:

- Kaspersky Work Space Security
- Kaspersky Business Space Security
- Kaspersky Enterprise Space Security
- Kaspersky Total Space Security

Le specifiche di ciascun programma sono riportate di seguito.

**Kaspersky WorkSpace Security** è un programma destinato alla protezione centralizzata delle workstation all'interno ed all'esterno di reti aziendali da tutte le attuali minacce di Internet (virus, spyware, attacchi di hacker, spam).

Caratteristiche e funzionalità:

- *Protezione completa da virus, spyware, attacchi degli hacker e spam;*
- *Difesa proattiva da nuovi programmi pericolosi le cui firme non sono ancora state aggiunte al database;*
- *Personal Firewall con sistema di rilevamento delle intrusioni e avvisi per gli attacchi degli hacker;*
- *Ripristino del sistema dopo modifiche nocive;*
- *Protezione dagli attacchi di phishing e dalla posta indesiderata;*
- *Distribuzione dinamica delle risorse durante le scansioni complete del sistema;*
- *Amministrazione remota del pacchetto software, compresa l'installazione, la configurazione e l'amministrazione centralizzata;*
- *Supporto per Cisco<sup>®</sup> NAC (Network Admission Control);*
- *Scansione antivirus della posta elettronica e del traffico Internet in tempo reale;*
- *Blocco delle finestre pop-up e dei banner pubblicitari su Internet;*
- *Funzionamento sicuro in qualsiasi tipo di rete, tra cui il Wi-Fi;*
- *Strumenti di creazione dei dischi di ripristino che consentono di ripristinare il sistema dopo una pandemia di virus;*
- *Sistema di reporting completo sullo stato della protezione;*
- *Aggiornamenti automatici al database;*
- *Supporto completo per sistemi operativi a 64 bit;*
- *Ottimizzazione delle prestazioni del programma per PC portatili (tecnologia Intel<sup>®</sup> Centrino<sup>®</sup> Duo);*
- *Capacità di disinfezione remota (Intel<sup>®</sup> Active Management, Intel<sup>®</sup> vPro<sup>™</sup>).*

**Kaspersky Business Space Security** garantisce la protezione ottimale delle risorse informative dell'azienda dalle minacce attuali su Internet. Kaspersky Business Space Security protegge le workstation ed i file server da tutti i tipi di minacce, trojan, e worm, previene le pandemie di virus e protegge le informazioni garantendo nel contempo un accesso istantaneo alle risorse di rete per gli utenti.

Caratteristiche e funzionalità:

- Amministrazione remota del pacchetto software, compresa l'installazione, la configurazione e l'amministrazione centralizzata;
- *Supporto per Cisco<sup>®</sup> NAC (Network Admission Control)*;
- *Protezione delle workstation e dei server da tutti i tipi di minacce su Internet*;
- *Tecnologia iSwift per evitare di ripetere la scansione dei file nella rete*;
- *Distribuzione del carico tra i processori del server*;
- *Messa in quarantena degli oggetti sospetti dalle workstation*;
- *Ripristino del sistema dopo modifiche nocive*;
- *Scalabilità del pacchetto software nell'ambito delle risorse di sistema disponibili*;
- *Difesa proattiva per le workstation da nuovi programmi pericolosi le cui firme non sono ancora state aggiunte al database*;
- *Scansione antivirus della posta elettronica e del traffico Internet in tempo reale*;
- *Personal Firewall con sistema di rilevamento delle intrusioni e avvisi per gli attacchi degli hacker*;
- *Protezione durante l'utilizzo di reti Wi-Fi*;
- *Autodifesa da programmi pericolosi*;
- *Messa in quarantena degli oggetti sospetti*;
- *Aggiornamenti automatici al database*.

### **Kaspersky Enterprise Space Security**

Questo programma include i componenti per la protezione delle workstation e dei server collegati dalle attuali minacce su Internet.

Elimina i virus dalla posta elettronica, proteggendo le informazioni e garantendo un accesso sicuro alle risorse di rete per gli utenti.

