

KASPERSKY LAB

---

Kaspersky<sup>®</sup> Administration Kit  
versione 6.0

Manuale dell'amministratore

KASPERSKY® ADMINISTRATION KIT  
VERSIONE 5.0

---

# Manuale dell'amministratore

© Kaspersky Lab  
Visitate il nostro sito web: <http://www.kaspersky.com/>

Data di revisione: Aprile 2007

# Sommario

CAPITOLO 1. KASPERSKY ADMINISTRATION KIT .....	7
1.1. Kaspersky Administration Kit .....	7
1.2. Le nuove funzioni della versione 5.0 .....	9
1.3. Requisiti hardware e software.....	9
1.4. Help Desk per utenti registrati.....	10
1.5. Convenzioni.....	11
CAPITOLO 2. KASPERSKY ADMINISTRATION KIT IN DETTAGLIO .....	12
2.1. Rete logica .....	12
2.2. Regole, impostazioni e attività .....	14
2.3. Connessione di client al server .....	16
2.4. Connessione sicura al server amministrativo.....	17
2.4.1. Certificato di Administration Server .....	18
2.4.2. Autenticazione del server amministrativo (quando l'Administration Console si connette al server).....	18
2.4.3. Autenticazione del server amministrativo durante la connessione con un client .....	19
2.5. Identificazione dei computer nella rete logica.....	19
2.6. Amministratori e operatori della rete logica .....	20
2.7. Estensione della protezione antivirus alla rete logica.....	22
2.8. Creazione di un sistema di gestione centralizzato .....	22
2.9. Manutenzione di una rete logica .....	23
2.10. Coordinamento degli interventi congiunti degli amministratori .....	24
2.11. Interfaccia utente .....	24
2.11.1. Finestra principale .....	24
2.11.2. Struttura ad albero della console .....	25
2.11.3. Il menu di scelta rapida.....	28
CAPITOLO 3. INSTALLAZIONE DI KASPERSKY ADMINISTRATION KIT .....	34
3.1. Installazione di MSDE per mezzo del pacchetto di installazione di Kaspersky Administration Kit.....	34
3.2. Installazione di Administration Server e di Administration Console.....	36

3.3. Disinstallazione dei componenti di Kaspersky Administration Kit.....	45
3.4. Aggiornamento della versione del programma .....	45
CAPITOLO 4. GUIDA INTRODUTTIVA .....	46
4.1. Avvio del programma e connessione al server amministrativo .....	46
4.2. Avvio rapido guidato .....	50
CAPITOLO 5. VISUALIZZAZIONE, CREAZIONE E CONFIGURAZIONE DI UNA RETE LOGICA .....	51
5.1. Visualizzazione della struttura della rete logica... <b>Error! Bookmark not defined.</b>	
5.2. Ricerca di un computer nella rete logica..... <b>Error! Bookmark not defined.</b>	
5.3. Creazione di una rete logica .....	<b>Error! Bookmark not defined.</b>
5.4. Creazione, modifica ed eliminazione di gruppi di reti logiche <b>Error! Bookmark not defined.</b>	
5.5. Aggiunta, spostamento ed eliminazione di un computer da una rete logica <b>Error! Bookmark not defined.</b>	
5.6. Trasferimento di un client in un'altra rete logica .. <b>Error! Bookmark not defined.</b>	
CAPITOLO 6. GERARCHIA DEI SERVER AMMINISTRATIVI .....	53
6.1. Connessione di un server amministrativo secondario a un server principale <b>Error! Bookmark not defined.</b>	
6.2. Visualizzazione della struttura della rete logica di un server amministrativo secondario..... <b>Error! Bookmark not defined.</b>	
CAPITOLO 7. INSTALLAZIONE E DISINSTALLAZIONE DI APPLICAZIONI SUI CLIENT .....	53
7.1. Installazione (distribuzione) e disinstallazione remota di software .....	54
7.1.1. Creazione dei pacchetti di installazione.....	55
7.1.2. Configurazione delle impostazioni del pacchetto di installazione di Network Agent .....	<b>Error! Bookmark not defined.</b>
7.1.3. Creazione di un'attività di distribuzione delle applicazioni.....	55
7.1.4. Configurazione dell'attività di installazione remota <b>Error! Bookmark not defined.</b>	
7.2. Distribuzione guidata dell'applicazione..... <b>Error! Bookmark not defined.</b>	
7.3. Installazione locale delle applicazioni .....	56
7.3.1. Installazione locale di Network Agent .....	<b>Error! Bookmark not defined.</b>
7.3.2. Installazione locale del plug-in Console di Network Agent <b>Error! Bookmark not defined.</b>	
7.3.3. Installazione delle applicazioni in modalità "silenziosa" <b>Error! Bookmark not defined.</b>	
CAPITOLO 8. GESTIONE REMOTA DELLE APPLICAZIONI KASPERSKY LAB <b>Error! Bookmark not defined.</b>	
8.1. Gestione delle regole.....	58
8.1.1. Creazione di una regola per un'applicazione <b>Error! Bookmark not defined.</b>	
8.1.2. Visualizzazione e modifica di una regola .....	59

8.1.3. Creazione di una regola per Network Agent.	<b>Error! Bookmark not defined.</b>
8.1.4. Distribuzione di regole sui server amministrativi secondari	<b>Error! Bookmark not defined.</b>
8.1.5. Esportazione e importazione di regole.....	<b>Error! Bookmark not defined.</b>
8.2. Gestione delle attività .....	60
8.2.1. Creazione di attività .....	<b>Error! Bookmark not defined.</b>
8.2.1.1. Creazione di attività di gruppo .....	<b>Error! Bookmark not defined.</b>
8.2.1.2. Creazione di attività globali .....	<b>Error! Bookmark not defined.</b>
8.2.1.3. Creazione di attività locali .....	<b>Error! Bookmark not defined.</b>
8.2.2. Visualizzazione e modifica delle impostazioni delle attività	<b>Error! Bookmark not defined.</b>
8.2.3. Attività di avvio/arresto applicazioni .....	<b>Error! Bookmark not defined.</b>
8.2.4. Esportazione e importazione di attività .....	<b>Error! Bookmark not defined.</b>
8.2.5. Avvio e interruzione delle attività .....	<b>Error! Bookmark not defined.</b>
8.2.6. Monitoraggio e visualizzazione dei risultati sulle prestazioni delle attività	<b>Error! Bookmark not defined.</b>
8.2.7. Distribuzione di attività di gruppo sui server amministrativi secondari	<b>Error! Bookmark not defined.</b>
8.3. Gestione delle impostazioni delle applicazioni .....	61
8.3.1. Visualizzazione e modifica delle proprietà del server amministrativo	<b>Error! Bookmark not defined.</b>
8.4. Impostazioni di Network Agent .....	<b>Error! Bookmark not defined.</b>
<b>CAPITOLO 9. AGGIORNAMENTO DEL DATABASE ANTIVIRUS E DEI MODULI DEL PROGRAMMA.....</b>	
	62
9.1. Creazione di un'attività di aggiornamento.....	<b>Error! Bookmark not defined.</b>
9.2. Configurazione dell'attività di aggiornamento .....	<b>Error! Bookmark not defined.</b>
9.3. Visualizzazione dell'elenco degli aggiornamenti .....	<b>Error! Bookmark not defined.</b>
9.4. Distribuzione degli aggiornamenti.....	<b>Error! Bookmark not defined.</b>
<b>CAPITOLO 10. EVENTI, REPORT E NOTIFICHE .....</b>	
	62
10.1. Registrazione e visualizzazione di eventi e ricezione delle notifiche	<b>Error! Bookmark not defined.</b>
10.2. Ricezione dei report.....	<b>Error! Bookmark not defined.</b>
10.2.1. Visualizzazione e modifica dei modelli di report	<b>Error! Bookmark not defined.</b>
10.2.2. Creazione di un modello di report .....	<b>Error! Bookmark not defined.</b>
10.2.3. Generazione e visualizzazione di report.....	<b>Error! Bookmark not defined.</b>
10.2.4. Generazione di report riassuntivi sui server amministrativi secondari	<b>Error! Bookmark not defined.</b>
<b>CAPITOLO 11. GESTIONE DELLE CHIAVI DI LICENZA.....</b>	
	64
11.1. Visualizzazione delle informazioni sulla chiave di licenza	<b>Error! Bookmark not defined.</b>
11.2. Installazione di una nuova chiave di licenza.....	<b>Error! Bookmark not defined.</b>
11.3. Creazione e visualizzazione di report sulla licenza	<b>Error! Bookmark not defined.</b>

---

CAPITOLO 12. COPIE DI BACKUP E RIPRISTINO DEI DATI DAL SERVER AMMINISTRATIVO .....	66
APPENDICE A. DOMANDE FREQUENTI (FAQ).....	67
APPENDICE B. GLOSSARIO .....	71
APPENDICE C. KASPERSKY LAB.....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
C.1. Altri prodotti Kaspersky Lab.....	<b>Error! Bookmark not defined.</b>
C.2. Recapiti .....	<b>Error! Bookmark not defined.</b>
APPENDICE D. CONTRATTO DI LICENZA..	<b>ERROR! BOOKMARK NOT DEFINED.</b>

---

# CAPITOLO 1. KASPERSKY ADMINISTRATION KIT

## 1.1. Kaspersky Administration Kit

Kaspersky® Administration Kit è studiato per centralizzare le prestazioni delle più importanti attività amministrative. Basato sulle applicazioni Kaspersky Anti-Virus Business Optimal e Kaspersky Anti-Virus Corporate Suite, offre il controllo completo della strategia di protezione antivirus dell'azienda. Kaspersky Administration Kit supporta tutte le configurazioni di rete che usano il protocollo TCP/IP.

Kaspersky Administration Kit è uno strumento ideato per gli amministratori delle reti aziendali e il personale responsabile della sicurezza antivirus.

L'applicazione offre le seguenti funzionalità:

- Distribuzione delle applicazioni Kaspersky Lab su computer remoti in ambiente Windows attraverso una connessione di rete. Creazione di un insieme personalizzato di applicazioni Kaspersky Lab su un computer dedicato e installazione istantanea di tali applicazioni multiple su qualsiasi computer collegato in rete.
- Efficiente gestione delle chiavi di licenza. Installazione centralizzata delle chiavi di licenza di tutte le applicazioni Kaspersky Lab, monitoraggio della corrispondenza tra i numeri delle licenze e le applicazioni Kaspersky Lab installate sulla rete, facile individuazione delle date di scadenza delle licenze.
- Gestione remota di applicazioni Kaspersky Lab multiple installate su computer in ambiente Windows da un'unica posizione. Realizzazione di un sistema di protezione antivirus multilivello gestito dalla workstation di un unico amministratore. Si tratta di una funzione particolarmente importante per le imprese dislocate in più sedi. Questa funzione consente di:
  - Creare *gruppi di amministrazione* di computer con funzioni e applicazioni simili;
  - Configurare simultaneamente le impostazioni delle applicazioni applicando *regole di gruppo*;
  - Personalizzare le installazioni in base ai requisiti dei singoli computer applicando le *impostazioni dell'applicazione*;

- Gestire applicazioni multiple assegnando *gruppi e attività globali*;
- Programmare attività per le applicazioni installate sui computer da diversi gruppi di amministrazione.
- Aggiornare automaticamente il database antivirus. Aggiornare dalla postazione centrale il database antivirus di tutte le applicazioni senza necessità di connettere ogni singolo computer ai server di aggiornamento di Kaspersky Lab. Programmare gli aggiornamenti in modo da eseguirli automaticamente a orari specifici e mantenere aggiornata la protezione antivirus, monitorando il processo sui computer client.
- Prelevare report da tutte le installazioni. Le funzionalità di reporting avanzate di Kaspersky Administration Kit consentono di ottenere dati statistici sul funzionamento di tutte le installazioni e di creare report basati sulle statistiche più recenti. Il programma consente di creare un report di rete cumulativo per una sola applicazione Kaspersky Lab (report per applicazione) o un report su tutte le applicazioni Kaspersky Lab installate su un singolo computer (report per computer).
- Ricevere notifiche su eventi specifici per e-mail. Specificare una serie di eventi per i quali si richiede notifica. Tali eventi che si verificano durante il funzionamento dell'applicazione, per esempio, possono essere il rilevamento di un virus, l'impossibilità di aggiornare o la comparsa di un nuovo computer in rete.

Kaspersky Administration Kit consiste di tre componenti principali:

- **Administration Server** è un archivio centralizzato di informazioni sulle applicazioni Kaspersky Lab installate sulla rete aziendale locale e uno strumento per la gestione efficiente delle stesse.
- Network Agent coordina Administration Server e le applicazioni Kaspersky Lab installate su un particolare nodo di rete (workstation o server). Questo componente supporta tutte le applicazioni di Kaspersky Anti-Virus Business Optimal e Kaspersky Anti-Virus Corporate Suite.
- Administration Console, un'interfaccia utente per i servizi di amministrazione Server e Agent, si integra con Microsoft Management Console (MMC).

## 1.2. Le nuove funzioni della versione 6.0

Kaspersky Administration Kit versione 5.0 introduce le seguenti nuove funzioni:

- Gestione di tutte le applicazioni Kaspersky Lab installate su computer basati su Windows.
- Gestione del sistema di protezione antivirus, anche nel caso di reti di grandi dimensioni (fino a decine di migliaia di PC).
- Integrazione dell'interfaccia utente Windows standard con Microsoft Management Console (MMC).
- **Gestione della protezione** antivirus per mezzo di attività specifiche.
- Assegnazione centralizzata di impostazioni generali a più computer dello stesso gruppo di amministrazione.
- Possibilità di creare regole di protezione antivirus assegnando attività di gruppo, applicare tali regole e monitorarne il funzionamento.
- Funzionalità di reporting avanzate.
- Sistema di connessione e reporting potenziato. Visualizzazione dei dati generali dello stato antivirus dell'intera rete o dei report di ogni applicazione gestita, per ogni singolo computer della rete.
- Sistema di gestione centralizzata delle chiavi di licenza. Consente di controllare la corrispondenza tra il numero delle licenze e il numero delle applicazioni Kaspersky Lab correntemente installate, di individuare le date di scadenza delle licenze e di aggiornare le chiavi di licenza con tempestività.

## 1.3. Requisiti hardware e software

Administration Server

- Requisiti software:
  - MSDE 2000 SP 3 or MS SQL Server 2000 SP 3<sup>1</sup>
  - Windows 2000 SP 1 o superiore; Windows XP SP 1 o superiore; Windows 2003 Server; Windows NT4 SP 6.a

---

<sup>1</sup> È possibile installare MSDE dal pacchetto di distribuzione in dotazione con Kaspersky Administration Kit.

- Requisiti hardware:
  - Processore Intel Pentium III, 800 MHz o più
  - 128 MB di RAM
  - 400 MB di spazio disponibile sul disco fisso

### **Administration Console**

- Requisiti software:
  - Windows 2000 SP 1 o superiore; Windows NT4 SP 6a; Windows XP SP 1 o superiore; Windows 2003 Server; Microsoft Management Console versione 1.2 o superiore
- Requisiti hardware:
  - Processore Intel Pentium II, 400 MHz o più
  - Almeno 64 MB di RAM
  - 10 MB di spazio disponibile sul disco fisso.

### **Network Agent**

- Requisiti software:
  - Windows 98; Windows ME; Windows 2000 SP 1 o superiore; Windows NT4 SP 6a; Windows XP SP 1 o superiore, e Windows 2003 Server
- Requisiti hardware:
  - Processore Intel Pentium, 233 MHz o più
  - 32 MB di RAM
  - 10 MB di spazio disponibile sul disco fisso

## 1.4. Help Desk per utenti registrati

Kaspersky Lab offre un ampio pacchetto di assistenza che consente ai propri utenti registrati di utilizzare tutte le funzioni disponibili dei prodotti Kaspersky Anti-Virus.

Registrandosi e acquistando una iscrizione, si ottiene il diritto ai seguenti servizi per tutta la durata dell'abbonamento:

- Nuove versioni del prodotto antivirus, gratuitamente;






- Consulenza telefonica e via e-mail su problematiche relative all'installazione, alla configurazione e alla gestione dell'applicazione antivirus;
- Informazioni sull'uscita di nuove applicazioni Kaspersky Lab e sui nuovi virus informatici (per gli utenti abbonati alla newsletter di Kaspersky Lab).



Kaspersky Lab non fornisce informazioni relative alla gestione e all'uso del sistema operativo e delle tecnologie associate.

## 1.5. Convenzioni

In questo manuale abbiamo adottato una serie di convenzioni volte a porre in evidenza le parti più importanti della documentazione. La tabella sottostante riporta le convenzioni utilizzate.

Convenzione	Significato
<b>Grassetto</b>	Titoli dei menu, comandi, intestazioni delle finestre, elementi delle finestre di dialogo, ecc.
 Nota	Informazioni supplementari, note.
 Attenzione	Informazioni importanti.
 <i>Per eseguire un programma:</i>  1. Passaggio 1. 2. ...  ...	Interventi necessari per eseguire un programma.
 <b>Attività:</b>	Descrizione dell'attività come esempio delle definizioni dei parametri, funzioni, ecc.
 <b>Soluzione</b>	Formulazione di una soluzione.

---

# CAPITOLO 2. KASPERSKY ADMINISTRATION KIT IN DETTAGLIO

## 2.1. Rete logica

Kaspersky Administration Kit offre funzioni di gestione per l'impresa che consentono il controllo di migliaia di computer da un'unica interfaccia amministrativa centralizzata. Questo comporta l'organizzazione dei computer di una rete aziendale in *gruppi di amministrazione* in base alle loro funzioni e alle applicazioni Kaspersky Lab installate. Ciò facilita notevolmente la gestione poiché tutti i computer appartenenti allo stesso gruppo sono trattati come una singola unità. Per esempio, un gruppo consiste solo di workstation, un altro solo di server file, ecc.

Una **rete logica** è una struttura gerarchica di *gruppi di amministrazione* composti da *computer client*. Le applicazioni Kaspersky Lab installate sui computer client vengono gestite per mezzo di Kaspersky Administration Kit.

Un **Administration Server Client** (*computer client*<sup>2</sup>) è un computer, un server o una workstation soggetti alla protezione antivirus. Il Network Agent e le applicazioni Kaspersky Lab gestiti devono essere installati su ciascun computer client.

