

**KASPERSKY LAB**

---

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

**Guida di distribuzione**

KASPERSKY® ADMINISTRATION KIT 6.0

---

# Guida di distribuzione

Kaspersky Lab Ltd.

Visitate il nostro sito Web: <http://www.kaspersky.com/>

Data di revisione: Settembre 2007

# Sommario

CAPITOLO 1. KASPERSKY® ADMINISTRATION KIT .....	5
1.1. Scopo, struttura e funzioni principali .....	5
1.2. Requisiti software e hardware.....	7
1.3. Kit di distribuzione.....	8
1.4. Servizi per gli utenti registrati .....	8
1.5. Scopo del presente documento .....	9
1.6. Legenda .....	9
CAPITOLO 2. SCHEMI TIPICI DI DISTRIBUZIONE DELLA PROTEZIONE ANTIVIRUS.....	11
2.1. Schemi di distribuzione della protezione antivirus sui computer della rete logica .....	11
2.2. Creazione di un sistema centralizzato di amministrazione della protezione antivirus .....	12
CAPITOLO 3. INSTALLAZIONE DI KASPERSKY ADMINISTRATION KIT .....	14
3.1. Installazione di MSDE dal pacchetto di distribuzione di Kaspersky Administration Kit .....	14
3.2. Installazione di Administration Server e Administration Console.....	16
3.3. Rimozione dei componenti di Kaspersky Administration Kit.....	32
3.4. Aggiornamento della versione dell'applicazione .....	32
CAPITOLO 4. INSTALLAZIONE E RIMOZIONE DI SOFTWARE SUI COMPUTER.....	34
4.1. Installazione remota del software .....	35
4.1.1. Creazione di un pacchetto d'installazione.....	36
4.1.2. Revisione e configurazione delle impostazioni del pacchetto d'installazione.....	39
4.1.3. Creazione e configurazione del pacchetto d'installazione di Network Agent .....	43
4.1.4. Creazione di un'attività per distribuire il pacchetto d'installazione sugli Administration Server slave.....	46

---

4.1.5. Distribuzione dei pacchetti d'installazione in un gruppo tramite Network Agent .....	48
4.1.6. Creazione di un'attività di installazione remota .....	51
4.1.7. Configurazione dell'attività di distribuzione .....	62
4.1.8. Rimozione remota di software.....	64
4.2. Distribuzione guidata .....	65
4.3. Installazione locale del software .....	69
4.3.1. Installazione locale di Network Agent .....	70
4.3.2. Installazione locale del plugin di amministrazione dell'applicazione .....	75
4.3.3. Installazione delle applicazioni in modalità non interattiva .....	76
APPENDICE A. GLOSSARIO .....	77
APPENDICE B. KASPERSKY LAB .....	85
A.B.1. Altri prodotti Kaspersky Lab .....	86
A.B.2. Per contattarci.....	94
APPENDICE C. CONTRATTO DI LICENZA.....	96

---

# CAPITOLO 1. KASPERSKY® ADMINISTRATION KIT

## 1.1. Scopo, struttura e funzioni principali

**Kaspersky® Administration Kit** è un'applicazione progettata come soluzione centralizzata per le più importanti attività di amministrazione associate con la gestione del sistema di protezione antivirus della rete aziendale, basata sulle applicazioni Kaspersky Lab incorporate in Kaspersky Anti-Virus Business Optimal e Kaspersky Corporate Suite. Kaspersky Administration Kit supporta tutte le configurazioni di rete che utilizzano il protocollo TCP/IP.

Kaspersky Administration Kit è uno strumento destinato agli amministratori di rete ed agli addetti alla sicurezza antivirus.