Caratteristiche e funzionalità:

- *Protezione delle workstation e dei file server da virus, trojan, e worm;*
- *Protezione dei server di posta Sendmail, Qmail, Postfix e Exim;*
- *Scansione dei messaggi di posta elettronica su Microsoft Exchange Server, comprese le cartelle condivise;*
- *Elaborazione di messaggi di posta elettronica ed altri oggetti per server Lotus Domino;*
- *Protezione dagli attacchi di phishing e dalla posta indesiderata;*
- *Prevenzione degli invii in massa e delle pandemie di virus;*
- Scalabilità del pacchetto software nell'ambito delle risorse di sistema disponibili;
- *Amministrazione remota del pacchetto software, compresa l'installazione, la configurazione e l'amministrazione centralizzata;*
- *Supporto per Cisco® NAC (Network Admission Control);*
- *Difesa proattiva per le workstation da nuovi programmi pericolosi le cui firme non sono ancora state aggiunte al database;*
- *Personal Firewall con sistema di rilevamento delle intrusioni e avvisi per gli attacchi degli hacker;*
- *Funzionamento sicuro durante l'utilizzo di reti Wi-Fi;*
- *Scansione del traffico Internet in tempo reale;*
- *Ripristino del sistema dopo modifiche nocive;*
- *Distribuzione dinamica delle risorse durante le scansioni complete del sistema;*
- *Messa in quarantena degli oggetti sospetti;*
- *Sistema di reporting completo sullo stato della protezione del sistema;*
- *Aggiornamenti automatici al database.*

## Kaspersky Total Space Security

Questa soluzione monitora tutti i flussi di dati in entrata ed uscita (posta elettronica, Internet e tutte le interazioni di rete). Include componenti per la protezione di workstation e dispositivi mobili, protegge le informazioni garantendo nel contempo agli utenti un accesso sicuro alle fonti informative dell'azienda ed a Internet, e garantisce comunicazioni di posta elettronica sicure.

Caratteristiche e funzionalità:

- *Protezione completa da virus, spyware, attacchi degli hacker e spam.* a tutti i livelli della rete aziendale, dalle workstation ai gateway Internet;
- *Difesa proattiva per le workstation da nuovi programmi pericolosi le cui firme non sono ancora state aggiunte al database;*
- *Protezione dei server di posta e dei servizi correlati;*
- *Scansione del traffico Internet (HTTP/FTP) in entrata nella rete locale in tempo reale;*
- *Scalabilità del pacchetto software nell'ambito delle risorse di sistema disponibili;*
- *Blocco dell'accesso delle workstation infette;*
- *Previene le pandemie di virus;*
- *Rapportoing centralizzato sullo stato di protezione;*
- *Amministrazione remota del pacchetto software, compresa l'installazione, la configurazione e l'amministrazione centralizzata;*
- *Supporto per Cisco<sup>®</sup> NAC (Network Admission Control);*
- *Supporto per i server proxy di tipo hardware;*
- *Filtraggio del traffico Internet tramite un elenco di server affidabili, tipi di oggetti e gruppi di utenti;*
- *Tecnologia iSwift per evitare di ripetere la scansione dei file nella rete;*
- *Distribuzione dinamica delle risorse durante le scansioni complete del sistema;*
- *Personal Firewall con sistema di rilevamento delle intrusioni e avvisi per gli attacchi degli hacker;*

- *Funzionamento sicuro per gli utenti in qualsiasi tipo di rete, tra cui il Wi-Fi;*
- *Protezione dagli attacchi di phishing e dalla posta indesiderata;*
- *Capacità di disinfezione remota (Intel® Active Management, Intel® vPro™);*
- *Ripristino del sistema dopo modifiche nocive;*
- *Autodifesa da programmi pericolosi;*
- *Supporto completo per sistemi operativi a 64 bit;*
- *Aggiornamenti automatici al database.*

### **Kaspersky Security for Mail Servers**

Questo programma protegge i server di posta ed i server collegati dai programmi nocivi e dalla posta spam. Il programma comprende le applicazioni in grado di proteggere tutti i server di posta standard (Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix ed Exim) e consente di configurare un gateway di posta elettronica dedicato. La soluzione comprende:

- [Kaspersky Administration Kit](#).
- [Kaspersky Mail Gateway](#).
- [Kaspersky Anti-Virus for Lotus Notes/Domino](#).
- [Kaspersky Anti-Virus for Microsoft Exchange](#).
- [Kaspersky Anti-Virus for Linux Mail Server](#).