I **gruppi** sono insiemi logici di client amministrati da un unico server. Tutti i computer appartenenti a un gruppo condividono:

- Le stesse *regole* di protezione antivirus specifiche di ogni applicazione.
- Le stesse attività (funzioni delle applicazioni) e impostazioni di configurazione. Per esempio, può trattarsi di un *pacchetto di installazione* personalizzato, dell'aggiornamento del database antivirus e dei moduli del programma, di scansioni manuali e di protezione in tempo reale.

L'amministratore può creare una gerarchia di gruppi di amministrazione nidificati a qualsiasi livello di specificità al fine di agevolare l'amministrazione delle applicazioni. I gruppi e i computer client possono occupare lo stesso livello gerarchico. Ogni computer client può appartenere a un unico gruppo.

---

<sup>2</sup> Da questo punto in poi, un computer client sarà chiamato client del server amministrativo.

Un **server amministrativo** è un computer della rete aziendale che esegue l'applicazione Administration Server. Sebbene il server amministrativo non sia un oggetto di una rete logica, può essere aggiunto alla rete logica come computer client.

I server amministrativi possono formare gerarchie del tipo "server master – server slave". Il server amministrativo master può avere più server slave (per informazioni più dettagliate sulla gerarchia dei server amministrativi, consultare il 4.4 a pag. 53).

Administration Server (o più precisamente l'applicazione del server amministrativo) consente di:

- Archiviare informazioni sulla struttura della rete logica (configurazione di rete)
- Archiviare backup delle configurazioni dei client
- Archiviare file di distribuzione per le applicazioni Kaspersky Lab
- Installazione a distanza delle applicazioni nei computer client
- Aggiornare database antivirus e moduli del programma
- Gestire regole e attività di gruppo dei computer client
- Archiviare informazioni su eventi verificatisi in computer client
- Generare report sulle prestazioni delle applicazioni nella rete logica
- Distribuire chiavi di licenza tra i computer client
- Inviare avvisi da attività eseguite nei computer client Per esempio, è possibile essere avvertiti della presenza di un virus in un computer client.

**Network Agent** mantiene la comunicazione tra il server amministrativo e i computer client. Fornisce informazioni sullo stato corrente delle applicazioni, invia e riceve comandi, aggiorna le informazioni sulla configurazione e avverte il server al verificarsi di eventi specificati. Per informazioni su come collegare Network Agent al server amministrativo consultare la sezione 2.3 a pag. 16.

I computer aziendali che eseguono la console di amministrazione sono detti **workstation degli amministratori**. Da queste workstation gli amministratori possono gestire remotamente tutti i componenti di Kaspersky Anti-Virus installati nella rete logica.

**Network Agent Console Plug-in**, uno speciale componente che offre l'interfaccia di gestione per ogni applicazione, viene fornito con tutte le applicazioni Kaspersky Lab gestite per mezzo di Kaspersky Administration Kit. Ogni applicazione ha i propri plug-in installati nella workstation degli amministratori. I plug-in presentano:

- Finestre di dialogo per la creazione e la modifica di regole per le applicazioni
- Finestre di dialogo per la creazione e la modifica di impostazioni delle applicazioni
- Finestre di dialogo per la configurazione di impostazioni di attività
- Informazioni sulle attività eseguite da un'applicazione
- Informazioni sugli eventi generati da un'applicazione
- Informazioni sugli eventi e le statistiche per ogni computer client inviate alla console di amministrazione.

Né le workstation degli amministratori né i server amministrativi sono oggetti della rete logica. Essi tuttavia possono essere aggiunti alla rete logica come computer client. Il numero di workstation degli amministratori è potenzialmente illimitato. Le workstation degli amministratori appartenenti a reti logiche diverse possono coincidere. Qualsiasi rete logica può essere amministrata da qualsiasi workstation degli amministratori disponibile nella rete locale.

In una rete logica, lo stesso computer può svolgere la funzione di computer client, server amministrativo e workstation degli amministratori.

## 2.2. Regole, impostazioni e attività

Un'**attività** è un'azione svolta da un'applicazione Kaspersky Lab. Esistono diversi tipi di attività, a seconda delle funzioni. Ogni attività corrisponde a specifiche impostazioni di applicazioni.



Per ulteriori informazioni sui tipi di attività, consultare la documentazione relativa alle applicazioni Kaspersky Lab.

Le **impostazioni delle applicazioni** sono parametri comuni a tutti i tipi di attività. Le **impostazioni delle attività** sono parametri specifici di ciascuno tipo di attività. Le impostazioni delle applicazioni e delle attività differiscono sempre tra loro.

Per far sì che un'applicazione esegua un'azione, è necessario configurare le impostazioni dell'applicazione, creare un'attività corrispondente ed eseguirla.

Per mezzo delle regole è possibile applicare impostazioni personalizzate alle applicazioni di più computer client di una rete logica. Una **regola** è un insieme di parametri delle applicazioni condivisi da tutti i computer di un gruppo. I parametri delle applicazioni differiscono da un gruppo all'altro. Una regola è specifica per ogni applicazione.

La regola di un'applicazione specifica comporta la configurazione di tutte le impostazioni disponibili per la stessa. Così, l'assegnazione di una regola comporta la configurazione sia delle impostazioni dell'applicazione sia delle impostazioni delle attività specifiche per l'applicazione in questione. L'unica eccezione è data dai parametri che devono essere definiti prima dell'avvio di un'attività. Per esempio, assegnare una regola ai computer client per attivare la protezione in tempo reale e la scansione manuale significa configurare le impostazioni di entrambe le attività.

Ogni regola è affiancata da una casella che indica se è possibile ridefinire un parametro modificando le impostazioni delle applicazioni o dell'attività oppure configurando le regole dei gruppi nidificati (al livello gerarchico più basso).

In un gruppo è possibile definire una sola regola per ogni applicazione. In ogni gruppo è possibile creare una regola specifica per un'applicazione. Un gruppo nidificato (secondario) eredita la regola del gruppo principale se non ha una regola definita.

È quindi possibile inserire tutti i computer in gruppo per condividere le stesse impostazioni delle applicazioni per mezzo delle regole. Tuttavia, alcune impostazioni di applicazioni e di attività relative a determinati computer di un gruppo possono essere modificate a meno che non sia stata impostata una regola volta a impedirne la modifica.

Le attività possono essere create centralmente e configurate attraverso la rete logica. L'attività assegnata a un gruppo di amministrazione è un'**attività di gruppo**; l'attività assegnata a un singolo computer client è definita **attività locale**; l'attività assegnata a più computer client appartenenti a gruppi diversi della rete logica è detta **attività globale**.

L'attività di gruppo può essere assegnata a un gruppo anche se l'applicazione è installata solo su alcuni computer client del gruppo. In questo caso, l'attività di gruppo sarà eseguita solo sui computer nei quali è installata l'applicazione.

I gruppi nidificati ereditano le attività dei relativi gruppi principali. Un'attività definita per un gruppo sarà condivisa da tutti i computer client del gruppo ma anche dai computer client appartenenti a tutti i gruppi nidificati ai livelli inferiori.



Le attività assegnate localmente a un computer client determinato saranno eseguite solo su quel computer. Le attività locali saranno aggiunte all'elenco delle attività correnti per tale computer client durante la sua sincronizzazione con il server amministrativo.

Poiché tutte le impostazioni di applicazioni sono gestite per mezzo di regole, è possibile modificare solo le impostazioni definite come modificabili in base alle rispettive regole o impostazioni specifiche di una determinata attività. Per esempio, per la scansione manuale di un'unità, è necessario specificare il nome del disco, le maschere dei file, ecc.

Le informazioni relative alle regole, alle impostazioni di applicazioni, alle attività e alle impostazioni di attività sono archiviate nel server e distribuite ai computer client durante la sincronizzazione. Dai client, il server amministrativo riceve i dati relativi alle modifiche locali non limitate dalla regola, alle applicazioni in esecuzione sui computer client, al loro status e alle attività assegnate.

Quando un'attività viene eseguita su un computer client, le impostazioni dell'applicazione sono determinate da:

- Impostazioni di attività e di applicazioni modificate (se non protette dalle modifiche in base alla regola corrente).
- Regola di gruppo se le impostazioni sono protette dalle modifiche o non sono state modificate.
- Regola principale se la regola di gruppo di un'applicazione non è stata definita.

È possibile programmare le attività in modo da avviarsi subito oppure eseguirle manualmente. I risultati delle prestazioni delle attività vengono salvati nel server amministrativo. L'amministratore può ricevere i risultati delle attività oppure visualizzare i report dettagliati.

## 2.3. Connessione di client al server

Per consentire la comunicazione tra i client e il server amministrativo, i computer client devono essere connessi al server (cfr. la sezione Capitolo 2 a pag. 12). Network Agent installato sui client offre questa funzionalità.

Le seguenti operazioni richiedono la connessione al server.

- Aggiornamento dell'elenco delle applicazioni installate nei computer client
- Sincronizzazione delle regole, impostazioni di applicazioni, attività e impostazioni di attività
- Aggiornamento delle informazioni sulle applicazioni e attività eseguite nei computer client
- Invio di eventi da elaborare sul server

Nella maggior parte dei casi, i computer client sono connessi al server. Tale connessione serve per lo scambio automatico di dati tra i client e il server e per l'invio al server di informazioni sugli eventi relativi alle applicazioni.

La sincronizzazione automatica viene eseguita a intervalli regolari definiti dalle impostazioni di Network Agent (per esempio una volta ogni 15 minuti). La durata dell'intervallo è impostata dall'amministratore.

Le informazioni su un evento vengono inviate al server subito dopo che si è verificato.

Nelle impostazioni del client, è possibile selezionare/deselezionare la casella **Mantieni connessione** (cfr. la sezione 4.3 a pag. **Error! Bookmark not defined.**) per mantenere attiva o interrompere la connessione client-server al termine delle operazioni sopra menzionate. Se la connessione con un client è difficoltosa per qualsiasi motivo (per esempio il client si trova dietro a una firewall, le porte del client non possono essere aperte, l'indirizzo IP del client è sconosciuto, ecc.) o se si ha necessità di monitorare costantemente le prestazioni delle applicazioni Kaspersky Lab è preferibile una connessione permanente.

L'amministratore può indurre forzatamente l'inizio della sincronizzazione facendo clic sul comando **Obbliga sincronizzazione** nel menu di scelta rapida (cfr. la sezione 2.11.3 a pag. 28). In questo caso la connessione viene stabilita dal server. Per abilitare la connessione, viene aperta la porta UDP sul computer client. Il server invia una richiesta di connessione alla porta UDP del client. In risposta, vengono verificati i diritti di connessione del server al client (in base a una firma digitale), e, se la firma risulta valida, viene stabilita la connessione.

È possibile utilizzare anche un secondo tipo di connessione per prelevare dati da computer client, aggiornare gli elenchi di applicazioni e attività eseguite sul client e aggiornare le statistiche relative alle applicazioni.

Tutte le transazioni tra i computer client e il server amministrativo sono garantite dal protocollo SSL (Secure Socket Layer). L'SSL fa uso di certificati elettronici per l'autenticazione del server e del client e consente la crittografia dei dati trasmessi e l'integrità del messaggio.

## 2.4. Connessione sicura al server amministrativo

Lo scambio di dati i computer client e il server amministrativo e le connessioni della console al server amministrativo sono garantiti dal dal protocollo SSL (Secure Socket Layer). Esso è responsabile dell'autenticazione delle parità in comunicazione, della crittografia dei dati trasferiti e della verifica dell'integrità dei dati. L'integrità dei dati garantisce che i dati non siano stati corrotti o alterati

durante il trasferimento. Una connessione dotata di abilitazione SSL comporta l'autenticazione di entrambe le estremità di una sessione di comunicazione in rete e la crittografia dei dati per mezzo del metodo della chiave chiusa.

## 2.4.1. Certificato di Administration Server

Il **certificato di Administration Server** viene utilizzato per autenticare l'Administration Console quando viene connessa al server amministrativo o vengono trasferiti dati dai computer client.

Esso viene creato durante l'installazione di Administration Server. Il certificato viene salvato nel server amministrativo, nella cartella **Cert** della directory di installazione.

Il certificato Administration Server può essere creato una sola volta, durante l'installazione del server. Per ripristinare il certificato, è necessario reinstallare Administration Server e ripristinare i dati perduti dal Backup (per le opzioni di backup, cfr. 4.13 a pag. 66).

## 2.4.2. Autenticazione del server amministrativo (quando l'Administration Console si connette al server)

Quando l'Administration Console si connette al server amministrativo per la prima volta, richiede il certificato al server e lo salva localmente, nella workstation dell'amministratore. In occasione delle successive connessioni della Console al server con questo nome, il server sarà autenticato per mezzo del certificato.

Se il server non supera l'autenticazione (vale a dire, il certificato corrente è diverso da quello archiviato nella workstation dell'amministratore), la Console informa l'utente e richiede al server un nuovo certificato (cfr. la Figura 13). Se la connessione viene confermata e viene ricevuto un altro certificato, l'Administration Console salva il nuovo certificato nel disco fisso per poter essere utilizzato in futuro al fine di autenticare il server.

### 2.4.3. Autenticazione del server amministrativo durante la connessione con un client

Quando un client si connette al server amministrativo per la prima volta, richiede il certificato al server e lo salva localmente.



Se il Network Agent è stato installato localmente su un client, l'amministratore può selezionare manualmente un certificato Administration Server (cfr. la sezione 4.6.2 a pag. 56).

La volta successiva che il client si connette al server amministrativo, il Network Agent richiede il certificato al server amministrativo e lo confronta con il certificato locale. Se i due certificati non corrispondono, l'accesso al server amministrativo è negato.

Se il server amministrativo stabilisce la connessione, Network Agent verifica in maniera analoga la richiesta di connessione abilitata UDP da parte del server.

## 2.5. Identificazione dei computer nella rete logica

I computer client nella rete logica sono identificati in base ai **nomi degli host**. Il nome di uno host deve essere esclusivo tra quelli connessi allo stesso server amministrativo.

Il nome è assegnato dal server amministrativo quando viene rilevato un nuovo computer nella rete Windows o quando Network Agent installato su un client si connette al server per la prima volta dopo l'installazione. Per impostazione predefinita, il nome dello host coincide con il nome del computer nella rete Windows (nome NetBIOS). Se esiste già uno host con quel nome, il server gli assegna un nome con un suffisso numerale, per esempio **Nome-1**, **Nome-2**, ecc. Questo nome di host sarà usato per identificare il computer nella rete logica.

Il server amministrativo si riferisce ai client in base ai rispettivi indirizzi IP. Se in un client è installato Network Agent, il suo indirizzo IP viene determinato automaticamente nel server ad ogni connessione del client. Se Network Agent non è installato o se il cliente non è ancora connesso al server amministrativo (per esempio, se Network Agent è stato installato localmente), il server amministrativo determina l'indirizzo IP del computer in base al nome NetBIOS o DNS.

## 2.6. Amministratori e operatori della rete logica

Solo due gruppi di utenti, gli **amministratori** e gli **operatori della rete logica**, sono in possesso dei diritti necessari ad amministrare le applicazioni attraverso Kaspersky Administration Kit.

L'**amministratore della rete logica** è un utente che installa e configura il pacchetto software Kaspersky Administration Kit nei computer in rete e gestisce le applicazioni Kaspersky Lab nei computer remoti di una rete logica.

L'amministratore della rete logica ha il controllo completo su tutte le funzioni di Kaspersky Administration Kit. Può svolgere le seguenti operazioni:

- Connettersi al server amministrativo
- Creare una rete logica e aggiungere gruppi e computer client dalla rete aziendale locale alla rete logica
- Installare il componente Network Agent nei computer client
- Creare e installare pacchetti di applicazioni Kaspersky Lab nei computer client e gestirne le chiavi di licenza
- Aggiornare le versioni delle applicazioni installate nei computer client
- Creare regole e assegnare attività a gruppi e singoli computer, modificare le impostazioni delle applicazioni
- Gestire centralmente le applicazioni installate nei computer client della rete logica e visualizzare i report utilizzando i servizi forniti dal server amministrativo, da Network Agent e dall'Administration Console

L'**operatore della rete logica** è un utente che monitorizza le prestazioni del sistema di protezione antivirus gestito attraverso Kaspersky Administration Kit.

L'operatore della rete logica dispone di diritti limitati per quanto riguarda le funzionalità di Kaspersky Administration Kit. Può svolgere le seguenti operazioni:

- Connettersi al server amministrativo
- Visualizzare la struttura della rete logica
- Visualizzare le impostazioni delle regole, le attività correnti e le proprietà delle applicazioni
- Eseguire e interrompere gruppi esistenti e attività globali
- Ricevere report e avvisi sugli eventi che si verificano nella rete logica

I diritti degli amministratori della rete logica sono assegnati a:

- Amministratori di dominio i cui computer sono incorporati nella rete logica
- Amministratori locali di computer che eseguono l'applicazione Administration Server
- Utenti appartenenti al gruppo degli amministratori di Kaspersky Lab.

I diritti degli operatori della rete logica sono assegnati agli utenti del gruppo **KLOperators**.

I gruppi **KLAdmins** e **KLOperators** vengono creati durante l'installazione del componente Administration Server. L'amministratore può scegliere di creare questi gruppi nel dominio di appartenenza del server amministrativo o direttamente nel computer che esegue l'applicazione Administration Server. I gruppi **KLAdmins** e **KLOperators** possono essere visualizzati e modificati per mezzo degli strumenti di amministrazione standard di Windows (**Utenti e gruppi locali**).

Tutte le operazioni avviate dagli amministratori della rete logica ereditano gli stessi diritti dell'account di servizio del server amministrativo. È possibile creare un gruppo **Amministratori Kaspersky Lab** per ogni server amministrativo. Questo gruppo potrà esercitare diritti amministrativi solo all'interno della rete logica.

Se più computer dello stesso dominio fanno parte di diverse reti logiche, l'amministratore di questo dominio è l'amministratore della rete logica per tutte quelle reti logiche. È possibile creare un solo gruppo **Amministratori Kaspersky Lab** per queste reti logiche durante l'installazione del primo server amministrativo. Per aggiungere nuovi membri al gruppo, servirsi degli strumenti di amministrazione standard di Windows. Tutte le operazioni avviate dagli amministratori della rete logica ereditano gli stessi diritti del server amministrativo corrispondente.

L'amministratore di dominio configura e gestisce le applicazioni Kaspersky Lab solo nei computer del dominio. Se alla rete logica appartengono computer di vari domini, è possibile assegnare i diritti di amministratore di rete logica a un amministratore di dominio agendo come segue:

- Abilitare le relazioni di trust tra i domini
- Aggiungere l'amministratore ai gruppi di amministratori di ogni dominio incluso nella rete logica.