L'applicazione consente all'amministratore di:

- Implementare o rimuovere le applicazioni Kaspersky Lab tramite una connessione di rete sui computer della rete. Questa funzione consente all'amministratore di copiare il gruppo desiderato di applicazioni Kaspersky Lab su un computer selezionato e quindi di implementare tali applicazioni sui computer della rete.
- Gestire le licenze. Questa funzione consente di installare le chiavi di licenza per tutte le applicazioni Kaspersky Lab installate in modo centralizzato, di monitorare il rispetto del contratto di licenza (vale a dire, la corrispondenza del numero di licenze col numero di applicazioni operanti nella rete) e la data di scadenza.
- Garantire la gestione remota centralizzata delle applicazioni Kaspersky Lab. Questa funzione consente all'amministratore di creare un sistema di protezione antivirus a più livelli, nonché di gestire il funzionamento di tutte le applicazioni da una singola workstation di amministrazione. Ciò è particolarmente importante per le aziende più grandi che dispongono di una rete locale formata da molti computer, che possono essere ubicati in molti edifici od uffici separati. Questa funzione consente all'amministratore di:
  - raggruppare i computer in *gruppi amministrativi* in base alle funzioni eseguite da tali computer ed all'insieme di applicazioni installate su di essi;
  - configurare le impostazioni dell'applicazione in modo centralizzato, creando ed applicando *regole di gruppo*;

- configurare le impostazioni individuali dell'applicazione per singoli computer tramite le *impostazioni dell'applicazione*.
- gestire il funzionamento delle applicazioni in modo centralizzato, creando e lanciando *attività di gruppo e globali*.
- impostare modelli individuali per il funzionamento dell'applicazione, creando e lanciando le attività per un insieme di computer di diversi gruppi amministrativi.
- Aggiornare automaticamente il database antivirus ed i moduli dell'applicazione sui computer. Questa funzione consente l'aggiornamento centralizzato del database antivirus per tutte le applicazioni Kaspersky Lab installate, senza dover accedere ai server di aggiornamento Kaspersky Lab su Internet per ciascun singolo aggiornamento. L'aggiornamento può essere eseguito automaticamente secondo il programma stabilito dall'amministratore. L'amministratore può monitorare l'installazione degli aggiornamenti sui computer client.
- Ricevere report specifici tramite un sistema dedicato. Questa funzione consente la raccolta centralizzata di informazioni statistiche sul funzionamento delle applicazioni Kaspersky Lab installate, monitorando la correttezza del loro funzionamento e creando report specifici in base alle informazioni ottenute. L'amministratore può creare un report cumulativo di rete sul funzionamento di un'applicazione o diversi rapporti sul funzionamento di un'applicazione installata su ciascun computer.
- Utilizzare il sistema di notifica eventi. Sistema di invio notifiche via mail. Questa funzione consente all'amministratore di creare un elenco di eventi per il funzionamento dell'applicazione, per il cui verificarsi riceverà notifiche. L'elenco di tali eventi può, ad esempio, contenere il rilevamento di un nuovo virus, il verificarsi di un errore durante l'aggiornamento del database antivirus su un computer, oppure il rilevamento di un nuovo computer nella rete.

L'applicazione Kaspersky Administration Kit è composta da tre componenti principali:

- **Administration Server** ha la funzione di memorizzare in posizione centralizzata le informazioni relative alle applicazioni Kaspersky Lab installate sulla rete aziendale e di gestire tali applicazioni.
- **Network Agent** coordina l'interazione tra Administration Server e le applicazioni Kaspersky Lab installate su uno specifico nodo di rete (una workstation o un server). Questo componente supporta tutte le applicazioni comprese nelle suite Kaspersky Lab Business Optimal e Kaspersky Corporate.
- **Administration Console** fornisce un'interfaccia utente per i servizi di amministrazione di Administration Server e Network Agent. Il modulo di

gestione è implementato come estensione della Microsoft Management Console (MMC).

## 1.2. Requisiti software e hardware

### Administration Server

- Requisiti software
  - Microsoft Data Access Components (MDAC) versione 2.8 e superiori
  - MSDE 2000 SP 3 o MS SQL Server 2000 SP 3<sup>1</sup> o superiori, o MySQL versione 5.0.22 (code page predefinita UTF-8) o MS SQL 2--5 o superiori o MS SQL 2005 Express o superiori;
  - Microsoft Windows 2000 SP 1 o superiori; Microsoft Windows XP Professional SP 1 o superiori; Microsoft Windows XP Professional x64 o superiori, Microsoft Windows Server 2003 o superiori; Microsoft Windows Server 2003 x64 o superiori, Microsoft Windows NT4 SP 6a o superiori.
- Requisiti hardware:
  - Processore Intel Pentium III , 800 MHz o superiore
  - 128 MB di RAM
  - 400 MB di spazio disponibile sul disco rigido