Le sue funzioni comprendono:

- *Protezione affidabile dai programmi nocivi o potenzialmente pericolosi;*
- *Filtraggio della posta indesiderata;*
- *La scansione della posta in entrata ed in uscita, nonché degli allegati;*
- *Scansione antivirus dei messaggi di posta elettronica su Microsoft Exchange Server, comprese le cartelle condivise;*
- *Elaborazione di messaggi di posta elettronica, database ed altri oggetti per server Lotus Domino;*
- *Filtraggio della posta elettronica in base agli allegati;*
- *Messa in quarantena degli oggetti sospetti;*
- *Sistema di amministrazione del programma molto semplice;*
- *Previene le pandemie di virus;*

- *Monitoraggio del sistema di protezione* tramite notifiche;
- *Sistema di reporting* per il funzionamento del programma;
- Scalabilità del pacchetto software nell'ambito delle risorse di sistema disponibili;
- *Aggiornamenti automatici al database.*

## **Kaspersky Security for Internet Gateways**

Questo programma garantisce l'accesso sicuro ad Internet per tutti i dipendenti di un'organizzazione, eliminando automaticamente i programmi nocivi e pericolosi dai dati in entrata tramite HTTP/FTP. La soluzione comprende:

- [Kaspersky Administration Kit](#).
- [Kaspersky Anti-Virus for Proxy Server](#).
- [Kaspersky Anti-Virus for Microsoft ISA Server](#).
- [Kaspersky Anti-Virus for Check Point FireWall-1](#).

Le sue funzioni comprendono:

- *Protezione affidabile dai programmi nocivi o potenzialmente pericolosi;*
- *Scansione del traffico Internet (HTTP/FTP) in tempo reale;*
- *Filtraggio del traffico Internet* tramite un elenco di server affidabili, tipi di oggetti e gruppi di utenti;
- *Messa in quarantena* degli oggetti sospetti;
- *Sistema di amministrazione semplice da utilizzare;*
- *Sistema di reporting per il funzionamento del programma;*
- *Supporto per i server proxy di tipo hardware;*
- Scalabilità del pacchetto software nell'ambito delle risorse di sistema disponibili;
- *Aggiornamenti automatici al database.*

## **Kaspersky® Anti-Spam**

Kaspersky® Anti-Spam è un'innovativa suite di software progettata per assistere le aziende con reti di piccole e medie dimensioni nella difesa contro i sempre più numerosi messaggi di posta elettronica non desiderati (spam). Il prodotto combina la rivoluzionaria tecnologia di analisi linguistica con metodi moderni di filtraggio della posta elettronica, tra cui le liste nere DNS e le caratteristiche delle



lettere formali. L'esclusiva combinazione di servizi consente agli utenti di identificare ed eliminare fino al 95% del traffico indesiderato.

Installato all'ingresso di una rete, Kaspersky® Anti-Spam è una barriera alla posta non desiderata controllando tutta la posta in entrata alla ricerca di spam. Il software è compatibile con qualsiasi sistema di posta già in uso presso il cliente, e può essere installato sia su server mail esistenti sia su server dedicati.

L'elevato grado di efficacia di Kaspersky® Anti-Spam è garantito dall'aggiornamento quotidiano del database di filtraggio dei contenuti con i campioni forniti dagli specialisti del laboratorio linguistico dell'azienda. I database vengono aggiornati ogni 20 minuti.

### **Kaspersky Anti-Virus® for MIMESweeper**

Kaspersky Anti-Virus® for MIMESweeper garantisce scansioni antivirus ad alta velocità del traffico su server che eseguono Clearswift MIMESweeper for SMTP / Clearswift MIMESweeper for Exchange / Clearswift MIMESweeper for Web.

Il programma è un plug-in ed esamina in tempo reale i messaggi e-mail in entrata ed in uscita alla ricerca di virus e processi..