In Kaspersky Administration Kit, i diritti utenti vengono assegnati conformemente all'autenticazione utente Windows nella rete locale.

## 2.7. Estensione della protezione antivirus alla rete logica

Esistono due situazioni comuni che illustrano come estendere un'affidabile protezione antivirus per mezzo di Kaspersky Administration Kit:

- È possibile effettuare l'installazione remota delle applicazioni Kaspersky Lab su computer client dell'intera rete logica da una singola workstation. L'installazione e la connessione al sistema di gestione remoto procedono automaticamente, senza necessità di intervento da parte dell'amministratore. È possibile installare il software antivirus su un numero qualsiasi di client con sistema operativo Windows.
- È possibile installare localmente le applicazioni Kaspersky Lab in ogni computer in rete. In questo caso, tutti i componenti necessari e la workstation dell'amministratore vengono installati manualmente. Le impostazioni di connessione vengono configurate durante l'installazione di Network Agent. Questa modalità è raccomandata nei casi in cui l'implementazione centralizzata sia impossibile.

## 2.8. Creazione di un sistema di gestione centralizzato

La prima fase della creazione di un sistema di gestione centralizzato per una rete aziendale con Kaspersky Administration Kit consiste nel progettare una rete logica. A questo stadio è necessario stabilire quanto segue:

Quale tipo di installazione scegliere: installazione remota o locale? La decisione dipende dalla presenza di strutture di dominio Windows nella rete aziendale.

Quali computer della rete locale svolgeranno la funzione di server amministrativo, workstation dell'amministratore e computer client? Osservare che tutti i computer sui quali sono installate le applicazioni Kaspersky Lab funzioneranno come computer client.

Quali criteri utilizzare per organizzare in gruppi i computer client? Quale sarà la gerarchia del gruppo?

Nella fase successiva, l'amministratore deve realizzare una rete logica, vale a dire installare i seguenti componenti di Kaspersky Administration Kit nei computer della rete:

Administration Server su un computer in rete (cfr. la sezione 3.2 a pag. 36).

Administration Console su un computer in rete dal quale l'amministratore gestirà le applicazioni Kaspersky Lab (cfr. la sezione 3.2 a pag. 36).

Creare quindi una struttura di rete logica, definire la gerarchia dei gruppi di amministrazione e assegnare i computer ai vari gruppi.

Nella fase successiva è necessario installare Network Agent e le applicazioni Kaspersky Lab selezionate nei computer client, e i Console Plug-in corrispondenti nella workstation dell'amministratore (cfr. il Capitolo 3 a pag. 34).

In fine è necessario configurare le applicazioni installate assegnando e applicando le regole di gruppo (cfr. la sezione **Error! Reference source not found.** a pag. **Error! Bookmark not defined.**) e creare le attività (cfr. la sezione **Error! Reference source not found.** a pag. **Error! Bookmark not defined.**).

Grazie alla procedura di Avvio rapido guidato, l'amministratore può creare con facilità un sistema di protezione antivirus per la propria rete e configurarla rapidamente (per una descrizione dettagliata della procedura, cfr. la sezione 4.2 a pag. 50). Configurare rapidamente il sistema di protezione antivirus significa creare una rete logica simile alla struttura di dominio della rete Windows ed estendere il sistema di protezione basato su Kaspersky Anti-Virus 5.0 for Windows Workstations.

## 2.9. Manutenzione di una rete logica

Dopo aver creato una rete logica e installato e configurato le applicazioni antivirus, si raccomanda di eseguire regolarmente le seguenti operazioni:

- Visualizzare i report con i risultati delle prestazioni dell'applicazione nei computer client (cfr. la sezione **Error! Reference source not found.** a pag. **Error! Bookmark not defined.**).
- Controllare la posta elettronica e leggere gli avvisi inviati dai computer client e dal server amministrativo alla casella di posta elettronica dell'amministratore (cfr. la sezione **Error! Reference source not found.** a pag. **Error! Bookmark not defined.**).



L'elenco completo degli avvisi inviati dalle applicazioni Kaspersky Anti-Virus è disponibile nella documentazione delle singole applicazioni.

- Eseguire a distanza dalla workstation dell'amministratore le attività richieste sui client. Per esempio, in caso di evento relativo a virus in un client, è possibile riparare i file nel computer remoto dalla workstation dell'amministratore.
- Aggiornare con tempestività il database antivirus nei computer client (cfr. il 4.10 a pag. 62).

- Aggiornare con tempestività i moduli del programma installati nei computer client (cfr. il 4.10 a pag. 62).
- Monitorare la disponibilità sul server di spazio per l'archiviazione dei dati inviati dai client, e di memoria per l'elaborazione di tali dati.
- Aggiungere nuovi computer alla rete logica e installarvi tempestivamente le necessarie applicazioni antivirus.
- Eseguire con regolarità il backup dei dati del sistema di amministrazione per mezzo dell'utilità `k1backup` (cfr. 4.13 a pag. 66).

## 2.10. Coordinamento degli interventi congiunti degli amministratori

Il sistema consente a più amministratori di lavorare simultaneamente con le stesse risorse. Le ultime modifiche apportate si sostituiscono alle impostazioni precedentemente salvate. Per questo motivo, al fine di evitare equivoci è necessario coordinare il lavoro congiunto di tutti gli amministratori della rete logica.

## 2.11. Interfaccia utente

Dalla workstation dell'amministratore è possibile creare, modificare e configurare la rete logica e gestire tutte le applicazioni Kaspersky Lab installate nei client. L'interfaccia di amministrazione è fornita dal componente Administration Console, un plug-in di amministrazione integrato in Microsoft Management Console (MMC). L'interfaccia di Kaspersky Administration Kit è compatibile con gli standard di MMC.

### 2.11.1. Finestra principale

La finestra principale del programma è dotata di menu, barra degli strumenti, pannello di visualizzazione e pannello dei dettagli. Il menu consente di gestire file e finestre di dialogo nonché di accedere agli argomenti della Guida. I pulsanti della barra degli strumenti consentono di accedere rapidamente alle opzioni di menu utilizzat con maggior frequenza. Il pannello di visualizzazione mostra lo spazio dei nomi gerarchico di **Kaspersky Administration Kit** come struttura ad albero della console. Il pannello dei dettagli visualizza i dati relativi all'oggetto selezionato nella struttura ad albero della console.

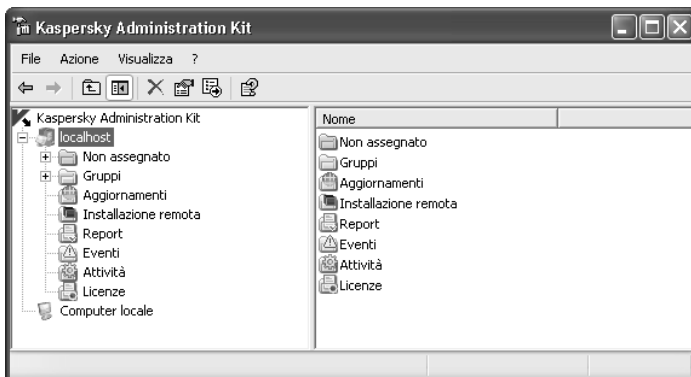


Figura 1. Finestra principale di Kaspersky Administration Kit

## 2.11.2. Struttura ad albero della console

La struttura ad albero della console visualizza le reti logiche create all'interno di una rete aziendale e le proprietà di un computer locale in cui è installata l'Administration Console.

Lo spazio dei nomi di **Kaspersky Administration Kit** può consistere di diversi nodi: **Kaspersky Administration Server (<Nome server>)** (in base al numero di istanze di Administration Server) e l'oggetto **Computer locale**.

L'oggetto **Computer locale** consente di amministrare localmente le applicazioni Kaspersky Lab installate nella workstation dell'amministratore.

Il nodo **Kaspersky Administration Server (<Nome server>)** è un contenitore che visualizza la struttura e le impostazioni del server amministrativo selezionato. Il nodo **KAV Server di Kaspersky Administration Server (<Nome server>)** contiene le seguenti cartelle:

- Non assegnati
- Gruppi
- Aggiornamenti
- Installazione remota
- Report
- Eventi
- Attività
- Licenze



Dopo l'installazione di Kaspersky Administration Kit, l'elemento **Non assegnati** indica la gerarchia del dominio e dei gruppi di lavoro della rete Windows. Le cartelle di ciascun livello superiore visualizzano i computer del dominio o gruppo di lavoro non assegnati alla rete logica. Dopo l'assegnazione di un computer a un gruppo, le informazioni su quel computer vengono eliminate dal nodo **Non assegnati**. Al contrario, quando un computer viene rimosso dalla rete logica, le informazioni su quel computer vengono di nuovo visualizzate nella cartella corrispondente del nodo **Non assegnati**.

È possibile configurare la visualizzazione della gerarchia del nodo **Non assegnati** in modo conforme alla struttura di Active Directory. Per fare questo, selezionare l'elemento **Proprietà** nel menu di scelta rapida del nodo **Non assegnati** e, nella scheda **Generale**, selezionare la casella **Visualizza insieme di strutture di Active Directory**.

Quando si evidenzia una cartella della struttura ad albero della console, nel pannello dei dettagli vengono visualizzate le seguenti informazioni relative alla cartella:

- Nome – Nome dei computer della rete logica
- Tipo di sistema operativo – tipo di sistema operativo installato in un computer client (Server/Workstation).



A seconda del tipo di sistema operativo, a fianco del nome del computer viene visualizzata la seguente icona:  Indica un server e  si riferisce a una workstation.

- **Dominio** – Dominio di Windows o gruppo di lavoro a cui appartiene il computer
- **Ultimo visibile** – Data in cui questo computer è stato identificato l'ultima volta dal server nella rete logica
- **Ultimo aggiornamento** – Data in cui il database antivirus o i moduli dell'applicazione del computer sono stati aggiornati l'ultima volta
- **Status** – Stato corrente del computer (OK/ Attenzione/ Critico) in base ai criteri impostati dall'amministratore.
- **Ultimo aggiornamento info** – Data in cui le informazioni relative al computer sono state aggiornate per l'ultima volta
- **Dominio DNS** – Dominio DNS a cui appartiene il computer
- **Nome DNS** – Nome DNS del computer
- **IP** – Indirizzo IP

Il nodo **Non assegnati** visualizza i contenuti del gruppo **Non assegnati**. Il server amministrativo crea e aggiorna i dati del gruppo **Non assegnati**. Il server richiede regolarmente i dati relativi ai nuovi computer aggiunti alla rete Windows e a quelli rimossi dalla rete. Sulla base di questa informazione, il server aggiorna il gruppo **Non assegnati** e la cartella **Non assegnati**. I nuovi computer visualizzati nella rete Windows vengono automaticamente inclusi in una cartella specifica del gruppo **Non assegnati** (cfr. la sezione 4.6.2 a pag. 57) o nel gruppo specificato della rete logica (cfr. la sezione **Error! Reference source not found.** a pag. 52).

Il nodo **Gruppi** consente di memorizzare, visualizzare, configurare e modificare la struttura della rete logica, le regole del gruppo e le attività del gruppo.

Gli oggetti principali della cartella **Gruppi** corrispondono al livello più elevato della gerarchia della rete logica. Le cartelle **Server**, **Regole** e **Attività** sono obbligatorie per ogni elemento del gruppo. Queste cartelle consentono di utilizzare i server amministrativi, le regole e le attività del livello gerarchico superiore.

Dopo l'installazione di Kaspersky Administration Kit, la cartella **Gruppi** non archivia altri elementi, e le cartelle **Server**, **Regole** e **Attività** sono vuote. L'amministratore può creare la struttura della rete logica aggiungendo computer client e gruppi nidificati alla cartella **Gruppi**.

Un elenco dei computer client di questa cartella viene visualizzato in forma tabulare nel pannello dei dettagli. Il formato e il contenuto della tabella sono simili a quelli della cartella **Non assegnati** (cfr. sopra).

I gruppi sono visualizzati come cartelle simili alla struttura della cartella **Gruppi** principale:

- Le cartelle Server, Regole e Attività vengono create automaticamente. Queste cartelle memorizzano informazioni sui server slave, le regole e le attività del gruppo e vengono create automaticamente alla creazione di ogni gruppo.
- Quando uno o più computer client vengono aggiunti a un gruppo, vengono visualizzati in forma tabulare nel pannello dei dettagli.
- Se viene creata una cartella nidificata all'interno della cartella corrente, la nuova cartella avrà la stessa struttura di quella principale.

Il contenuto della cartella selezionata nella struttura ad albero della console viene visualizzato nel pannello dei dettagli.

Oltre alle informazioni nella cartella **Non assegnati**, sono disponibili i seguenti dati per ciascun client:

- Ultima connessione – Data e ora in cui il client si è connesso l'ultima volta al server amministrativo.

- Data ultima scansione completa – Data e ora dell'ultima scansione antivirus completa del client.
- Virus rilevati – Numero totale di virus intercettati dalla prima scansione all'ultimo azzeramento del contatore. Per azzerare il contatore, fare clic su Azzerata contatore virus nel menu di scelta rapida o nel menu Azione.
- Status protezione in tempo reale – Lo stato corrente della protezione in tempo reale per il client.

È possibile gestire gli oggetti della cartella **Gruppi** per mezzo dei comandi del menu di scelta rapida (cfr. la sezione 2.11.3 a pag. 28).

Il nodo **Aggiornamenti** contiene un elenco degli aggiornamenti disponibili per i client.

Il nodo **Installazione remota** dispone di un elenco di pacchetti di installazione per le applicazioni Kaspersky Lab, utilizzabili per distribuire le applicazioni ai computer client.

Il nodo **Report** visualizza i modelli di report sullo stato della protezione della rete logica.

Il nodo **Eventi** visualizza un elenco di eventi che si sono verificati durante il funzionamento dell'applicazione e registrati nel database del server amministrativo.




Il nodo **Attività** visualizza un elenco di attività globali assegnate ad alcuni computer della rete logica.










Il nodo **Licenze** visualizza le licenze installate nei computer client.

### 2.11.3. Il menu di scelta rapida

Ad ogni tipo di oggetto nello spazio dei nomi **Kaspersky Administration Server** della struttura ad albero della console corrisponde un menu di scelta rapida specifico. Oltre ai comandi MMC standard, questi menu contengono opzioni specifiche per il trattamento degli oggetti. Nella tabella sottostante sono elencati ulteriori comandi per oggetti specifici.











Tabella 1






Oggetto	Comando	Pulsant e barra dei menu	Azione
<b>Kaspersky Administrati on Kit</b>	Nuovo/Kaspersky Administration Server		Aggiunta di un server amministrativo alla struttura ad albero della console
<b>&lt;Nome server&gt;</b>	Server di accesso		Connessione al server amministrativo
	Disconnetti		Disconnessione dal server amministrativo
	Avvio rapido guidato		Esegue l'Avvio rapido guidato
	Distribuzione guidata applicazione		Avvio della Distribuzione guidata applicazione
	Proprietà		Visualizzazione della finestra di dialogo Proprietà di Administration Server
<b>Non assegnati</b>	Proprietà		Visualizzazione delle statistiche del gruppo
<b>Gruppi</b>	Installa		Avvio del programma di installazione remota guidata
	Aggiorna applicazione		Avvio del programma di aggiornamento remoto guidato
	Azzera contatore virus		Azzeramento dei contatori dei virus in tutti i client del gruppo
	Nuovo/Gruppo		Aggiunta di un nuovo gruppo alla struttura della rete logica


Oggetto	Comando	Pulsant e barra dei menu	Azione
	Nuovo/Workstation		Aggiunta di un nuovo client al gruppo
	Proprietà		Visualizzazione delle proprietà del gruppo
<b>Criteria</b>	Nuovo/Regola		Creazione di una nuova regola
<b>Attività</b>	Nuovo/Attività		Creazione di una nuova attività di gruppo
<b>Aggiornamenti</b>	Proprietà		Visualizzazione delle proprietà del nodo <b>Aggiornamenti</b>
<b>Installazione e remota</b>	Nuovo/Pacchetto		Creazione di un nuovo pacchetto di installazione
<b>Report</b>	Nuovo/Report		Creazione di nuovo modello di report
<b>Eventi</b>	Visualizza/Filtro		Applicazione di un filtro per la tabella di anteprima dell'evento
<b>Attività</b>	Nuovo/Attività		Creazione di una nuova attività globale
<b>Licenze</b>	Aggiungi chiave di licenza		Installazione di una nuova chiave di licenza

Nel pannello dei dettagli, ad ogni elemento selezionato nella struttura ad albero della console corrisponde anche uno specifico menu di scelta rapida con opzioni di trattamento. Gli elementi principali e i comandi corrispondenti del menu di scelta rapida sono elencati nella tabella.

Tabella 2

Elemento	Comando	Pulsante barra dei menu	Azione
<b>Regole</b>	Taglia		Trasferimento di una regola negli Appunti
	Incolla		Inserimento di una regola dagli Appunti
	Copia		Copia di una regola negli Appunti
	Elimina		Eliminazione di una regola
	Proprietà		Visualizzazione della finestra di dialogo Proprietà regole
<b>Workstation</b>	Obbliga sincronizzazione		Sincronizzazione dei dati della workstation e del server amministrativo
	Taglia		Trasferimento di un computer client negli Appunti
	Incolla		Inserimento di un computer client dagli Appunti
	Elimina		Eliminazione di un computer client dal gruppo
	Proprietà		Visualizzazione delle proprietà del computer client
	Azzerata contatore virus		Azzeramento dei contatori dei virus in un client specifico
<b>Attività</b>	Avvia		Avvio dell'attività

Elemento	Comando	Pulsante barra dei menu	Azione
	Interrompi		Interruzione dell'attività
	Sospendi		Sospensione dell'attività
	Riprendi		Recupero dell'attività
	Taglia		Trasferimento di un'attività negli Appunti
	Incolla		Inserimento di un'attività dagli Appunti alle attività di gruppo
	Copia		Copia di un'attività negli Appunti
	Elimina		Eliminazione di un'attività
	Proprietà		Visualizzazione della finestra di dialogo Proprietà attività
<b>Pacchetto di installazione</b>	Installa		Creazione di un'attività di distribuzione applicazioni
	Elimina		Eliminazione del pacchetto di installazione
	Proprietà		Visualizzazione della finestra di dialogo Proprietà pacchetto di installazione
<b>Modello report</b>	Genera		Creazione e visualizzazione in anteprima del modello per il report selezionato
	Elimina		Eliminazione del modello del report

Elemento	Comando	Pulsante barra dei menu	Azione
	Proprietà		Visualizzazione della finestra di dialogo Proprietà modello report

---

# CAPITOLO 3. INSTALLAZIONE DI KASPERSKY ADMINISTRATION KIT

La procedura di installazione guidata suggerisce di installare i componenti di Kaspersky Administration Kit (Administration Server e Administration Console) nel computer da cui viene lanciata la procedura stessa. Questa configurazione è raccomandata nei casi in cui sia stata appena iniziata la creazione del sistema di gestione remoto.