### Administration Console

- Requisiti software:
  - Microsoft Windows 2000 SP 1 o superiori; Microsoft Windows XP Professional SP 1 o superiori; Microsoft Windows XP Home Edition SP1 o superiori; Microsoft Windows XP Professional x64 o superiori; Microsoft Windows Server 2003 o superiori; Microsoft Windows Server 2003 x64 o superiori, Microsoft Windows NT 4 SP 6a o superiori;
  - Microsoft Management Console versione 1.2 o superiori

---

<sup>1</sup> MSDE può essere installato dal pacchetto incluso nel pacchetto di distribuzione di Kaspersky Administration Kit .

- Requisiti hardware:
  - Processore Intel Pentium II , 400 MHz o superiore
  - Almeno 64 MB di RAM
  - 10 MB di spazio libero sul disco rigido

### **Network Agent**

- Requisiti software:
  - Microsoft Windows 98; Microsoft Windows ME; Microsoft Windows 2000 SP 1 o superiori; Microsoft Windows NT4 SP 6a o superiori; Microsoft Windows XP Professional SP 1 o superiori, Microsoft Windows XP Professional x64 o superiori, Windows Server 2003 o superiori; Microsoft Windows Server 2003 x64 o superiori
- Requisiti hardware:
  - Processore Intel Pentium, 233 MHz o superiore
  - 32 MB di RAM
  - 10 MB di spazio disponibile sul disco rigido

## 1.3. Kit di distribuzione

Questo prodotto software viene distribuito gratuitamente con qualsiasi applicazione Kaspersky Lab inclusa nei pacchetti Kaspersky Anti-Virus Business Optimal e Kaspersky Corporate Suite (confezione "retail"), e può essere scaricato dal sito web di Kaspersky Lab all'indirizzo [www.kaspersky.com](http://www.kaspersky.com).

## 1.4. Servizi per gli utenti registrati

Kaspersky Lab offre un pacchetto di assistenza completo, che consente agli utenti autorizzati di godere di tutte le funzioni disponibili con i prodotti Kaspersky Lab.

Una volta acquistata una licenza per qualsiasi prodotto Kaspersky Lab incluso in Kaspersky Anti-Virus Business Optimal o Kaspersky Corporate Suite, si diventa utenti registrati di Kaspersky Administration Kit. Ciò consente di godere dei seguenti servizi per l'intera durata della licenza:

- Nuova versione dell'applicazione software antivirus;
- Consulenze su installazione, configurazione e funzionamento dell'applicazione antivirus per telefono, o in base a richieste inviate tramite un modulo Web;

Quando si invia una richiesta al Servizio di assistenza tecnica, specificare le informazioni relative alla licenza per l'applicazione Kaspersky Lab utilizzata in congiunzione con Kaspersky Administration Kit.

- Informazioni sulle nuove applicazioni Kaspersky Lab e sui nuovi virus informatici (per gli iscritti alla newsletter di Kaspersky Lab).

Kaspersky Lab non fornisce informazioni relative al funzionamento ed all'utilizzo del sistema operativo utilizzato, ne su altre tecnologie.

## 1.5. Scopo del presente documento

Questa guida descrive l'installazione di Kaspersky Administration Kit e l'installazione remota delle applicazioni in una rete informatica relativamente semplice.

I concetti generali e lo schema operativo delle applicazioni sono disponibili nella Guida dell'amministratore di Kaspersky Administration Kit; le descrizioni passo-passo delle azioni richieste durante l'utilizzo dell'applicazione sono disponibili nel Manuale di riferimento per Kaspersky Administration Kit.

Per visualizzare le domande frequenti poste dai nostri utenti agli specialisti dell'assistenza tecnica di Kaspersky Lab, visitate il nostro sito web e seguite il collegamento **Services → Knowledge base**. Questa sezione contiene informazioni sull'installazione, la configurazione ed il funzionamento delle applicazioni Kaspersky Lab, nonché sulla rimozione dei virus più diffusi e la disinfezione dei file infetti.

## 1.6. Legenda

In questo documento vengono utilizzate diverse caratteristiche di formattazione ed icone, in funzione dello scopo e del significato del testo. La seguente tabella elenca le convenzioni utilizzate nel testo.