## B.2. Recapiti

Per domande, commenti e suggerimenti, rivolgetevi a un nostro distributore o direttamente a Kaspersky Lab. Saremo lieti di aiutarvi per qualsiasi questione legata ai nostri prodotti, per telefono o via posta elettronica. Tutte le raccomandazioni e i suggerimenti pervenuti saranno presi in considerazione e valutati con attenzione.

|                       |  |
|-----------------------|--|
| Assistenza tecnica    | Per qualsiasi informazione relativa al supporto tecnico, visitare la pagina <a href="http://www.kaspersky.com/supportinter.html">http://www.kaspersky.com/supportinter.html</a><br>Helpdesk: <a href="http://support.kaspersky.ru/helpdesk.html?LANG=it">http://support.kaspersky.ru/helpdesk.html?LANG=it</a> |
| Informazioni generali | WWW: <a href="http://www.kaspersky.it">http://www.kaspersky.it</a><br><a href="http://www.viruslist.com">http://www.viruslist.com</a><br>Posta elettronica: <a href="mailto:info@kaspersky.com">info@kaspersky.com</a>   |

---

# APPENDICE C. CONTRATTO DI LICENZA

Contratto di licenza standard per l'utente finale

AVVERTENZA PER TUTTI GLI UTENTI: SI RACCOMANDA DI LEGGERE ATTENTAMENTE IL SEGUENTE CONTRATTO DI LICENZA ("CONTRATTO"), PER LA LICENZA DEL SOFTWARE KASPERSKY ANTI-VIRUS FOR WINDOWS WORKSTATIONS 6.0 ("SOFTWARE") PRODOTTO DA KASPERSKY LAB.

QUANDO ACQUISTA IL PRESENTE SOFTWARE VIA INTERNET, FACENDO CLIC SUL PULSANTE DI ACCETTAZIONE, L'UTENTE ACCONSENTE (IN QUALITÀ DI PRIVATO O PERSONA GIURIDICA) AD ESSERE VINCOLATO DAL PRESENTE CONTRATTO E A DIVENTARNE UNA DELLE PARTI. IN CASO CONTRARIO, FACENDO CLIC SUL PULSANTE CHE INDICA LA MANCATA ACCETTAZIONE DI TUTTE LE CONDIZIONI DEL PRESENTE, L'UTENTE RINUNCIA A INSTALLARE IL SOFTWARE.

SE IL SOFTWARE È STATO ACQUISTATO SU SUPPORTO FISICO E L'UTENTE HA ROTTO IL SIGILLO DELLA BUSTA DEL CD, ACCONSENTE (IN QUALITÀ DI PRIVATO O PERSONA GIURIDICA) AD ESSERE VINCOLATO DAL PRESENTE CONTRATTO. SE L'UTENTE NON ACCETTA TUTTE LE CONDIZIONI DEL PRESENTE CONTRATTO, EGLI DOVRÀ ASTENERSI DAL ROMPERE IL SIGILLO DELLA BUSTA DEL CD, SCARICARE, INSTALLARE O UTILIZZARE QUESTO SOFTWARE.

CONFORMEMENTE ALLA NORMATIVA RELATIVA AL SOFTWARE KASPERSKY PER SINGOLI UTENTI ACQUISTATO SCARICANDO IL FILE DAL SITO WEB DI KASPERSKY LAB O DEI SUOI PARTNER, IL CLIENTE PUÒ RESTITUIRE IL PRODOTTO AL RIVENDITORE PER LA SOSTITUZIONE O IL RIMBORSO COMPLETO ENTRO QUATTORDICI (14) GIORNI LAVORATIVI DALLA DATA DELL'ACQUISTO, A PATTO CHE LA CONFEZIONE NON SIA STATA APERTA.

IL SOFTWARE KASPERSKY PER UTENTI SINGOLI NON ACQUISTATO ONLINE SU INTERNET NON PUÒ ESSERE RESTITUITO PER IL RIMBORSO NÉ PER LA SOSTITUZIONE SE NON DIVERSAMENTE STABILITO DAL PARTNER CHE RIVENDE IL PRODOTTO. IN QUESTO CASO, KASPERSKY LAB NON È VINCOLATO DALLE CLAUSOLE STABILITE DAL PARTNER.

IL DIRITTO ALLA RESTITUZIONE E AL RIMBORSO SPETTA SOLO ALL'ACQUIRENTE ORIGINARIO.