Prima dell'installazione, accertarsi che la configurazione di cui si dispone sia conforme ai requisiti hardware e software per il server amministrativo e la workstation dell'amministratore (cfr. la sezione 1.3 a pag. 9).

Per archiviare le informazioni relative al server amministrativo viene utilizzato un server Microsoft SQL o MSDE (Microsoft Data Engine). Pertanto, se la rete aziendale non dispone né dell'uno né dell'altro è necessario installare uno dei due prima di procedere con l'installazione di Administration Server. Per installare MSDE, è possibile servirsi del pacchetto di installazione di Kaspersky Administration Kit. Per istruzioni su come installare MSDE dal CD di installazione di Kaspersky Administration Kit consultare le sezioni successive (cfr. la sezione 3.1 a pag. 34).

Per installare Kaspersky Administration Kit su computer, è necessario disporre dei diritti di amministrazione locale per il computer in questione, e dei diritti di amministratore per il dominio Windows a cui esso appartiene.

## 3.1. Installazione di MSDE per mezzo del pacchetto di installazione di Kaspersky Administration Kit

MSDE viene installato localmente dal pacchetto di installazione di Kaspersky Administration Kit.



*Per installare MSDE:*

1. Inserire il CD di Kaspersky Administration Kit nell'unità CD-Rom ed eseguire il file **setup.exe** nella cartella **MSDE2KSP3**. Si apre una procedura guidata per l'installazione del programma. Dopo aver selezionato le impostazioni di installazione, avviare la procedura. Seguire le istruzioni dell'applicazione.
2. Le prime fasi dell'installazione consistono nell'estrazione e nella copia dei file sul disco fisso, nell'accettazione del contratto di licenza e nell'inserimento delle informazioni sull'utente.
3. Nella finestra di dialogo **Scegliere la cartella di destinazione**, specificare quanto segue:
  - La cartella di destinazione dei file di MSDE (nel campo **Programmi**). Il percorso predefinito è Programmi\Microsoft SQL Server. Se la cartella non esiste, il programma la crea.
  - La cartella in cui sarà salvato il database del server MSDE (nel campo **File di dati**). Il percorso predefinito è Programmi\Microsoft SQL Server.
4. Per scegliere destinazioni diverse, fare clic su **Sfogli...**

Nella finestra di dialogo Nome dell'istanza di MSDE 2000 (cfr. la Figura 2), scegliere il nome da assegnare al server MSDE.

Il nome predefinito è KAV\_CS\_Admi\_Kit. Selezionare la casella Predefinito se si accetta di usare il nome predefinito.

Se si preferisce scegliere un nome diverso, deselezionare la casella Predefinito e digitare il nuovo nome tynel campo **Nome dell'istanza**.



Figura 2. Installazione MSDE. Selezione di un nome per l'istanza.

Dopo aver configurato le impostazioni di installazione, è possibile rivederle e iniziare la procedura. A questo punto, MSDE è stato installato come richiesto per il funzionamento di Kaspersky Administration Kit.



Se installato dal pacchetto di installazione di Kaspersky Administration Kit, MSDE può essere utilizzato solo per questa applicazione.

## 3.2. Installazione di Administration Server e di Administration Console



*Per installare Administration Server e Administration Console:*

1. Eseguire il file **Setup.exe** dal CD di Kaspersky Anti-Virus per avviare la procedura di installazione guidata. Dopo aver selezionato le impostazioni di installazione, avviare la procedura. Seguire le istruzioni dell'applicazione.
2. Le prime fasi dell'installazione consistono nell'estrazione e nella copia dei file sul disco fisso, nell'accettazione del contratto di licenza e nell'inserimento delle informazioni sull'utente.

3. Selezionare la cartella di destinazione. La cartella predefinita è **Programmi\Kaspersky Lab\Kaspersky Administration Kit**. Se la cartella non esiste, il programma la crea automaticamente. Per scegliere una cartella diversa, fare clic su **Sfoggia...**
4. Scegliere i componenti di Kaspersky Administration Kit che si desidera installare (cfr. la Figura 3):
  - **Kaspersky Administration Console** – per installare Administration Console;
  - **Kaspersky Administration Server** – per installare Administration Server.

Si può scegliere di installare entrambi i componenti o solo Administration Console. Al contrario, non è possibile installare Administration Server senza installare anche Administration Console. Per impostazione predefinita, vengono installati entrambi i componenti.

Nella finestra di dialogo della procedura di installazione sono indicate le seguenti informazioni di riferimento:

- Il campo **Descrizione** sul lato sinistro visualizza le informazioni relative al componente selezionato.
- Il campo **Spazio** richiesto su visualizza i requisiti di memoria per i componenti selezionati.
- Il campo **Spazio** disponibile indica la memoria disponibile nel disco su cui si stanno installando i componenti.

Se si è scelto di installare solo Administration Console, non sono necessarie altre operazioni. Il programma di installazione guidata suggerisce a questo punto di rivedere le impostazioni di installazione e di avviare la procedura.

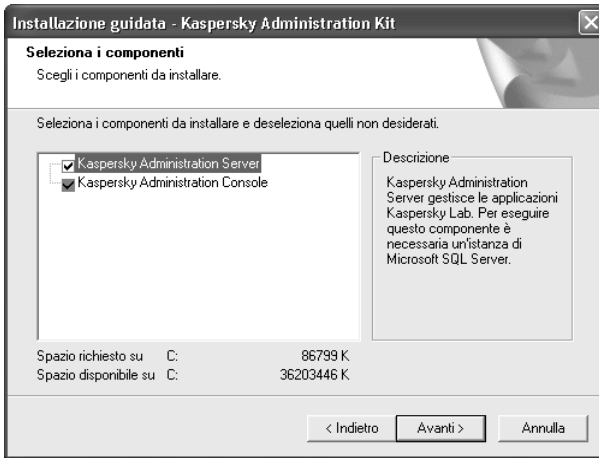


Figura 3. Installazione di Kaspersky Administration Kit. Selezione dei componenti da installare.

5. Se si è scelto di installare anche Administration Server, definire il percorso della cartella condivisa (cfr. la Figura 4) in cui saranno salvati:
  - I file necessari per l'installazione remota delle applicazioni Kaspersky Lab (essi vengono copiati nel server amministrativo al momento della creazione dei pacchetti di installazione)
  - Le copie degli aggiornamenti dalla posizione originaria al server amministrativo

I diritti di lettura di questa cartella saranno assegnati a tutti gli utenti.

È possibile selezionare una delle seguenti opzioni:

- Crea nuova cartella condivisa – Per creare una nuova cartella, digitare il percorso desiderato nel campo sottostante e indicare il nome nel campo Nome condivisione.
- Seleziona cartella condivisa esistente – Selezionare una cartella condivisa tra le cartelle esistenti.

La cartella condivisa può trovarsi nel computer locale o in qualsiasi computer remoto della rete aziendale.

La cartella predefinita Condivisione viene creata nella directory Kaspersky Administration Kit.

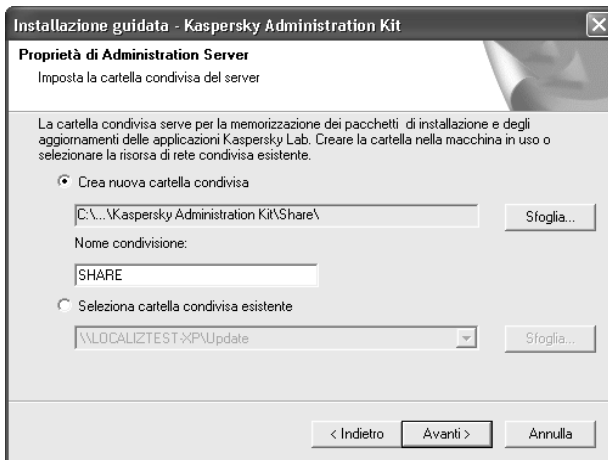


Figura 4. Installazione di Kaspersky Administration Kit. Creazione di una cartella condivisa.

6. Definire le impostazioni della porta per la connessione al server amministrativo (cfr. la Figura 5):
  - Il campo **Porta server** indica il numero della porta usata per connettersi al server amministrativo. La porta predefinita è la 14000. Se questa è già in uso, cambiare numero.
  - Il campo **Porta SSL server** indica il numero della porta usata per connettersi al server amministrativo tramite SSL. La porta predefinita è la 13000.

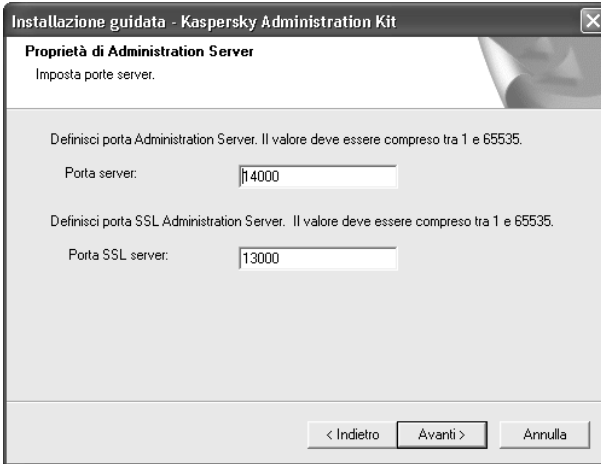


Figura 5. Installazione di Kaspersky Administration Kit. Impostazioni porta

7. Definire l'account di servizio in cui sarà avviato il server amministrativo nel computer in questione (cfr. la Figura 6).



Figura 6. Installazione di Kaspersky Administration Kit. Impostazione dell'account di servizio.

È possibile selezionare una delle seguenti opzioni:

- **Account utente di dominio** – Per avviare Administration Server in un account utente di dominio. Administration Server eseguirà tutte le operazioni con i diritti assegnati a tale account. Per la fase successiva è necessario specificare il nome utente di dominio per accedere al server.



Se la rete aziendale ha una struttura di dominio Windows, si raccomanda di accedere ad Administration Server per mezzo dell'account amministratore di dominio. In questo caso, Administration Server ha accesso a tutte le necessarie risorse amministrative.

- **Account di sistema locale** – Per avviare Administration Server in nell'account Sistema locale. Questa opzione è raccomandata se la rete non ha una struttura di **dominio** Windows. In questo caso non è necessario selezionare un utente ed è possibile individuare direttamente il database del server MSDE (cfr. il Passaggio 0 a pag. 43).



Per il corretto funzionamento di Kaspersky Administration Kit, l'account di servizio per l'avvio del server amministrativo deve avere diritti di amministratore per il computer in cui si trova il database MSDE.

8. Se si imposta Administration Server per l'avviamento in un account utente di dominio, è necessario specificare il nome utente nella finestra di dialogo successiva della procedura di installazione guidata.

Nella finestra di dialogo (cfr. la Figura 7) specificare il nome utente tra quelli registrati nel dominio. Per fare questo, digitare il nome desiderato nel campo **Nome utente** o fare clic su **Sfoglia...** per selezionare un utente.

Se l'account dell'utente specificato non ha diritti di amministratore, Administration Server sarà avviato in questo account ma con funzionalità di Kaspersky Administration Kit limitate. Per esempio, a causa dei diritti limitati dell'account selezionato, l'installazione basata su script su computer remoti può risultare impossibile (cfr. la sezione **Error! Reference source not found.** a pag. 55), oppure alcuni domini della rete Windows possono non essere accessibili. In ogni caso viene visualizzato l'avviso corrispondente (cfr. la Figura 8).



Per eseguire le applicazioni installate forzatamente su client remoti, l'account utente deve disporre del diritto di **Accesso come servizio**. Per avviare attività di installazione remota in situazioni di avvio, è necessario disporre dei diritti di modifica di tali situazioni nel database del controller di dominio.

Nel campo **Password**, digitare la password utente per l'account utente di dominio.

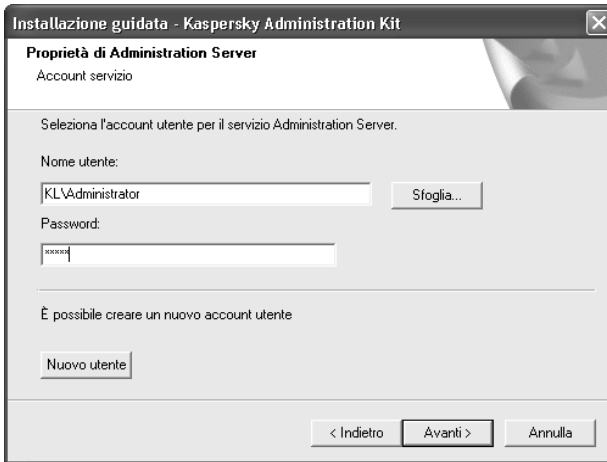


Figura 7. Installazione di Kaspersky Administration Kit. Selezione di un utente.

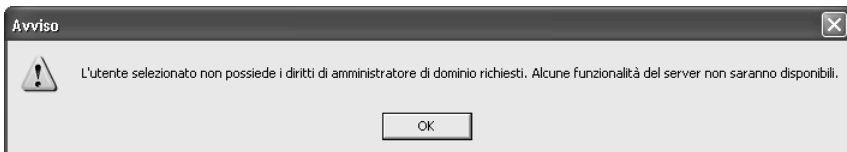


Figura 8. Installazione di Kaspersky Administration Kit.  
Avvertenza sulle funzionalità limitate di Administration Server.

Se l'account di dominio selezionato dispone dei diritti di amministratore di dominio ma non del diritto di **Accesso come servizio**, tale diritto gli sarà assegnato automaticamente (cfr. la Figura 9).

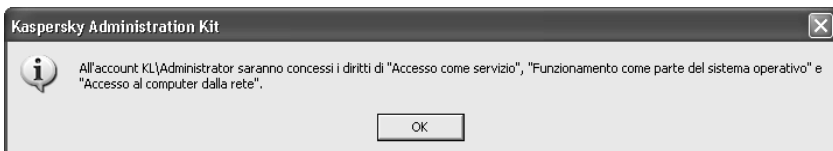


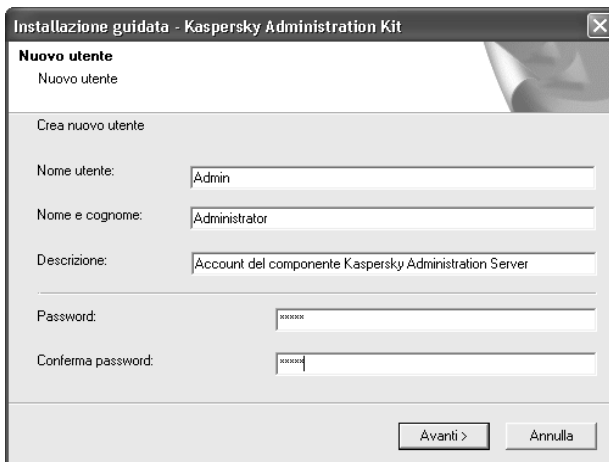
Figura 9. Installazione di Kaspersky Administration Kit.  
Messaggio di assegnazione del diritto di **Accesso come servizio** all'utente.

I diritti di amministratore di dominio consentono di creare un utente speciale e di utilizzarne l'account per accedere ad Administration Server. I

diritti di amministratore di dominio e di **Accesso come servizio** vengono assegnati automaticamente all'utente in questione.

Per creare un utente speciale, fare clic sul pulsante **Nuovo utente...** e inserire le seguenti informazioni nella nuova finestra di dialogo (cfr. la Figura 10):

- Nome utente nel campo **Nome utente** (obbligatorio).
- Nome e cognome completo dell'utente nel campo **Nome e cognome** (facoltativo).
- Informazioni sull'utente nel campo **Descrizione**. Il valore predefinito è Account del componente Kaspersky Administration Server (facoltativo).
- Password nel campo **Password** (obbligatorio).
- Conferma della password nel campo **Conferma password** (obbligatorio).



Installazione guidata - Kaspersky Administration Kit

**Nuovo utente**  
Nuovo utente

Crea nuovo utente

Nome utente:

Nome e cognome:

Descrizione:

Password:

Conferma password:

Avanti > Annulla

Figura 10. Installazione di Kaspersky Administration Kit.  
Creazione di un nuovo utente.

9. Nella fase successive è necessario definire la risorsa (server MSDE o Microsoft SQL) da utilizzare per l'archiviazione del database di Administration Server (cfr. la Figura 11). Senza questa impostazione non è possibile passare alla fase successiva dell'installazione.



Se Administration Server viene eseguito in Windows XP SP2, la firewall integrata blocca le porte TCP 13000 e 14000. Pertanto è necessario aprirle manualmente per consentire l'accesso ad Administration Server.

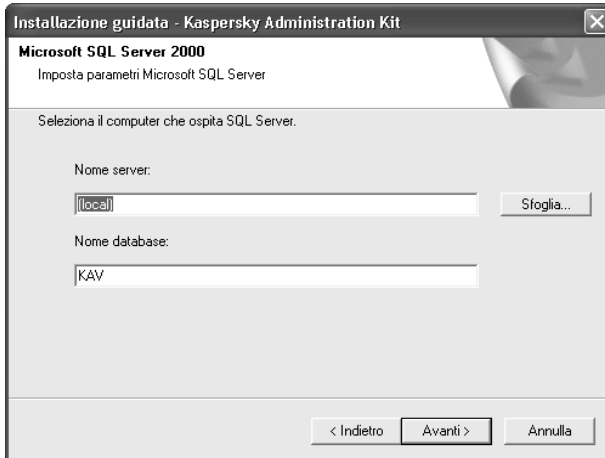


Figura 11. Installazione di Kaspersky Administration Kit. Selezione di un server SQL.

Se nella rete aziendale si trova un server MSDE o MS SQL e si prevede di utilizzarlo per Kaspersky Administration Kit, specificare il nome del server nel campo **Nome server** e il nome del database nel campo **Nome database**. **KAV** è il nome del database predefinito.

Fare clic su **Sfoggia...** per visualizzare un elenco di tutti i server Microsoft SQL presenti in rete. Se il server SQL si trova sullo stesso computer dal quale si sta installando Kaspersky Administration Kit, nel campo **Nome server** viene automaticamente specificato il valore **locale**.