Convenzione	Significato
<b>Carattere grassetto</b>	Titoli di menu, comandi, titoli di finestre, elementi della finestra di dialogo, ecc.
Nota	Informazioni supplementari, note.
Attenzione	Informazioni che richiedono particolare attenzione.

<b>Convenzione</b>	<b>Significato</b>
<i>Per eseguire un'azione:</i> 1. Passaggio 1. 2. ...	Descrizione dei passaggi consecutivi e delle azioni possibili da parte dell'utente
[modificatore] – nome modificatore.	Modificatore della riga di comando
Testo nei messaggi informativi e nel testo della riga di comando	Testo dei file di configurazione, dei messaggi informativi e della riga di comando

---

# CAPITOLO 2. SCHEMI TIPICI DI DISTRIBUZIONE DELLA PROTEZIONE ANTIVIRUS

## 2.1. Schemi di distribuzione della protezione antivirus sui computer della rete logica

Due sono gli scenari più comuni che mostrano come implementare una protezione antivirus affidabile con Kaspersky Administration Kit:

- È possibile installare le applicazioni in remoto sui computer client della rete logica da una singola workstation. L'installazione e la connessione al sistema di gestione remota procedono automaticamente, senza alcuna interazione con l'amministratore, consentendo l'installazione del software antivirus su qualsiasi numero di computer client.
- È possibile installare le applicazioni localmente su ciascun computer della rete. In questo caso, l'installazione di tutti i componenti richiesti e della workstation dell'amministratore è manuale. Le impostazioni di connessione vengono selezionate durante l'installazione di Network Agent. La distribuzione viene effettuata in questo scenario solo se è impossibile la distribuzione centralizzata.

L'installazione remota può essere utilizzata per installare qualsiasi applicazione selezionata dall'utente.

Tuttavia, si tenga presente che Kaspersky Administration Kit consente esclusivamente l'amministrazione delle applicazioni di Kaspersky Lab il cui pacchetto di distribuzione comprenda un componente specializzato: il plugin di amministrazione delle applicazioni.

## 2.2. Creazione di un sistema centralizzato di amministrazione della protezione antivirus

Il primo passo nella creazione di un sistema di gestione centralizzata su una rete aziendale tramite Kaspersky Administration Kit è progettare una rete logica. In questa fase, è necessario prendere le seguenti decisioni:

1. Selezionare sezioni isolate all'interno della rete e determinare il numero di copie di Administration Server da installare. Utilizzare la gerarchia dei server di amministrazione consentirà di diminuire considerevolmente il carico sui canali di comunicazione ed aumentare l'affidabilità del sistema.
2. Quali computer nella struttura della rete aziendale opereranno come Administration Server principale e quali come slave dell'Administration Server, workstation di amministrazione e computer client. Si noti che tutti i computer sui quali siano installate applicazioni Kaspersky Lab agiranno quali computer client.
3. I criteri da utilizzare per organizzare i computer client in gruppi. La gerarchia di gruppo da utilizzare.
4. Lo scenario di distribuzione da utilizzare: installazione remota o locale?

Durante la fase successiva, l'amministratore deve creare una rete logica, vale a dire installare i seguenti componenti di Kaspersky Administration Kit sui computer della rete:

1. Installare Administration Server sui computer che fanno parte della rete aziendale.
2. Installare Administration Console sui computer dai quali verrà effettuata l'amministrazione.
3. Assegnare gli amministratori della rete logica, determinare quali altre categorie di utenti interagiranno col sistema ed assegnare un elenco di funzioni da eseguire a ciascuna categoria.
4. Creare elenchi di utenti ed assegnare a ciascun gruppo i diritti di accesso richiesti per l'esecuzione delle funzioni assegnate a tale gruppo e relativi ai diritti di accesso.

Dopodiché, è necessario creare una gerarchia degli Administration Server e creare per ciascun Server una struttura di rete logica come segue: creare una

gerarchia dei gruppi amministrativi e distribuire i computer tra i corrispondenti gruppi.

Durante la fase successiva, sarà necessario installare Network Agent e le applicazioni Kaspersky Lab selezionate sui computer client, quindi installare i relativi plugin di amministrazione sulla workstation di amministrazione.