1. *Concessione della licenza.* Previo pagamento delle tasse di licenza applicabili e nel rispetto dei termini e delle condizioni del presente Contratto, con il presente Kaspersky Lab concede all'utente il diritto non esclusivo e non trasferibile di utilizzare una copia della versione specificata del Software e la documentazione in accompagnamento (la "Documentazione") per la durata del presente Contratto e unicamente a uso aziendale interno.

1.1 *Uso.* Il numero di computer dell'utente che può essere protetto dal Software è specificato nel file chiave di licenza ed indicato nella finestra "Servizio". Il software non può essere utilizzato per proteggere reti con un numero di computer superiore a tale numero.

1.1.1 Il Software è "in uso" su un computer quando è caricato nella memoria temporanea (vale a dire nella memoria ad accesso casuale o RAM) o è installato nella memoria permanente (per esempio disco fisso, CD-ROM, o altro dispositivo di memoria) di quel computer. La presente licenza autorizza l'utente a creare il numero di copie di backup del Software necessarie per il suo utilizzo legale e unicamente a scopi di backup, a condizione che tutte le copie contengano le informazioni di proprietà del software. L'utente è tenuto a mantenere traccia del numero e dell'ubicazione di tutte le copie del Software e della Documentazione e a prendere tutte le ragionevoli precauzioni per proteggere il Software da copia o utilizzo non autorizzati.

1.1.2 Il Software protegge i computer dai virus e dagli attacchi di rete la cui firma sia contenuta nei database degli elenchi delle minacce e degli attacchi di rete disponibili presso i server di aggiornamento di Kaspersky Lab.

1.1.3 Qualora l'utente venda il computer su cui è installato il Software, dovrà assicurarsi che tutte le copie del Software siano state cancellate.

1.1.4 All'utente è fatto divieto di decompilare, reingegnerizzare, disassemblare o altrimenti ridurre qualsiasi parte del presente Software a una forma leggibile dall'uomo e di permettere a terzi di compiere tali azioni. Le informazioni di interfaccia necessarie per ottenere l'interoperatività del software con programmi per computer creati indipendentemente sarà fornita da Kaspersky Lab dietro richiesta e dietro pagamento dei ragionevoli costi e delle spese sostenute per procurarsi e fornire tali informazioni. Qualora Kaspersky Lab notificasse al cliente che, per qualsiasi ragione, inclusa senza tuttavia ad essa limitarsi quella dei costi, non intende fornire tali informazioni, l'utente sarà autorizzato a intraprendere le azioni necessarie per ottenere l'interoperatività a condizione di eseguire le operazioni di decompilazione o reverse engineering entro i limiti previsti dalla legge.

1.1.5 L'utente non deve effettuare la correzione di errori o altrimenti modificare, adattare o tradurre il Software, né creare opere da esso derivate derivate, né permettere a terzi di copiarlo (in modo diverso da quanto espressamente permesso nel presente documento).

1.1.6 All'utente è fatto divieto di affittare, noleggiare o prestare il Software a terzi oltre che di trasferire o di fornire a terzi la licenza in concessione.

1.1.7 Kaspersky Lab può richiedere all'utente di installare la versione più recente del Software (la versione più recente nonché il più recente pacchetto di manutenzione).

1.1.8 All'utente è fatto divieto di utilizzare il Software con strumenti automatici, semi-automatici o manuali progettati per creare firme virus, routine di rilevazione virus, qualsiasi altro dato o codice per la rilevazione di codici o dati maligni.

1.1.9 Rimozione dei prodotti potenzialmente pericolosi. L'utente riconosce e concorda che, oltre al rilevamento del software dannoso e nocivo, il Prodotto possa anche identificare, rimuovere e/o disabilitare i prodotti potenzialmente pericolosi, tra cui quelli considerati o classificati come Adware, Riskware, Pornware, ecc.