Se nella rete non ci sono server MS SQL o non è possibile utilizzare i server esistenti, è necessario installarlo (cfr. la sezione 3.1 a pag. 34).

Per installare Microsoft SQL Server nel computer su cui si sta installando Kaspersky Administration Kit, è necessario annullare l'installazione corrente, installare SQL Server, quindi riavviare l'installazione.

Per installare Microsoft SQL Server su un computer remoto, non è necessario interrompere l'installazione di Kaspersky Administration Kit. È possibile installare Microsoft SQL Server e passare quindi all'installazione di Kaspersky Administration Kit.

Visualizzare le impostazioni di installazione di Kaspersky Administration Kit e avviare il programma di installazione.

Al termine dell'installazione, il comando di scelta rapida di Kaspersky Administration Kit viene visualizzato nel menu **Avvio\Programmi\Kaspersky Administration Kit**.

Administration Server viene installato su un computer con le seguenti impostazioni predefinite:

- Nome: Kaspersky Administration Server;
- Caricamento automatico all'avvio del sistema;
- Account: Account Sistema locale o account definito dall'utente (alle pagg. 39 e 41).

Per visualizzare le proprietà dei servizi di **Kaspersky Administration Server** e monitorare le prestazioni del programma, usare lo strumento di amministrazione **Servizi**. I risultati delle prestazioni dei servizi di **Kaspersky Administration Server** vengono registrati nel registro di sistema di Windows nel computer in cui è installato Administration Server.

I gruppi utenti locali **KLAdmins** e **KLOperators** vengono creati in un computer in cui sia installato Administration Server. Se Administration Server è configurato in modo da operare in un account utente assegnato al dominio, i gruppi **KLAdmins** e **KLOperators** vengono aggiunti all'elenco dei gruppi utenti di dominio. Per modificare i gruppi, è possibile utilizzare gli strumenti amministrativi Windows standard.

### 3.3. Disinstallazione dei componenti di Kaspersky Administration Kit

Per disinstallare i componenti di Kaspersky Administration Kit, servirsi degli strumenti Windows standard (**Start** → **Pannello di controllo** → **Installazione applicazioni**). Administration Server e Administration Console saranno rimossi.

### 3.4. Aggiornamento della versione del programma

Per aggiornare Kaspersky Administration Kit dalla versione 4.x alla versione 5.0, disinstallare la versione precedente e installare la nuova, seguendo le istruzioni di installazione descritte in questo manuale.

---

# CAPITOLO 4. GUIDA INTRODUTTIVA

## 4.1. Avvio del programma e connessione al server amministrativo

Per avviare Kaspersky Administration Kit, selezionare **Kaspersky Administration Kit** all'interno del gruppo **Kaspersky Administration Kit** del menu **Avvio\Programmi**. Il gruppo del programma viene creato solo nelle workstation degli amministratori durante l'installazione di Administration Console.



È possibile usare Kaspersky Administration Kit solo se il server amministrativo è in funzione.

Dopo l'avvio, la finestra principale del programma visualizza la struttura ad albero della console con lo spazio nome **Kaspersky Administration Kit** al livello più alto. Affinché il programma visualizzi la struttura della rete logica e le sue impostazioni, è necessario connettersi al server amministrativo. Il programma riceve le informazioni relative alla struttura della rete logica dal server amministrativo e le visualizza nella struttura ad albero della console.



*Per connettersi a un server amministrativo, selezionare il nodo **Kaspersky Administration Server (<Nome server>)** nella struttura ad albero della console.*

L'applicazione cerca quindi di connettersi al server amministrativo. Se nella rete vi sono più server amministrativi, il programma si connette all'ultimo server a cui si era connesso nella precedente sessione di Kaspersky Administration Kit. Al primo avvio dell'applicazione, si presuppone che Administration Server e Administration Console siano in esecuzione sullo stesso computer. Pertanto il programma tenterà di rilevare Administration Server su quel computer.

Se il server non viene rilevato, l'applicazione richiede di specificarne il nome manualmente nella finestra di dialogo **Accesso** (cfr. la Figura 12). Digitare il nome del server nel campo **Indirizzo server**. È possibile inserire l'indirizzo IP o il nome NetBIOS (nome del computer nella rete MS Windows). La comunicazione tra Administration Server e

Administration Console avviene mediante SSL. Se si desidera disabilitare il protocollo SSL, deselegionare la casella **Usa connessione SSL**. Questo tuttavia potrebbe pregiudicare la sicurezza delle informazioni e l'integrità dei dati.



Per connettersi al server amministrativo attraverso una porta diversa da quella predefinita, digitare **<Nome server>:<Numero porta>** nel campo **Indirizzo server**.

Impostazioni di connessione

Indirizzo server:

Usa connessione SSL

Usa compressione dati

Utilizza server proxy

Indirizzo server proxy:

Nome utente:

Password:

OK Annulla Opzioni <<

Figura 12. Connessione al server amministrativo

Fare clic sul pulsante **Opzioni** per visualizzare/nascondere le seguenti impostazioni avanzate di connessione:

- **Usa connessione SSL.** Selezionare la casella per trasmettere dati tra Administration Server e Administration Console mediante SSL. Deselezionare la casella se non si desidera applicare il protocollo SSL. Questo tuttavia potrebbe pregiudicare l'integrità e la sicurezza dei dati trasmessi.
- **Utilizza server proxy.** Selezionare la casella se si desidera connettersi al server amministrativo per mezzo di un server proxy. Indicare l'indirizzo per la connessione al server proxy nel campo **Indirizzo server proxy**. Compilare i campi **Nome utente** e **Password** se il server proxy richiede l'autorizzazione dell'utente.

Administration Console verifica quindi i diritti dell'utente di connettersi al server amministrativo. Se la connessione avviene mediante SSL, Administration Console autentica Administration Server (cfr. la sezione 2.4.2 a pag. 18) prima di verificare i diritti dell'utente.

Se ci si connette al server per la prima volta o se il certificato del server per questa sessione è diverso dalla copia locale, viene visualizzata una

richiesta di connessione al server e di un nuovo certificato (cfr. la Figura 13). Selezionare una delle seguenti operazioni:

- **Connettersi al server e scaricare il certificato** – Selezionare questa opzione per connettersi al server amministrativo e ottenere un nuovo certificato.
- **Specificare il percorso del file certificato** – Selezionare questa opzione per specificare la posizione del certificato. Fare clic su **Sfoglia...** per cercare il file del certificato. Il file presenta l'estensione .cer e si trova nella cartella Cert all'interno della directory Kaspersky Administration Kit nel server amministrativo. La Console tenta di autenticare il server utilizzando il certificato specificato dall'utente.



È possibile copiare il certificato in una cartella condivisa o su un dischetto. Questa copia potrà essere utilizzata per configurare le impostazioni di accesso.



Figura 13. Richiesta di connessione al server amministrativo.

I diritti dell'utente vengono verificati per mezzo della procedura di autenticazione utente di Windows. Se l'utente non è autorizzato ad accedere al server amministrativo, vale a dire non è in possesso dei diritti di operatore della rete logica (**KLOperators**) o di amministratore (**KLAdmins**), provare a collegarsi da un altro account (cfr. la Figura 14). Nell'apposito spazio, indicare l'account utente (nome e password) con diritti di operatore di rete logica o di amministratore.



Figura 14. Registrazione di un utente per l'accesso al server amministrativo

Se la connessione riesce, la struttura della rete logica e le impostazioni appaiono nella struttura ad albero della console.



*Per disconnettersi da un server amministrativo, selezionare il nodo **Kaspersky Administration Server (<Nome server>)** nella struttura ad albero della console e fare clic su **Disconnetti** nel menu di scelta rapida o nel menu **Azione**.*

Se nella rete Windows vi sono più server amministrativi, è possibile gestire le reti logiche dalla workstation di un amministratore. Per selezionare un'altra rete logica, connettersi al server amministrativo desiderato o aggiungere dei server alla struttura della rete e connettersi a uno di essi.



È possibile gestire simultaneamente più server amministrativi e reti logiche solo se si possiedono diritti di operatore o di amministratore per ciascuna di tali reti.



*Per connettersi al server amministrativo:*

Selezionare il nodo **Kaspersky Administration Server (<Nome server>)** nella struttura ad albero della console della finestra principale di **Kaspersky Administration Kit** e fare clic sull'opzione **Server di accesso** nel menu di scelta rapida o nel menu **Azione**. Nella finestra di dialogo **Accesso** (cfr. la Figura 12), digitare il nome del server (vedere sopra) e, se necessario, selezionare la casella **Usa connessione SSL** per abilitare la connessione sicura.



Se non si possiedono i diritti di operatore della rete logica o di amministratore per la rete selezionata, l'accesso al server amministrativo sarà negato.

Se la connessione riesce, il contenuto del nodo **Kaspersky Administration Server (<Nome server>)** viene aggiornato.



Per aggiungere un nuovo server amministrativo alla struttura ad albero della console:

Selezionare il nodo **Kaspersky Administration Server** dalla finestra principale di Kaspersky Administration Kit, aprire il menu di scelta rapida e fare clic sul comando **Nuovo/KAV Server** (o selezionare questo comando dal menu **Azione**).

Come risultato, nella struttura ad albero della console appare un nuovo nodo dal nome **Kaspersky Administration Server (<Non connesso>)**. Esso può essere utilizzato per connettersi a un altro server installato nella rete Windows.

## 4.2. Avvio rapido guidato

Per mezzo di una procedura guidata di Kaspersky Administration Kit, è possibile configurare un set minimo di parametri per la creazione di un sistema di gestione centralizzata di protezione antivirus. Questa procedura consente di configurare i seguenti parametri:

- Rete logica con una struttura simile a quella di domini e gruppi utenti della rete Windows. Importare la struttura della rete logica dalle precedenti versioni di Kaspersky Administration Kit (versione 4.0 o 4.5) (selezionate dall'amministratore).



Se un computer non è disponibile in modalità **Non assegnati** durante la creazione di una rete logica (disattivata o disconnessa dalla rete), la procedura guidata non lo aggiunge alla rete logica. Tale computer potrà essere aggiunto in seguito durante la configurazione manuale della rete logica (cfr. la sezione **Error! Reference source not found.** a pag. 52).



La creazione di una rete logica per mezzo della procedura di Avvio rapido guidato non pregiudica l'integrità della rete: vengono aggiunti nuovi gruppi che non sostituiscono quelli esistenti. Un computer client già assegnato a un gruppo esistente non viene aggiunto in questa fase, poiché il gruppo **Non assegnati** visualizza solo i computer non inclusi nella rete logica.

- Workstations. Essa si chiama **Aggiornamento attività per Kaspersky Anti-Virus for Windows Workstations** e presenta impostazioni predefinite.

## 4.3. Visualizzazione, creazione e configurazione di una rete logica

La struttura della rete logica, la gerarchia e i gruppi amministrativi devono essere definiti in fase di pianificazione. Per creare una rete logica, è necessario aprire la finestra principale di Kaspersky Administration Kit, creare una gerarchia di gruppi nella cartella **Gruppi** e aggiungervi dei client.

Per creare una rete logica basata sulla struttura del dominio e del gruppo utenti nella rete Windows, è possibile usare la procedura di Avvio rapido guidato (cfr. la sezione 4.2 a pag. 50).



*Per creare manualmente una rete logica:*

- Connettersi al server amministrativo (cfr. il Capitolo 4 a pag. 46).
- Organizzare una gerarchia di gruppo creando dei gruppi nidificati (cfr. la sezione **Error! Reference source not found.** a pag. **Error! Bookmark not defined.**).
- Aggiungere ai gruppi i client necessari (cfr. la sezione **Error! Reference source not found.** a pag. 52).



Per attivare l'installazione automatica delle applicazioni Kaspersky Lab sui nuovi computer aggiunti alla rete, con MS Windows 98/ME, è necessario che essi siano dotati di Network Agent.

Se un gruppo viene trasferito in un altro gruppo, vengono spostati anche tutti i gruppi nidificati, i client e le regole e attività di gruppo. Al gruppo rimosso vengono assegnate nuove impostazioni secondo la nuova posizione nella gerarchia della rete logica.

Accertarsi che il nome del gruppo trasferito sia esclusivo. Per evitare conflitti di nome, rinominare il gruppo prima di spostarlo. Se il nome non è esclusivo all'interno di un gruppo, in fondo al nome del nuovo gruppo viene aggiunto automaticamente un suffisso numerico: **\_1, \_2, ....**



Non è possibile rinominare la cartella **Gruppi** perché si tratta di un elemento incorporato di Administration Console.

Un gruppo può essere eliminato dalla rete logica se non contiene gruppi nidificati o computer client. Per eliminare il gruppo selezionato, fare clic su **Elimina** nel menu di scelta rapida o nel menu **Azione**.

---

## 4.4. Gerarchia dei server amministrativi

Più server amministrativi possono costituire una gerarchia di tipo “primario–secondario”. Il server principale di questa gerarchia può avere numerosi server secondari.

Attraverso i server secondari, il server primario può svolgere le seguenti attività:

- Creare regole globali sia per i server amministrativi secondari sia per i computer client connessi a tali (per ulteriori informazioni sull'argomento, cfr. la sezione **Error! Reference source not found.** a pag. **Error! Bookmark not defined.**).
- Creare attività globali sia per i server amministrativi secondari sia per i computer client connessi a tali (cfr. la sezione **Error! Reference source not found.** a pag. **Error! Bookmark not defined.**).
- Trasferire i computer client da un server amministrativo a un altro server.
- Creare report sintetici relativi a tutti i server amministrativi secondari (cfr. la sezione **Error! Reference source not found.** a pag. **Error! Bookmark not defined.**).
- Distribuire gli aggiornamenti dal server amministrativo principale ai server secondari (cfr. la sezione **Error! Reference source not found.** a pag. **Error! Bookmark not defined.**).



Ogni computer client inserito in una struttura di rete logica deve essere connesso a un solo server amministrativo.

L'amministratore deve controllare la connessione dei computer client al server amministrativo per mezzo dell'opzione di ricerca dei computer attraverso le reti logiche di diversi server in base alle rispettive proprietà di rete.

## 4.5. Installazione e disinstallazione di applicazioni sui client

Prima dell'installazione, accertarsi che i computer client siano conformi ai requisiti hardware e software (cfr. la sezione 1.3 a pag. 9).

Network Agent stabilisce la connessione tra il server amministrativo e i computer client. Pertanto deve essere installato su ogni computer connesso al sistema di gestione remota prima di installare le applicazioni antivirus.

## 4.6. Installazione (distribuzione) e disinstallazione remota di software

È possibile installare e disinstallare remotamente solo le applicazioni Kaspersky Lab dotate di uno speciale file con una definizione di applicazione nel CD di installazione del programma. Questo file **.kpd** serve per creare e salvare un pacchetto di installazione in Administration Server. Il pacchetto di installazione contiene anche i file con le definizioni delle impostazioni del pacchetto stesso.



Il pacchetto di installazione contiene il file usato per l'installazione locale delle applicazioni in modalità silenziosa.



*Per installare le applicazioni Kaspersky Lab su client remoti:*

- Creare un pacchetto di installazione per l'applicazione che si desidera installare (cfr. la sezione 4.6.1 a pag. **Error! Bookmark not defined.**) (se il pacchetto non è ancora stato creato). Una volta creato il pacchetto di installazione, verrà installato il plug-in della Console sulla workstation dell'amministratore.
- Specificare un'attività di distribuzione dell'applicazione (cfr. la sezione **Error! Reference source not found.** a pag. 55).

Tale attività sarà programmata per essere eseguita ad orari specificati. Le installazioni non gestite proseguono su tutti i client di destinazione fino al completamento; il server amministrativo deve ricevere l'informazione dell'avvenuta installazione delle applicazioni su tutti i client. L'applicazione installata viene avviata sui computer client al termine dell'installazione. Le impostazioni dell'applicazione in ogni client saranno configurate in base alle regole e alle impostazioni predefinite del gruppo di appartenenza.

Il processo di installazione può essere interrotto (cfr. la sezione **Error! Reference source not found.** a pag. **Error! Bookmark not defined.**).



Se l'installazione remota in un client è stata completata con successo, non sarà avviata nuovamente sullo stesso computer la volta successiva.

## 4.6.1. Creazione dei pacchetti di installazione

Al termine della procedura guidata, un nuovo pacchetto di installazione viene aggiunto al nodo **Installazione remota** e visualizzato nel pannello dei dettagli.

Le impostazioni predefinite del pacchetto di installazione di Network Agent forniscono le funzionalità di base del programma. È possibile iniziare a usare il componente con le impostazioni predefinite subito dopo l'installazione.



In caso di reinstallazione di Network Agent su un client, le impostazioni di connessione e il certificato di Administration Server vengono aggiornati automaticamente.



Dopo l'installazione di Network Agent, non è più possibile modificare il nome della cartella deputata a contenere i nuovi computer aggiunti al gruppo **Non assegnati**. Non è possibile modificare questa impostazione per mezzo di regole o impostazioni dell'applicazione.

## 4.6.2. Creazione di un'attività di distribuzione delle applicazioni

Vi sono due metodi per eseguire un'attività di distribuzione delle applicazioni sui computer client: **Installazione "push"** e **installazione basata su script con login**.

L'**installazione "push"** consente di effettuare l'installazione remota di applicazioni su computer client specifici della rete logica. Nell'esecuzione dell'attività di distribuzione delle applicazioni, il server amministrativo copia i file di installazione per l'applicazione desiderata dalla cartella condivisa in ciascun computer client, ed esegue il programma di setup su tali computer. Per forzare l'installazione di un'applicazione, il server amministrativo deve disporre dei diritti di avviare applicazioni a distanza su client della rete logica. Questo metodo è raccomandato per l'installazione di applicazioni su computer con MS Windows NT/2000/2003/XP che supportano questa funzionalità, o su computer con MS Windows 98/Me su cui è installato Network Agent.



Se il server amministrativo e un client interagiscono attraverso i canali di Internet o se la connessione è protetta da una firewall, non è possibile utilizzare le cartelle condivise per il trasferimento dei dati. In questo caso, Network Agent può essere usato per trasferire file di installazione nel client (cfr. la sezione **Error! Reference source not found.** a pag. **Error! Bookmark not defined.**). Su tali computer, Network Agent deve essere installato localmente.