## 2. Assistenza.

- (i) Kaspersky Lab fornirà all'utente i servizi di assistenza ("Servizi di assistenza") di seguito definiti per il periodo specificato nel File chiave di licenza e indicato nella finestra "Servizio", a partire dalla data di acquisto, dietro:
- (a) pagamento della tariffa di assistenza corrente; e
  - (b) Il Servizio di assistenza tecnica di Kaspersky Lab ha inoltre diritto di richiedere all'utente finale ulteriore identificazione per assegnare l'identificatore che dà diritto ai Servizi di Assistenza.
  - (c) Fino all'attivazione del software e/o all'ottenimento dell'identificatore dell'utente finale (ID cliente) il servizio di assistenza presterà assistenza esclusivamente per l'attivazione del Software e la registrazione dell'utente finale.
- (ii) Con la compilazione del Modulo di sottoscrizione ai servizi di assistenza, l'utente accetta i termini della politica di tutela della riservatezza adottata da Kaspersky Lab, consultabile su [www.kaspersky.com/privacy](http://www.kaspersky.com/privacy), e acconsente esplicitamente al trasferimento dei propri dati in paesi esterni a quello di residenza, come specificato nella politica di tutela della riservatezza.
- (iii) I Servizi di Assistenza termineranno alla scadenza, salvo rinnovo annuo dietro il pagamento della tariffa annuale corrente e dietro soddisfacente nuova compilazione del Modulo di sottoscrizione ai servizi di assistenza .
- (iv) Per "Servizi di assistenza" si intende:
- Aggiornamenti orari del database antivirus

- Aggiornamenti del database contro gli attacchi di rete
  - Aggiornamenti del database anti-spam
    - I. Aggiornamenti gratuiti del software, inclusi gli aggiornamenti della versione
    - II. Assistenza tecnica tramite Internet o linea telefonica dedicata forniti dal distributore e/o dal rivenditore;
    - III. Aggiornamenti per la rilevazione e la disinfezione dei virus 24 ore su 24.
- (v) I servizi di assistenza vengono forniti solo se e quando sul computer dell'utente è installata l'ultima versione del Software come disponibile sul sito Web ufficiale di Kaspersky Lab ([www.kaspersky.com](http://www.kaspersky.com)).

3. *Diritti di proprietà.* Il Software è protetto dalle leggi sul copyright. Kaspersky Lab e i relativi fornitori possiedono e mantengono tutti i diritti, l'autorità e gli interessi del Software e ad esso correlati, inclusi tutti i diritti di proprietà, i brevetti, i marchi commerciali e gli altri diritti di proprietà intellettuale ad esso connessi. Il possesso, l'installazione o l'utilizzo del Software non trasferiscono all'utente alcun diritto relativo alla proprietà intellettuale del Software e non determinano l'acquisizione di diritti sul Software salvo quelli espressamente indicati nel presente Contratto.

4. *Riservatezza.* L'utente riconosce che il Software e la Documentazione, inclusa la specifica configurazione e la struttura dei singoli programmi, costituiscono informazioni proprietarie riservate di Kaspersky Lab. L'utente non dovrà divulgare, fornire o altrimenti rendere disponibili tali informazioni riservate in qualsivoglia forma a terzi senza previo consenso scritto di Kaspersky Lab. Dovrà inoltre applicare ragionevoli misure di sicurezza volte a proteggere tali informazioni riservate ma, senza tuttavia limitarsi a quanto sopra espresso dovrà fare quanto in suo potere per tutelare la sicurezza del codice di attivazione.

#### 5. *Garanzia limitata.*

- (i) Kaspersky Lab garantisce che, per un periodo di sei (6) mesi a decorrere dal primo download o processo d'installazione, il Software acquistato su supporto fisico opererà sostanzialmente in conformità alle funzionalità descritte nella Documentazione, a condizione che sia utilizzato in modo corretto e nella maniera specificata nella Documentazione stessa.
- (ii) L'utente si assume ogni responsabilità in merito alla scelta del presente Software per le proprie esigenze. Kaspersky Lab non garantisce che il Software e/o la Documentazione siano idonei a soddisfare le esigenze dell'utente né che il suo utilizzo sia esente da interruzioni o privo di errori.
- (iii) Kaspersky Lab non garantisce che il Software identifichi tutti i virus ed i messaggi spam noti, né esclude che possa occasionalmente riportare erroneamente un virus in un titolo non infettato da quel virus.

- (iv) Kaspersky Lab non garantisce la protezione fornita dal Software dopo la data di scadenza (vedere la sezione.2 (i))
- (v) L'indennizzo dell'utente e la completa responsabilità di Kaspersky Lab per la violazione della garanzia di cui al paragrafo (i) saranno a discrezione di Kaspersky Lab, che deciderà se riparare, sostituire o rimborsare il Software in caso di reclamo a Kaspersky Lab o suoi fornitori durante il periodo di garanzia. L'utente dovrà fornire tutte le informazioni ragionevolmente necessarie per agevolare il Fornitore nel ripristino dell'articolo difettoso.
- (vi) La garanzia di cui al punto (i) non è applicabile qualora l'utente (a) apporti modifiche al presente Software o determini la necessità di modificarlo senza il consenso di Kaspersky Lab, (b) utilizzi il Software in modo difforme dall'uso previsto o (c) impieghi il Software per usi diversi da quelli permessi ai sensi del presente Contratto.
- (vii) Le garanzie e le condizioni specificate in questo Contratto sostituiscono qualsiasi altra condizione, garanzia o termine relativi alla fornitura o alla presunta fornitura, all'impossibilità di fornire o al ritardo nella fornitura del Software o della Documentazione che, se non fosse per questo paragrafo (vi), potrebbero verificarsi tra Kaspersky Lab e l'utente o sarebbero altrimenti impliciti o incorporati nel presente Contratto o in qualsiasi altro contratto collaterale, per disposizione statutaria, legislazione vigente o altro, che con ciò sarebbero esclusi (inclusi, senza limitazione, le condizioni implicite, le garanzie o altri termini relativi all'adeguatezza della qualità, all'idoneità allo scopo o all'uso di competenza e cura ragionevoli).

#### 6. *Limitazione di responsabilità.*

- (i) Nessun elemento nel presente Contratto deve escludere o limitare la responsabilità di Kaspersky Lab relativamente a (a) responsabilità civile per frode, (b) decesso o lesioni personali causate da un suo mancato esercizio di cautela ai sensi del diritto consuetudinario o dalla violazione negligente di una delle condizioni del presente Contratto, o (c) da qualsiasi altra responsabilità che non possa essere esclusa per legge..
- (ii) Ai sensi del paragrafo (i), Kaspersky Lab non deve essere ritenuto responsabile (relativamente al contratto, per responsabilità civile, restituzione o altro) per i seguenti danni o perdite (siano questi danni o perdite previsti, prevedibili, noti o altro):
  - (a) Perdita di reddito;
  - (b) Perdita di utili effettivi o presunti (inclusa la perdita di utili sui contratti);
  - (c) Perdita di liquidità;
  - (d) Perdita di risparmi presunti;
  - (e) Perdita di attività;

- (f) Perdita di opportunità;
  - (g) Perdita di avviamento;
  - (h) Danni alla reputazione;
  - (i) Perdita, danni o corruzione di dati; o
  - (j) Eventuali perdite indirette o conseguenti o danni arrecati in qualsiasi modo (inclusi, a scanso di dubbi, i danni o le perdite del tipo specificato nei paragrafi (ii), da (a) a (ii), (i).
- (iii) Ai sensi del paragrafo (i), la responsabilità di Kaspersky Lab (né a fini del contratto, frode, restituzione o in nessun'altra maniera) derivante da o in relazione alla fornitura del Software non supererà in nessun caso l'importo corrispondente all'onere ugualmente sostenuto dall'utente per il Software.

7. Il presente Contratto contiene per intero tutti gli intendimenti delle parti relativamente all'oggetto del presente e sostituisce tutti gli eventuali accordi, impegni e promesse precedenti tra l'utente e Kaspersky Lab, sia orali che per iscritto, che possano scaturire o essere impliciti da qualsiasi cosa scritta o pronunciata oralmente in fase di negoziazione tra Kaspersky Lab o suoi rappresentanti e l'utente precedentemente al presente Contratto; tutti gli accordi precedenti tra le parti relativamente all'oggetto di cui sopra decadranno a partire dalla Data di entrata in vigore del presente Contratto.

---

Quando l'utente utilizza la versione di prova del Software, non avrà diritto all'Assistenza tecnica specificata nella Clausola 2 del presente Contratto di licenza, né potrà vendere la copia in suo possesso a terzi.

L'utente avrà diritto ad utilizzare il Software a scopi dimostrativi per il periodo specificato nel file chiave di licenza, a partire dal momento in cui viene attivato (questo periodo può essere visualizzato nella finestra Servizio dell'interfaccia grafica utente del software).