**L'installazione basata su script con login** consente di avviare la distribuzione di applicazioni quando un utente specifico si collega al dominio (più utenti). In base alla programmazione delle attività, la condizione di avvio del programma di setup è definita nello script di login di utenti specifici. Il programma di setup dell'applicazione è conservato nella cartella condivisa nel server amministrativo. Per avviare attività di distribuzione di applicazioni, è necessario che il server amministrativo disponga dei diritti di modifica degli script di login nel database del controller di dominio. Quando un utente specificato si collega al dominio, l'installazione viene avviata sul computer client da cui l'utente si è collegato. Questo metodo è raccomandato se si stanno installando applicazioni Kaspersky Lab su computer con MS Windows 95/98/Me..



Per installare applicazioni Kaspersky Lab su client che non appartengono al dominio, accedere come utente con diritti di amministratore su tali client per avviare l'attività di installazione remota.

- Modifica account per l'avvio di questa attività.
- Seleziona se reinstallare le applicazioni esistenti su un client.
- Specifica la modalità di distribuzione dei file di installazione sui client.
- Determina il numero di tentativi per l'avvio dell'attività (se l'attività è programmata).

### 4.6.3. Installazione locale delle applicazioni

L'installazione locale viene eseguita separatamente su ciascun computer. Per installare localmente un'applicazione, sono necessari i diritti di amministratore sul computer interessato.

I paragrafi seguenti descrivono un piano ipotetico di installazione locale delle applicazioni Kaspersky Lab:

- Installare Network Agent e stabilire la connessione tra il client e il server amministrativo (cfr. la sezione **Error! Reference source not found.** a pag. 57).

- Installare le applicazioni desiderate sui computer da includere nel sistema di protezione antivirus seguendo le istruzioni riportate nei rispettivi manuali.
- Installare i plug-in di gestione per ogni applicazione installata sulla workstation dell'amministratore (cfr. la sezione **Error! Reference source not found.** a pag. **Error! Bookmark not defined.**).

Kaspersky Administration Kit supporta l'installazione locale delle applicazioni in modalità "silenziosa", sulla base dei file creati durante la realizzazione del pacchetto di installazione (cfr. la sezione **Error! Reference source not found.** a pag. **Error! Bookmark not defined.**).

---

## 4.7. Gestione delle regole

È possibile creare una regola per un'applicazione solo se sulla workstation dell'amministratore è presente il plug-in Console per l'applicazione interessata.



Le impostazioni di applicazioni locali hanno una priorità più elevata rispetto alle impostazioni di regole. Affinché una regola possa avere effetto sui computer client, è necessario bloccare determinati parametri.

La nuova regola creata sarà aggiunta alla cartella **Regole** del gruppo selezionato e di tutti i gruppi nidificati all'interno dello stesso come regola ereditata. La nuova regola sarà visualizzata nel pannello dei dettagli. La regola sarà assegnata ai client durante la prima sincronizzazione client/server.

Essa sarà applicata come segue. Se su un client sono in esecuzione attività residenti (protezione in tempo reale), le nuove impostazioni della regola saranno applicate a tali attività senza soluzione di continuità. Le attività periodiche in corso in un client (come la scansione manuale o l'aggiornamento del database) continueranno a usare le vecchie impostazioni. Le nuove impostazioni della regola saranno applicate al successivo avvio delle attività interessate. Per visualizzare le impostazioni dell'applicazione con la nuova regola, aprire le schede **Applicazioni** e **Attività** nella finestra di dialogo **Proprietà <Nome computer>** che visualizza le proprietà di un client specifico.

È possibile copiare o trasferire le regole da un gruppo a un altro ed eliminarle per mezzo dei comandi **Copia/Incolla**, **Taglia/Incolla** o **Elimina** nel menu di scelta rapida o nel menu **Azione**. Le regole possono anche essere trascinate in una diversa destinazione per mezzo del mouse.

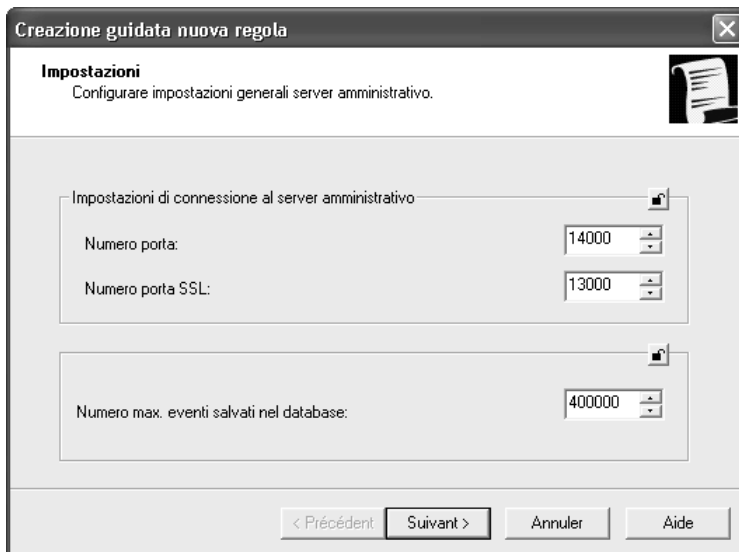


Figura 15. Creazione di una regola per Kaspersky Anti-Virus 5.0 for Windows Workstations

## 4.7.1. Visualizzazione e modifica di una regola

In fase di modifica, è possibile cambiare la regola o bloccare le impostazioni di regole e di applicazioni per i gruppi nidificati.



*Per visualizzare e/o modificare le impostazioni delle regole di un gruppo:*

Nella struttura ad albero della console, scegliere il gruppo e selezionare la relativa cartella **Regole**. Nel pannello dei dettagli, è visibile un elenco di tutte le regole create per il gruppo. Selezionare la regola desiderata e fare clic sul comando **Proprietà** nel menu di scelta rapida o nel menu **Azione**.

Si apre la finestra di dialogo **Proprietà <Nome regola>** con alcune schede che consentono di configurare regole di gruppo per un'applicazione. Le schede sono specifiche per ogni applicazione e la loro descrizione è fornita nei rispettivi manuali. Osservare che le schede **Generale**, **Applicazione** ed **Elaborazione eventi** sono comuni a tutte le applicazioni.

**attività/Importa.** Questo comando può essere selezionato anche dal menu **Azione**.

Nella finestra che si apre, specificare il nome del file in cui importare la regola e fare clic su **Apri**.



Se nel gruppo esiste già una regola per questa applicazione, non sarà possibile importare una nuova regola.

## 4.8. Gestione delle attività

È possibile gestire le applicazioni Kaspersky Lab installate sui client della rete logica creando e avviando attività. È possibile inoltre assegnare e implementare a distanza le stesse attività utilizzate localmente. Per ulteriori informazioni sulle attività di ciascuna applicazione Kaspersky Lab, consultare la documentazione corrispondente.

L'applicazione Kaspersky Administration Kit consente le seguenti attività:

- **Distribuzione del prodotto** (cfr. la sezione 4.6.2 a pag. **Error! Bookmark not defined.**)
- **Scaricamento degli aggiornamenti** (cfr. la sezione **Error! Reference source not found.** a pag. 62).
- **Modifica di Kaspersky Administration Server** (cfr. il **Error! Reference source not found.** a pag. **Error! Bookmark not defined.**)

Poiché queste attività vengono create e modificate in maniera diversa, questi aspetti saranno approfonditi in apposite sezioni di questo manuale.

È possibile creare attività di gruppo, globali o locali per ogni tipo di attività (cfr. la sezione 2.2 a pag. 14). L'attività di distribuzione delle applicazioni può essere assegnata a un gruppo (attività di gruppo) o a tutti i computer (attività globale). L'attività di scaricamento degli aggiornamenti può essere solo un'attività globale.

Le attività assegnate a un gruppo vengono salvate nella cartella **Attività** dei gruppi corrispondenti. Le attività globali si trovano nel nodo **Attività**, che rappresenta uno speciale archivio nella struttura ad albero della console. Per visualizzare l'elenco delle attività locali assegnate a un client, aprire la scheda **Attività** nella finestra di dialogo **Proprietà <Nome computer>** (cfr. la sezione **Error! Reference source not found.** a pag. **Error! Bookmark not defined.**)

La cronologia delle attività viene registrata e salvata in base alle impostazioni correnti. Essa può essere salvata a livello centrale (sul server amministrativo) o localmente, su ciascun computer client (cfr. la sezione **Error! Reference source not found.** a pag. **Error! Bookmark not defined.**). L'amministratore e altri utenti

possono ricevere comunicazione dei risultati delle prestazioni delle attività, in base alle impostazioni dell'attività corrente.

Per visualizzare i risultati delle prestazioni dell'attività per ciascun client, aprire la finestra di dialogo **Proprietà <Nome computer>** facendo clic sul pulsante **Cronologia** nella scheda **Attività** (vedere di seguito). In tal modo si visualizzano informazioni conservate nel server amministrativo:

Se la cronologia dell'attività è stata salvata localmente in una workstation, usare la console amministrativa installata su tale computer.

## 4.9. Gestione delle impostazioni delle applicazioni

Kaspersky Administration Kit consente di gestire le applicazioni installate sui client remoti della rete logica configurando le impostazioni dell'applicazione. È possibile modificare solo le impostazioni modificabili definite in base alla regola di gruppo per l'applicazione.

---

## 4.10. Aggiornamento del database antivirus e dei moduli del programma

Il regolare aggiornamento dei database antivirus, l'installazione dei moduli del programma aggiornati e l'aggiornamento delle versioni del programma sono fattori essenziali per il mantenimento di un'efficace protezione della rete contro qualsiasi minaccia.

Il database antivirus basato sul web di Kaspersky Lab viene aggiornato ogni tre ore. Si raccomanda di aggiornare il database antivirus con la massima frequenza e di installare con tempestività tutte le patch del programma.

Per aggiornare il database antivirus e i moduli del programma delle applicazioni gestite mediante Kaspersky Administration Kit, è necessario assegnare un'attività globale a Kaspersky Administration Kit che gli consenta di prelevare gli aggiornamenti. Kaspersky Administration Kit scaricherà quindi i database e i moduli aggiornati da un'apposita origine, in base alle impostazioni dell'attività globale (vedere di seguito). Gli aggiornamenti scaricati vengono salvati nel server amministrativo in una speciale cartella condivisa da cui verranno ridistribuiti tra i client della rete logica, a seconda dell'attività di aggiornamento programmata per l'applicazione. Per garantire una sicurezza costante, è necessario creare attività di aggiornamento per tutte le applicazioni antivirus incluse nel sistema di protezione della rete logica.

Per istruzioni sulle modalità di creazione di attività di aggiornamento, consultare i manuali d'uso delle singole applicazioni.

Grazie al sistema di gestione remoto, è possibile distribuire automaticamente gli aggiornamenti prelevati dal server amministrativo attraverso tutte le reti logiche. Si raccomanda di distribuire automaticamente gli aggiornamenti, poiché ciò contribuirà a ridurre il traffico Internet e il numero di interrogazioni inviate dai client al server. La distribuzione automatica degli aggiornamenti consente di evitare errori di configurazione delle attività di aggiornamento per un vasto numero di client.

## 4.11. Eventi, report e notifiche

Kaspersky Administration Kit è un potente strumento per il monitoraggio costante del sistema di protezione antivirus.

Esso consente di visualizzare tutti gli eventi che si verificano nel server amministrativo e nelle applicazioni gestite mediante Kaspersky Administration Kit.

Gli eventi possono essere registrati sia nel **Registro eventi Windows** sia nel registro eventi di Kaspersky Administration Kit. Se si registrano gli eventi nel Registro eventi Windows, visualizzare e gestire i registri degli eventi per mezzo dello strumento Windows standard **Event Viewer**. Per visualizzare gli eventi salvati nel registro eventi di Kaspersky Administration Kit, usare Administration Console (cfr. la sezione **Error! Reference source not found.** a pag. **Error! Bookmark not defined.**).

Tutti gli eventi verificatisi durante l'esecuzione dell'applicazione vengono registrati e salvati in base alle regole dell'applicazione (cfr. la sezione 4.7.1 a pag. 59) e alle impostazioni dell'attività (cfr. la sezione **Error! Reference source not found.** a pag. **Error! Bookmark not defined.**). L'amministratore e/o gli utenti possono essere avvisati in merito agli eventi registrati. Il metodo di notifica e le impostazioni dipendono anch'essi dalle regole e dalle impostazioni dell'applicazione.

È possibile visualizzare i report sullo status corrente della protezione antivirus in base alle informazioni salvate nel server amministrativo. I report possono essere creati per l'intero sistema di protezione antivirus, per i computer appartenenti allo stesso gruppo o per i computer di gruppi diversi. È possibile visualizzare i seguenti tipi di report:

- **Report dell'attività antivirus** – Contiene informazioni sui risultati della scansione antivirus di tutti i client della rete logica.
- **Report della protezione antivirus** – Visualizza informazioni sui client protetti in maniera inadeguata.
- **Report versione software** – Visualizza informazioni sulle versioni delle applicazioni Kaspersky Lab installate sui client.
- **Report versione database antivirus Kaspersky Lab** – Contiene informazioni sulle versioni del database antivirus usato dalle applicazioni KL.
- **Report degli errori** – Registra i dati sugli errori generati dalle applicazioni eseguite sui computer client.
- **Report dei desktop più infettati** – Registra i computer client sui quali è stato rilevato il maggior numero di oggetti sospetti e infetti.
- **Report licenza** – Visualizza informazioni sullo stato corrente delle chiavi di licenza utilizzate dalle applicazioni KL e sulla conformità delle licenze alle clausole del contratto di licenza (disponibile solo per l'intera rete logica).

Dai dati del registro eventi di Kaspersky Administration Kit salvati sul server amministrativo, il programma è in grado di generare report sullo stato corrente del sistema di protezione antivirus sulla base di modelli preimpostati. I modelli dei report sono conservati nel nodo **Report** nella struttura ad albero della console.

Esistono sette modelli standard, corrispondenti ad altrettanti tipi di report:

- Report dell'attività antivirus
- Report versione software
- Report versione database antivirus
- Report errori
- Report dei desktop più infettati
- Report licenza

## 4.12. Gestione delle chiavi di licenza

Il contratto di licenza sottoscritto dopo l'acquisto di un'applicazione Kaspersky Lab garantisce all'utente il diritto di utilizzare le applicazioni Kaspersky Anti-Virus per tutta la durata del periodo di licenza.

Durante tale periodo, l'utente può:

- Utilizzare le funzionalità antivirus dell'applicazione
- Aggiornare il database antivirus
- Aggiornare le versioni dell'applicazione
- Ricevere, telefonicamente o via e-mail, assistenza tecnica su aspetti riguardanti l'installazione, la configurazione e il funzionamento dell'applicazione antivirus
- Inviare oggetti infetti o sospetti a Kaspersky Lab per una analisi approfondita

Il programma installato verifica automaticamente il contratto di licenza e ne determina il periodo di validità tramite una chiave di licenza che è parte integrante di ogni applicazione Kaspersky Lab. Un'applicazione può avere una sola chiave di licenza valida. La chiave di licenza contiene le clausole per l'utilizzo del software che possono essere lette e verificate da componenti specifici del programma.

Allo scadere del periodo di licenza, l'utente non è più in grado di avvalersi delle opzioni sopra riportate. Per rinnovare la licenza, è necessario rinnovare ed installare una nuova chiave.

Kaspersky Administration Kit aiuta a monitorare a livello centrale la validità delle chiavi di licenza installate sui computer client connessi alla rete aziendale, e a rinnovarle quando necessario.

Quando una chiave di licenza viene installata tramite Kaspersky Administration Kit, le informazioni su tale chiave vengono registrate nel server amministrativo. Queste informazioni vengono utilizzate per creare report sullo stato della licenza, e informare l'amministratore sull'avvicinarsi della scadenza o sul superamento del numero massimo di utilizzi consentito.

È possibile configurare i parametri di notifica della chiave di licenza nella finestra di dialogo delle proprietà del server amministrativo (cfr. la sezione **Error! Reference source not found.** a pag. **Error! Bookmark not defined.**) nella cartella **Elaborazione eventi (Error! Reference source not found.)**. Nel nodo **Licenze** è riportata una lista completa delle chiavi di licenza installate sui computer client. Per ogni chiave sono disponibili le seguenti informazioni:

- **Numero di serie** – Numero di serie della chiave di licenza
- **Tipo** – Tipo di chiave di licenza (ad esempio, commerciale o di prova)
- **Limita conteggio computer** – Numero massimo di computer che possono utilizzare la chiave di licenza
- **Periodo licenza** – Periodo di validità della chiave di licenza

Per visualizzare informazioni sulle chiavi di licenza installate su client specifici per determinate applicazioni, aprire la scheda **Licenze** nella finestra di dialogo delle proprietà dell'applicazione (cfr. la sezione **Error! Reference source not found.** a pag. **Error! Bookmark not defined.**).

---

## 4.13. Copie di backup e ripristino dei dati dal server amministrativo

Si può eseguire il backup o il ripristino dei seguenti oggetti:

- database del server amministrativo, contenente regole, attività, impostazioni dell'applicazione ed eventi caricati sul server stesso;
- informazioni sulle reti logiche e sulle configurazioni dei client;
- file di installazione per l'installazione remota delle applicazioni (contenuto della cartella Pacchetti);
- certificato del server amministrativo.



Se il percorso della cartella condivisa è stato cambiato durante il ripristino dei dati, assicurarsi che le attività che ne fanno uso funzionino correttamente (attività di aggiornamento, di installazione remota) e, se necessario, configurare il percorso di conseguenza.

---

# APPENDICE A. DOMANDE FREQUENTI (FAQ)

Questo capitolo è dedicato alle domande più frequenti poste dai nostri utenti sull'installazione, la configurazione e il funzionamento di Kaspersky Anti-Virus; faremo il possibile per fornire risposte più esaurienti possibile.



***Domanda:** È possibile usare Kaspersky Anti-Virus con altri programmi antivirus?*

Per evitare conflitti si raccomanda di disinstallare eventuali altri programmi antivirus presenti nel computer prima di installare Kaspersky Anti-Virus.



***Perché Kaspersky Anti-Virus rallenta le prestazioni del server e impone un carico notevole sulla CPU?***

La ricerca dei virus è un problema matematico che comporta un'intensa attività computazionale e richiede l'analisi delle strutture, il calcolo delle "checksum" e la trasformazione dei dati matematici. Per questo motivo la velocità del processore è la principale risorsa consumata da un software antivirus, e ogni nuovo virus aggiunto al database antivirus aumenta la durata complessiva della scansione. Si tratta di un compromesso necessario per la sicurezza dei dati custoditi nel computer.

A differenza di altri produttori di software antivirus che accelerano il processo di scansione escludendo dai propri database i virus più difficilmente rilevabili o meno frequenti nella regione geografica del rivenditore del prodotto, oltre ai formati di file che richiedono complesse analisi (per esempio file PDF),

Kaspersky Lab ritiene che la funzione di un programma antivirus consista nel garantire ai propri utenti una sicurezza completa ed efficace. Noi riteniamo che una "protezione parziale" sia perfino peggiore di una protezione assente che almeno obbliga l'utente ad adottare delle precauzioni.

Kaspersky Anti-Virus offre ai propri utenti il massimo della protezione. Gli utenti più esperti hanno la possibilità di accelerare il processo di scansione antivirus a discapito della sicurezza globale disattivando l'analisi di determinati tipi di file, ma questo tipo di operazione è sconsigliato a chi desidera la massima sicurezza.

Al fine di garantire la massima protezione, Kaspersky Anti-Virus riconosce oltre 700 formati di archivi e file compressi. Ciò è essenziale in quanto i codici eseguibili dannosi possono annidarsi all'interno di file di qualsiasi

formato riconosciuto. Tuttavia, a dispetto dell'incremento quotidiano del numero di virus rilevati da Kaspersky Anti-Virus (circa 30 nuovi virus ogni giorno) e del numero crescente di formati file riconosciuti, ogni nuova versione del prodotto funziona a una velocità superiore rispetto alle precedenti. Ciò è reso possibile dall'uso di nuove tecnologie esclusive come iChecker™ e i-Stream™, sviluppate da Kaspersky Lab. Grazie a queste tecnologie, un file viene esaminato una sola volta, durante la prima scansione antivirus. Le volte successive viene esaminato solo se nel frattempo ha subito delle modifiche. In tal modo, le prestazioni del programma antivirus migliorano in maniera considerevole dopo la prima scansione.



*Domanda: Perché mi occorre un file chiave? La mia copia dell'applicazione antivirus funziona senza?*

No, senza chiave di licenza Kaspersky Anti-Virus non funziona.

Se non si è ancora deciso se acquistare Kaspersky Anti-Virus oppure no, possiamo fornire una chiave temporanea (chiave di prova) funzionante per due settimane o un mese. Al termine di quel periodo la chiave viene bloccata.



*Domanda: La mia applicazione antivirus non funziona.*

*Cosa devo fare?*

Innanzitutto, controllare se il nostro sito web o questo manuale forniscono una soluzione al problema, soprattutto in questa sezione.

Inoltre consigliamo di richiedere assistenza al rivenditore presso cui si era acquistato Kaspersky Anti-Virus o di scrivere al nostro servizio di assistenza tecnica ([support@kaspersky.com](mailto:support@kaspersky.com) o all'indirizzo indicato nelle informazioni sulla chiave di licenza).

Per avere la garanzia di una risposta nel più breve tempo possibile, si consiglia di seguire questi suggerimenti:

- Nell'intestazione del messaggio indicare il sistema operativo del server e il nome del componente che dà problemi, e descrivere brevemente il problema. Ad esempio: MS Windows 2000, Kaspersky Anti-Virus 5.0 for Windows Workstations, l'aggiornamento del database antivirus non funziona.
- Comporre i messaggi in formato testo semplice.
- All'inizio del messaggio indicare la versione esatta del sistema operativo e del pacchetto di distribuzione di Kaspersky Anti-Virus, nonché il nome del file della chiave di licenza.

- Descrivere il problema in maniera chiara e concisa. Ricordare che, quando leggono il messaggio, i tecnici dell'assistenza non conoscono ancora il problema. Saranno in grado di fornire una soluzione solo dopo aver compreso a fondo e riprodotto il problema.
- Inviare i seguenti dati al servizio di assistenza tecnica (comprimerli in un archivio prima di inviarli):
  - File log antivirus;
  - Chiave di licenza
- Ricordarsi di specificare nel messaggio se il sistema è dotato di:
  - Controller SCSI;
  - Processore particolarmente vecchio o particolarmente nuovo, o processori multipli;
  - Meno di 64 MB o più di 2 GB di RAM.
- Quantificare approssimativamente il traffico giornaliero e specificare se vi sono picchi di traffico.



***Domanda:** Uso un server proxy e l'applicazione di aggiornamento non funziona sul mio computer. Cosa devo fare?*

I seguenti problemi possono provocare l'incapacità di prelevare gli aggiornamenti in caso di uso di un server proxy:

- Impostazioni di rete errate.

Esistono due opzioni per la configurazione delle impostazioni di rete durante la configurazione del servizio di aggiornamento: si possono utilizzare le impostazioni di MS Internet Explorer o impostazioni personalizzate. Il servizio di aggiornamento a volte utilizza erroneamente le impostazioni di MS Internet Explorer. Ciò può verificarsi nei seguenti casi:

  - La connessione Internet non è configurata;
  - Le impostazioni di MS Internet Explorer non sono disponibili se nessuno degli utenti è collegato;
  - Il server proxy richiede l'autorizzazione.

In tutti questi casi è necessario specificare i parametri di rete direttamente tra le impostazioni del servizio di aggiornamento.
- Il server proxy utilizzato appartiene a un tipo non supportato dal servizio di aggiornamento di Kaspersky Anti-Virus.

Il servizio di aggiornamento non funziona attraverso Kerio WinRoute, poiché WinRoute non supporta completamente il protocollo HTTP 1.0. In questo caso si raccomanda di utilizzare qualsiasi altro server proxy.

Il servizio di aggiornamento non funziona neanche attraverso Microsoft ISA Server con protocollo FTP. In questo caso si raccomanda di procurarsi gli aggiornamenti dai server di Kaspersky Lab tramite protocollo HTTP.

---

## APPENDICE B. GLOSSARIO

Il presente manuale contiene alcuni termini specifici relativi alla protezione antivirus. Il glossario è un elenco delle definizioni di tali termini. Al fine di agevolare la consultazione del glossario, le voci sono organizzate in ordine alfabetico.

### A

**Administration Console** – Un componente di Kaspersky Administration Kit che fornisce l'interfaccia utente per i servizi amministrativi di Administration Server e Network Agent.

**Administration Server** – Un componente di Kaspersky Administration Kit che salva a livello centrale le informazioni relative alle applicazioni Kaspersky Lab installate sui client e gestisce tali applicazioni.

**Aggiornamenti disponibili** – Service Pack contenente gli aggiornamenti urgenti accumulati in un determinato periodo di tempo e le più recenti modifiche alla struttura dell'applicazione.

**Aggiornamento** – Una funzione di Kaspersky Anti-Virus che consente di aggiornare/aggiungere nuovi file (database antivirus o moduli dell'applicazione) scaricati dai server di aggiornamento di Kaspersky Lab.

**Amministratore della rete locale** – Un utente che installa, configura e mantiene Kaspersky Administration Kit, e opera la gestione remota delle applicazioni Kaspersky Lab installate sui computer della rete logica.

**Archiviazione di backup** – Una cartella contenente le copie di backup dei dati di Administration Server creati dall'utilità di backup.

**Attività** – Un'azione cui è stato assegnato un nome, svolta da un'applicazione Kaspersky Lab.

**Attività di gruppo** – Un'attività definita per tutti i client appartenenti a un gruppo e operativa su di essi.

**Attività globale** – Un'attività definita per un certo numero di client appartenenti a gruppi amministrativi distinti e operativa su di essi.

**Attività locale** – Un'attività definita per un unico client e operativa su di esso.

### B

**Backup** – La creazione di copie di sicurezza di un file nella cartella BACKUP prima di trattarlo (riparazione o eliminazione). Il file di backup potrà essere successivamente ripristinato, per esempio per un'ulteriore scansione con una versione più aggiornata del database antivirus.

**Blocco di oggetti** – Funzione che impedisce alle applicazioni esterne di accedere a un oggetto. L'oggetto bloccato è protetto dalla lettura, esecuzione, modifica o eliminazione.

## C

**Cartella BACKUP** – Una directory contenente copie di backup di oggetti eliminati o riparati.

**Certificato di Administration Server** – Un certificato utilizzato per autenticare il server amministrativo alla connessione di Administration Console e la trasmissione dei dati tra server e client. Esso viene creato durante l'installazione di Administration Server e salvato nella cartella **Cert** all'interno della cartella di installazione.

**Chiave di licenza** – Un file con estensione *.key* che svolge la funzione di "chiave" personale, necessario per il corretto funzionamento delle applicazioni Kaspersky Lab. La chiave di licenza è inclusa nel kit di distribuzione se il prodotto è stato acquistato presso un rivenditore Kaspersky Lab. Se il prodotto è stato acquistato online, la chiave di licenza viene inviata per posta elettronica. Senza di essa, Kaspersky Anti-Virus NON FUNZIONA.

**Client, server amministrativo (o computer client)** – Un computer, server o workstation con Network Agent e applicazioni Kaspersky Lab gestite.

## D

**Database antivirus** – Un database creato dagli specialisti di Kaspersky Lab, contenente le definizioni dettagliate di tutti i virus esistenti noti e dei relativi metodi di intercettazione e riparazione. Le applicazioni antivirus utilizzano il database per individuare ed eliminare con efficacia i virus. Il database antivirus disponibile sui siti web di Kaspersky Lab viene aggiornato regolarmente man mano che compaiono nuove minacce. Gli utenti registrati delle applicazioni Kaspersky Lab possono accedere agli aggiornamenti del database. Per garantire una costante protezione antivirus del computer, si raccomanda di scaricare regolarmente gli aggiornamenti.

**Database di posta elettronica** – Database contenente i messaggi di posta elettronica memorizzati nel computer. Ogni messaggio in arrivo o in uscita viene salvato nel database subito dopo la ricezione o l'invio. La scansione del database viene eseguita in modalità manuale.

**Disinfezione** – Metodo di trattamento di un oggetto infetto. La riparazione può permettere il recupero parziale o totale dei dati, o portare alla conclusione che il file in esame non può essere riparato. Gli oggetti vengono riparati per mezzo del database antivirus. Se la riparazione è la prima opzione applicata a un oggetto, cioè la prima azione eseguita dopo l'intercettazione di un oggetto infetto, il programma ne crea una copia di backup. Qualora alcuni dati vadano perduti durante la riparazione, il backup può essere utilizzato per il loro recupero.

**E**

**Eliminazione di un oggetto** – Un metodo di gestione di un oggetto che consiste nella sua rimozione fisica da un computer. È il metodo raccomandato per il trattamento degli oggetti infetti. Se l'eliminazione è la prima opzione applicata a un oggetto, è necessario crearne una copia di backup prima di procedere. Il backup consente l'eventuale ripristino dell'oggetto eliminato.

**Esclusioni** – Impostazioni definite dall'utente volte ad escludere determinati oggetti dalla scansione. È possibile personalizzare le regole di esclusione dalla *scansione in tempo reale* e dalla *scansione manuale*, per esempio disabilitando la scansione di archivi durante una scansione completa o escludendo dei file dalla scansione per mezzo di maschere.

**G**

**Gestione centrale di un'applicazione** – Gestione di un'applicazione tramite Kaspersky Administration Kit.

**Gestione locale** – La gestione di un'applicazione attraverso un'interfaccia locale.

**Gruppo amministrativo** – Computer raggruppati in base alle rispettive funzioni e applicazioni Kaspersky Lab installate. Il raggruppamento agevola considerevolmente il processo di gestione e consente all'amministratore di gestire tutti i computer come un'unica entità. Un gruppo può contenere a sua volta altri gruppi. Per ogni applicazione installata sui computer del gruppo possono essere create regole e attività di gruppo.

**I**

**Impostazioni, applicazioni** – Impostazioni di applicazioni specifiche per tutti i tipi di attività eseguite dall'applicazione.

**Impostazioni, attività** – Impostazioni di applicazioni specifiche per ogni tipo di attività.

**Installazione "push"** – Un metodo di installazione remota che consente di installare il software Kaspersky Lab su computer specifici della rete logica. Per forzare l'installazione di un'applicazione, il server amministrativo deve disporre dei diritti di avviare applicazioni su client remoti. Questo metodo è raccomandato per computer con MS Windows NT/2000/2003/XP che supportano questa funzionalità, o per computer con MS Windows 98/Me su cui è installato Network Agent.

**Installazione basata su script** – Un metodo di installazione che associa l'attività di installazione remota a un account utente specifico (più account). Quando l'utente specificato accede al dominio, l'applicazione viene installata sul client dell'utente. Questo metodo è raccomandato in caso di computer con MS Windows 95/98/Me

**Installazione remota** – Installazione delle applicazioni Kaspersky Lab per mezzo dei servizi forniti da Kaspersky Administration Kit.

**Isolamento** – Metodo di trattamento di un *oggetto sospetto*. L'accesso a tale oggetto viene bloccato e il file trasferito nella cartella della quarantena per essere elaborato in seguito.

## K

**Kaspersky Administration Kit** – Un'applicazione creata per centralizzare le prestazioni delle più importanti attività amministrative, che offre il controllo completo del sistema di protezione antivirus dell'azienda basato sulle applicazioni Kaspersky Lab.

## L

**Livello di gravità** – Un parametro che classifica un evento registrato durante il funzionamento di Kaspersky Anti-Virus. Esistono quattro livelli di gravità:

- **Critico**
- **Errore**
- **Avviso**
- **Info**

Eventi dello stesso tipo possono avere stati di gravità diversi a seconda della situazione specifica.

**Livello raccomandato** – Il livello di protezione antivirus basato sulle impostazioni predefinite raccomandate dagli esperti di Kaspersky Lab, che garantisce la sicurezza ottimale del computer. È il livello predefinito.

## M

**Massima velocità** – Il livello di protezione che garantisce la massima velocità del sistema ma offrendo una minore sicurezza.

## N

**Network Agent** – Un componente di Kaspersky Administration Kit che fornisce la comunicazione tra Administration Server e le applicazioni Kaspersky Lab installate su nodi specifici della rete (workstation o server). Questo componente è comune a tutte le applicazioni di Kaspersky Anti-Virus Business Optimal e Corporate Suite.

## O

**Oggetti d'avvio** – un insieme di programmi necessari per l'esecuzione e il corretto funzionamento del sistema operativo e di altri programmi installati nel computer. Il sistema operativo li esegue ad ogni avvio. Alcuni virus cercano di infettarli e possono provocare un errore di avvio.

**Oggetto infetto** – Un oggetto contenente un virus. Si raccomanda di interrompere qualsiasi attività su questi oggetti poiché possono infettare il computer.

**Oggetto OLE** – Un oggetto collegato ad altri file o incorporati in essi mediante la tecnologia OLE.

**Oggetto sospetto** – un oggetto contenente una variante del codice di un virus noto o un codice somigliante a quello di un virus ma attualmente ignoto agli specialisti di Kaspersky Lab.

**Operatore della rete logica** – Un utente che monitorizza il sistema di protezione antivirus gestito attraverso Kaspersky Administration Kit.

## P

**Pacchetto di installazione** – Un pacchetto di file utilizzati per installare le applicazioni Kaspersky Lab su host remoti di una rete logica. I pacchetti di installazione si basano su uno speciale file **.kpd** incluso nel kit di distribuzione dell'applicazione, contenente un numero minimo di parametri che garantiscono le funzionalità di base dell'applicazione subito dopo l'installazione. I valori dei parametri sono impostazioni predefinite delle applicazioni.

**Periodo di validità della licenza** – Il periodo nel quale l'utente ha il diritto di fruire delle funzionalità complete di Kaspersky Anti-Virus. Di norma, il periodo di validità della licenza definito dall'apposita chiave è di un anno dalla data dell'acquisto. Dopo la scadenza della licenza, il prodotto conserva la funzionalità ma non consente di usufruire del servizio di *aggiornamento del database antivirus*.

**Plug-in Console (gestione)** – Uno speciale componente che fornisce un'interfaccia per la gestione remota di un'applicazione attraverso Administration Console. I plug-in sono specifici di ogni applicazione e sono presenti in tutte le applicazioni Kaspersky Lab che possono essere gestite tramite Kaspersky Administration Kit.

**Protezione in tempo reale** – Una modalità di scansione basata su un'applicazione antivirus residente in memoria. In modalità di protezione in tempo reale, l'applicazione effettua la scansione antivirus di ogni oggetto aperto a fini di lettura, scrittura o esecuzione. Prima di abilitare l'accesso all'oggetto, Kaspersky Antivirus ne esegue la scansione. In caso di virus, blocca l'accesso all'oggetto, lo ripara o lo elimina (a seconda delle impostazioni scelte dall'utente).

**Protezione massima** – Il livello di protezione che garantisce la massima sicurezza del computer, riducendo leggermente le caratteristiche prestazionali del sistema.

## Q

**Quarantena** – Una speciale area di archiviazione in cui isolare oggetti infetti e sospetti.

## R

**Regola** – vedi **Regola di gruppo**

**Regola di gruppo** – Una serie di impostazioni di applicazioni in un gruppo amministrativo gestito tramite Kaspersky Administration Kit. Le regole di

gruppo possono essere diverse per ogni gruppo. Esse sono specifiche per ogni applicazione. Le regole comportano la configurazione di tutti i parametri delle applicazioni.

**Ripristino** – Ripristino dei dati di Administration Server per mezzo di un'utilità di backup. Le informazioni sul ripristino sono disponibili nell'archiviazione di backup. L'utilità consente di ripristinare:

- Certificato Administration Server
- Database di Administration Server dove sono conservate regole, impostazioni delle applicazioni ed eventi registrati nel server amministrativo
- File di installazione per l'installazione remota delle applicazioni (contenuto della cartella Pacchetti)
- Informazioni sulle configurazioni della rete logica e dei client

## S

**Scansione dei file per estensione** – Modalità di scansione in cui il programma considera l'estensione dei file.

**Scansione dei file per formato** – Modalità di scansione in cui il programma analizza i contenuti di un file, per la precisione l'identificatore di formato nell'intestazione del file.

**Scansione manuale completa** – Una modalità definita dall'amministratore che esamina tutti i file del computer e ripara/elimina gli oggetti infetti rilevati.

**Server di aggiornamento Kaspersky Lab** – Un elenco di siti web http e ftp di Kaspersky Lab da cui è possibile scaricare gli aggiornamenti sul proprio computer.

**Soglia di attività dei virus** – Numero di virus rilevati in un intervallo di tempo specificato. Quando tale limite viene superato, la situazione viene considerata **Attacco di virus**. Si tratta di un parametro importante per la definizione delle epidemie di virus perché consente all'amministratore di rispondere tempestivamente alle nuove minacce e adottare misure preventive per la protezione della rete.

---

**Status della protezione antivirus** – Lo status corrente della protezione antivirus che definisce il livello di sicurezza del computer.

**T**

**Tecnologia IChecker** – Una tecnologia ideata per escludere dalle scansioni successive i file salvati su dischi formattati NTFS se non hanno subito variazioni rispetto alla scansione precedente. La tecnologia IStreams è stata implementata utilizzando un metodo di archiviazione delle checksum dei file nei flussi NTFS supplementari.

**Tecnologia IChecker** – Una tecnologia ideata per escludere gli oggetti dalle scansioni successive se non hanno subito variazioni rispetto alla scansione precedente. La tecnologia IChecker è stata implementata utilizzando il database delle checksum degli oggetti.

**U**

**Unità virtuali (RAM drive)** – Area della RAM di un personal computer che emula un disco fisico regolare.

**V**

**Virus ignoto** – un nuovo virus non ancora registrato nel *database antivirus*. Di regola, Kaspersky Anti-Virus rileva i virus ignoti per mezzo dell'*analizzatore euristico di codici* e indica come *sospetti* gli oggetti che li contengono.

**W**

**Workstation dell'amministratore** – Un computer su cui è installato il componente Administration Console di Kaspersky Administration Kit. La console consente all'amministratore di realizzare e gestire un sistema di protezione antivirus mediante le applicazioni Kaspersky Lab.

---

## APPENDICE C. KASPERSKY LAB

Fondata nel 1997, Kaspersky Lab è diventata un leader indiscusso nel settore delle tecnologie per la sicurezza informatica. Produce una vasta gamma di applicazioni per la sicurezza dei dati e offre soluzioni complete di alto livello per garantire la sicurezza di computer e reti contro ogni tipo di programma dannoso, messaggi di posta elettronica non sollecitati e indesiderati e attacchi di pirateria informatica.

Kaspersky Lab è un'azienda internazionale con sede nella Federazione Russia e rappresentanti nel Regno Unito, 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 vari membri della 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 consente all'azienda di offrire una protezione completa contro 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 ne hanno fatto un'azienda leader tra i 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 della protezione antivirus. Il prodotto di punta dell'azienda, Kaspersky Anti-Virus, offre una protezione completa a tutti i livelli di una rete, inclusi workstation, server di file, sistemi di posta elettronica, firewall e gateway di Internet e computer portatili. I suoi strumenti di gestione, pratici e di facile utilizzo, garantiscono l'automazione avanzata per una sollecita protezione antivirus ad ogni livello dell'impresa. Numerose imprese di grande notorietà si affidano a Kaspersky Anti-Virus, per esempio Nokia ICG (USA), F-Secure (Finlandia), Aladdin (Israele), Sybari (USA), G Data (Germania), Deerfield (USA), Alt-N (USA), Microworld (India) e BorderWare (Canada).

Gli utenti Kaspersky Lab possono usufruire di una vasta serie di servizi supplementari volti a garantire sia un funzionamento stabile dei prodotti dell'azienda, sia 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.

## C.1. Altri prodotti Kaspersky Lab

### Kaspersky Anti-Virus® 6.0

Kaspersky Anti-Virus 6.0 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, directory 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:

- **Controllo delle modifiche del 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.
- **Monitoraggio dei processi nella RAM.** Kaspersky Anti-Virus 6.0 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 standard.
- **Monitoraggio delle variazioni del registro del SO** dovute al controllo del registro interno del sistema.
- **Blocco di macro VBA pericolose** nei documenti di Microsoft Office.
- **Ripristino del sistema** in seguito ai danni provocati da spyware nocivo a causa della registrazione di tutte le variazioni del registro e del file system del computer, e un'opportunità di eseguire il roll-back a discrezione dell'utente.

## **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 news disponibili e il loro contenuto dai server di notizie di Kaspersky Lab con la frequenza specificata.

Il programma esegue le seguenti funzioni:

- Visualizza nella barra delle applicazioni lo status corrente dell'attività dei virus.
- Il prodotto consente di iscriversi e cancellarsi dai canali news.
- Recupera le notizie da ogni canale a cui è iscritto con la frequenza specificata e informa sulle ultime notizie.
- Consente di consultare le notizie sui canali a cui è iscritto.
- Consente di consultare l'elenco dei canali e il loro status.
- Consente di aprire nel browser pagine con particolari di notizie.

News Agent è un'applicazione Microsoft Windows stand-alone che può essere utilizzata da sola o con varie 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 funziona direttamente dal browser web avvalendosi della tecnologia Microsoft ActiveX®. Gli utenti hanno così la possibilità di esaminare il computer in caso di sospetto di infezione virale. Con questo servizio, è possibile:

- Escludere dalla scansione archivi e database di posta.
- Selezionare per la scansione database antivirus standard/estesi.
- Salvare un report dei risultati di 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 riparare i file pericolosi. Kaspersky OnLine Scanner Pro funziona direttamente dal browser web avvalendosi della tecnologia Microsoft ActiveX®. Grazie a questo servizio, è possibile:

- Escludere dalla scansione archivi e database di posta.
- Selezionare per la scansione database antivirus standard/estesi.

- Salvare un report dei risultati di scansione in formato txt o html.

### **Kaspersky® Security for PDA**

Kaspersky® Security for PDA offre un'affidabile protezione antivirus dei dati salvati su vari tipi di computer palmari e smartphone. Il programma contiene una serie ottimale di strumenti di protezione antivirus:

- **anti-virus scanner** per esaminare le informazioni (salvate sia nella memoria interna del PDA o smartphone oppure in schede di memoria di qualsiasi tipo) su richiesta;
- **un monitor antivirus** che intercetta i virus durante il trasferimento di dati con l'utility HotSync™ o prelevati da dispositivi portatili.

Esso offre l'accesso criptato al dispositivo e codifica tutti i dati memorizzati nel dispositivo e nelle schede di memoria.

### **Kaspersky Anti-Virus® Business Optimal**

Il pacchetto offre una protezione completa esclusiva e configurabile dei dati per reti aziendali di piccole e medie dimensioni.

Kaspersky Anti-Virus® Business Optimal garantisce la protezione antivirus completa<sup>3</sup> per:

- *Workstation* con Microsoft Windows 98/ME, Microsoft Windows NT/2000/XP Workstation e Linux;
- *File server* con Microsoft Windows NT 4.0 Server, Microsoft Windows 2000/2003 Server/Advanced Server, Microsoft Windows 2003 Server, Novell NetWare, FreeBSD e OpenBSD, Linux e Samba Servers;
- *Client di posta*, tra cui Microsoft Exchange 2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail e Qmail;
- *Gateway di Internet*: CheckPoint Firewall –1; Microsoft ISA Server 2000 Standard Edition.

Il kit di distribuzione di Kaspersky Anti-Virus® Business Optimal comprende Kaspersky® Administration Kit, uno *strumento esclusivo per la gestione e l'amministrazione automatizzate*.

La vasta gamma di applicazioni antivirus disponibili offre la massima libertà di scelta in base al sistema operativo e alle applicazioni in uso.

---

<sup>3</sup> In base al tipo di kit di distribuzione.

## Kaspersky® Corporate Suite

Questo pacchetto è stato sviluppato al fine di offrire una protezione totale dei dati di reti aziendali di qualsiasi dimensione e complessità. I componenti del pacchetto garantiscono la protezione di tutti i nodi di una rete aziendale, anche in ambienti informatici misti. Kaspersky® Corporate Suite supporta la maggior parte dei sistemi operativi e delle applicazioni in uso nelle aziende. Tutti i componenti del pacchetto sono gestiti da una console mediante un'unica interfaccia utente. Kaspersky® Corporate Suite è un affidabile sistema di protezione di alto livello totalmente compatibile con le esigenze specifiche di ogni configurazione di rete.

Kaspersky® Corporate Suite include la protezione antivirus completa per:

- *Workstation* con Microsoft Windows 98/ME, Microsoft Windows NT/2000/XP Workstation e Linux;
- File server con Microsoft Windows NT 4.0 Server, Microsoft Windows 2000, 2003 Server/Advanced Server, Novell NetWare, FreeBSD, OpenBSD, Linux e Samba Servers;
- *Client di posta*, inclusi Microsoft Exchange Server 2000/2003, Lotus Notes/Domino, Sendmail, Postfix, Exim e Qmail;
- *Gateway di Internet*: CheckPoint Firewall –1; Microsoft ISA Server 2004 Enterprise Edition;
- *Computer palmari* (PDA) con Microsoft Windows CE e Palm OS, oltre a smartphone con Microsoft Windows Mobile 2003 for Smartphone e Microsoft Smartphone 2002.

Il kit di distribuzione di Kaspersky® Corporate Suite comprende Kaspersky® Administration Kit, uno *strumento esclusivo per la gestione e l'amministrazione automatizzate*.

La vasta gamma di applicazioni antivirus disponibili offre la massima libertà di scelta in base al sistema operativo e alle applicazioni in uso.

## 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 una tecnologia all'avanguardia in cui il programma analizza dal punto di vista linguistico il testo dei messaggi, i moderni metodi di filtraggio della posta elettronica (incluse le liste nere DNS e le caratteristiche della posta formale) e una raccolta esclusiva di servizi che consentono agli utenti di individuare ed eliminare fino al 95% del traffico indesiderato.

Installato all'ingresso di una rete, Kaspersky® Anti-Spam funziona come filtro 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 consentito dall'aggiornamento quotidiano del database di filtraggio dei contenuti con i campioni forniti dagli specialisti del laboratorio linguistico. I database vengono aggiornati ogni 20 minuti.

### **Kaspersky® SMTP Gateway**

Kaspersky® SMTP-Gateway for Linux/Unix è una soluzione studiata per la scansione antivirus della posta trasmessa mediante SMTP. L'applicazione contiene una serie di strumenti supplementari per il filtraggio del traffico e-mail per nome e per tipo di allegati MIME, oltre a una serie di strumenti volti a ridurre il carico sul sistema di posta e a prevenire gli attacchi informatici. La DNS Black List protegge dai messaggi di posta elettronica provenienti da server noti come origine di spam.

### **Kaspersky Security® for Microsoft Exchange 2003**

Kaspersky Security for Microsoft Exchange esegue la scansione antivirus di messaggi inviati e ricevuti e di messaggi conservati sul server, compresi quelli conservati in cartelle pubbliche, e blocca la corrispondenza non desiderata per mezzo di tecnologie antispam "intelligenti" in combinazione con tecnologie Microsoft. L'applicazione esamina tutti i messaggi in arrivo su un Exchange Server attraverso il protocollo SMTP, controllando che non contengano virus per mezzo delle tecnologie antivirus Kaspersky Lab, e che non vi siano attributi di SPAM. L'applicazione blocca lo spam sulla base di attributi formali (indirizzo di posta, indirizzo IP, formato della lettera, intestazione) e analizza i contenuti dei messaggi e dei loro allegati per mezzo di tecnologie intelligenti, comprese esclusive firme grafiche per l'individuazione dello spam grafico. L'applicazione esamina sia il corpo del messaggio sia i file allegati.

### **Kaspersky® Mail Gateway**

Kaspersky Mail Gateway è una soluzione completa per la protezione antivirus degli utenti dei sistemi di posta. Questa applicazione, installata tra la rete aziendale e Internet, esamina tutti i componenti dei messaggi e-mail per escludere la presenza di virus e altro malware (Spyware, Adware, ecc.) ed esegue il filtraggio antispam centralizzato del flusso dei messaggi. Questa soluzione offre anche alcune funzioni supplementari di filtraggio del traffico di posta.

## C.2. Recapiti

Per qualsiasi domanda, commento o suggerimento, l'utente può rivolgersi ai distributori o direttamente a Kaspersky Lab, che sarà lieta di offrire assistenza per qualsiasi problematica relativa ai suoi prodotti, sia per telefono che per e-mail. 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> Helpdesk: <a href="http://www.kaspersky.com/helpdesk.html">http://www.kaspersky.com/helpdesk.html</a>
Informazioni generali	WWW: <a href="http://www.kaspersky.com">http://www.kaspersky.com</a> <a href="http://www.viruslist.com">http://www.viruslist.com</a> Messaggio: <a href="mailto:info@kaspersky.com">info@kaspersky.com</a>

---

# APPENDICE D. CONTRATTO DI LICENZA

Contratto di licenza standard con 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 INTERNET SECURITY ("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.

AI SENSI DELLA LEGISLAZIONE VIGENTE, PER QUANTO RIGUARDA IL SOFTWARE KASPERSKY PREVISTO PER SINGOLI UTENTI, ACQUISTATO ONLINE DAL SITO WEB DI KASPERSKY LAB O DEI SUOI PARTNER, IL CLIENTE HA QUATTORDICI (14) GIORNI LAVORATIVI DI TEMPO DALLA CONSEGNA DEL PRODOTTO PER RESTITUIRLO AL RIVENDITORE A FINI DI SOSTITUZIONE O DI RIMBORSO, A CONDIZIONE CHE IL SOFTWARE NON SIA STATO DISSIGILLATO.

PER QUANTO RIGUARDA IL SOFTWARE KASPERSKY PREVISTO PER SINGOLI UTENTI NON ACQUISTATO ONLINE VIA INTERNET, QUESTO SOFTWARE NON POTRÀ ESSERE RESTITUITO NÉ SOSTITUITO, ECCEZION FATTA PER LE CLAUSOLE CONTRARIE DEL PARTNER CHE VENDE IL PRODOTTO. IN QUESTO CASO, KASPERSKY LAB NON SARÀ RITENUTO RESPONSABILE DELLE CLAUSOLE DEL PARTNER.

IL DIRITTO ALLA RESTITUZIONE E AL RIMBORSO SI RIFERISCE SOLO ALL'ACQUIRENTE ORIGINARIO.

Qualsiasi riferimento al "Software" nel presente documento sarà da intendersi comprensivo di codice di attivazione fornito da Kaspersky Lab come parte integrante di Kaspersky Internet Security 6.0.

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. È possibile installare una copia del Software su un computer.

1.1 *Uso.* Il Software è concesso in licenza in qualità di singolo prodotto; non può essere utilizzato su più di un computer o da più di un utente per volta, salvo diversamente specificato nella presente Sezione.

1.1.1 Il Software è "in uso" su un computer quando è caricato nella memoria temporanea (per esempio random access memory o RAM) oppure installato nella memoria permanente (per esempio disco fisso, CD-ROM o altro dispositivo di memorizzazione) 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 archivio, 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 Qualora l'utente metta in vendita il computer su cui è installato il Software, egli dovrà accertarsi che tutte le copie del Software siano state precedentemente cancellate.

1.1.3 È fatto divieto all'utente di decompilare, decodificare, disassemblare o altrimenti ridurre qualsiasi parte di questo Software in forma leggibile o consentire a terzi di farlo. 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.

1.1.4 L'utente non deve né deve permettere ad altri (in modo diverso da quanto espressamente permesso nel presente) di effettuare la correzione di errori o altrimenti modificare, adattare o tradurre il Software né creare opere derivate dal Software.

1.1.5 È fatto divieto all'utente di concedere in locazione, in leasing o in prestito a terzi il Software o trasferire o cedere in sublicenza a terzi i diritti a lui conferiti dalla licenza.

1.1.6 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.

## 2. Assistenza.

(i) Kaspersky Lab metterà a disposizione dell'utente i servizi di assistenza ("Servizi di assistenza") specificati di seguito, per la durata di un anno dal momento dell'attivazione, previo:

- (a) pagamento della tariffa di assistenza corrente; e
- (b) compilazione del Modulo di richiesta dei Servizi di assistenza fornito in allegato al presente Contratto o disponibile nel sito web di Kaspersky Lab, nel quale si richiede all'utente di fornire il proprio codice di attivazione fornito all'utente da Kaspersky Lab con il presente Contratto. Kaspersky Lab ha il diritto di stabilire, a propria discrezione, se l'utente abbia soddisfatto o meno questa condizione per la fornitura dei Servizi di Assistenza.

Il servizio di assistenza diventerà disponibile in seguito all'attivazione del Software. Il servizio di assistenza tecnica di Kaspersky Lab ha facoltà di richiedere all'utente finale un'ulteriore registrazione per poter usufruire dei servizi di assistenza.

Fino all'attivazione del Software e/o all'ottenimento dell'identificativo dell'utente finale (ID cliente) il servizio di assistenza tecnica offre 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 e 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 intendono

- (a) Aggiornamento del database antivirus ogni ora
- (b) Aggiornamenti del database degli attacchi di rete
- (c) Aggiornamenti del database antispyware

- (d) Aggiornamenti gratuiti del software, inclusi gli aggiornamenti della versione;
- (e) Assistenza tecnica via Internet e numero verde fornita dal distributore e/o dal rivenditore;
- (f) Aggiornamenti per il rilevamento e l'eliminazione di virus entro 24 ore.

(v) I servizi di assistenza sono forniti solo se e quando l'utente dispone della versione del Software più recente disponibile sul sito web ufficiale Kaspersky Lab ([www.kaspersky.com](http://www.kaspersky.com)) installata sul computer.

**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 [6] mesi a decorrere dal primo caricamento o installazione il Software acquistato su supporto fisico opererà sostanzialmente in conformità alle funzioni descritte nella Documentazione, a condizione che sia utilizzato in modo corretto e nella maniera specificata nella Documentazione.

(ii) L'utente si assume ogni responsabilità relativamente al fatto che il presente Software soddisfi i propri requisiti. 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 noti né esclude che possa occasionalmente eseguire il report erroneo di un virus in un titolo non infettato da quel virus.

(iv) 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.

(v) 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.

(vi) Le garanzie e le condizioni stabilite dal presente Contratto sostituiscono eventuali altre condizioni, garanzie o termini relativi alla fornitura o fornitura presunta dello stesso; la mancata fornitura o eventuali ritardi nella fornitura del Software o della Documentazione che, salvo per il presente paragrafo (vi) potrebbero avere effetto tra Kaspersky Lab e l'utente o potrebbero essere diversamente impliciti o integrati nel presente Contratto o in un eventuale accordo collaterale mediante statuto, diritto consuetudinario o altrimenti, sono esclusi mediante il presente (inclusi, senza tuttavia ad essi limitarsi, le condizioni implicite, le garanzie o altri termini relativi a qualità soddisfacente, idoneità per l'uso previsto o esercizio di ragionevoli competenze e cautele).

#### *6. Responsabilità limitata.*

(i) Nessun elemento del presente Contratto escluderà o limiterà la responsabilità di Kaspersky Lab in merito 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, (c) eventuali altre responsabilità che non possano essere escluse per legge.

(ii) Ai sensi del paragrafo (i) di cui sopra, 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 affari;
- (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 scampo 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.