Se l'installazione viene eseguita in remoto, Network Agent può essere installato con qualsiasi applicazione; in tal caso non è necessaria l'installazione separata di Network Agent.

Durante la fase finale, è necessario configurare le applicazioni installate assegnando ed applicando le regole di gruppo e creando le attività.

Tramite la Procedura guidata di avvio rapido, l'amministratore può creare con facilità un sistema di protezione antivirus per la sua rete ed eseguirne la configurazione di base. La configurazione rapida del sistema di protezione antivirus implica la creazione di una rete logica identica alla struttura di dominio della rete Windows e del sistema di protezione antivirus, basato sulla versione 5.0 e 6.0 di Kaspersky Anti-Virus for Windows Workstations.

---

# CAPITOLO 3. INSTALLAZIONE DI KASPERSKY ADMINISTRATION KIT

Prima di iniziare l'installazione, verificare che il computer soddisfi i requisiti software e hardware per Administration Server e la workstation dell'amministratore (vedere la sezione 1.3 a pagina 8).

Per conservare le informazioni di Administration Server vengono utilizzati MSDE (Microsoft Data Engine), MySQL Server o Microsoft SQL server . Se non sono installati né MSDE né SQL Server, sarà necessario installare uno di questi programmi prima di installare Administration Server. Per fare ciò, è possibile utilizzare i pacchetti di distribuzione disponibili. Per installare MSDE è anche possibile utilizzare il pacchetto di distribuzione di Kaspersky Administration Kit. La procedura di installazione di MSDE da Kaspersky Administration Kit viene trattata in dettaglio di seguito (vedere la sezione 3.1 a pagina 14).

Per installare Kaspersky Administration Kit, sono necessari i diritti dell'amministratore locale per il computer sul quale viene eseguita l'installazione.

L'installazione guidata propone di installare i componenti applicativi di Kaspersky Administration Kit (Administration Server e Administration Console) sul computer sul quale viene eseguita l'installazione guidata. Tale configurazione è consigliata nella fase iniziale di creazione del sistema centralizzato di amministrazione.

## 3.1. Installazione di MSDE dal pacchetto di distribuzione di Kaspersky Administration Kit

Prima di installare MSDE è necessario installare Microsoft Data Access Components (MDAC) 2.8 o superiore (il pacchetto di distribuzione è disponibile sul sito Web di Microsoft).

L'installazione di MSDE dal pacchetto di distribuzione di Kaspersky Administration Kit su un computer viene eseguita a livello locale.

Per installare MSDE:

1. Lanciare il file eseguibile nella directory **MSDE2KSP3** del CD d'installazione di Kaspersky Administration Kit 5.0. L'installazione guidata

proporrà allora di configurare le impostazioni ed eseguire l'applicazione. Attenersi alle istruzioni dell'installazione guidata.

2. I primi passi consistono nel decomprimere i file richiesti dal pacchetto di distribuzione e copiarli sul disco rigido del computer, verificare il software richiesto, accettare il contratto di licenza e fornire le informazioni richieste sull'utente e l'azienda.
3. Quindi, definire quanto segue nella finestra di dialogo **Cartella di installazione**:
  - nel campo **Moduli dell'applicazione** - la cartella d'installazione dei file applicativi di MSDE. La cartella predefinita è: **<Disco:\Programmi\Microsoft SQL Server**. Se questa cartella non esiste, verrà creata automaticamente.
  - nel campo **Database** - una cartella che verrà utilizzata per memorizzare il database MSDE Server. Anche in questo caso la cartella predefinita è **<Disco:\Programmi\Microsoft SQL Server**.

Per selezionare la cartella utilizzare il pulsante **Sfoggia**.

4. Dopodiché, nella finestra di dialogo **Nome SQL Server**(vedere la figura Figura 1), specificare il nome da assegnare a questo server.

L'impostazione predefinita non prevede la creazione di un nome, e per indirizzare il server viene utilizzato il nome del computer sul quale è installato il server.

Se si desidera assegnare un nome diverso, deselezionare la casella **Predefinito** ed immettere un nuovo nome nel campo **Nome SQL Server**.

Una volta configurate le impostazioni, è possibile rivederle e avviare l'installazione. Una volta terminata l'installazione, MSDE sarà installato sul computer.

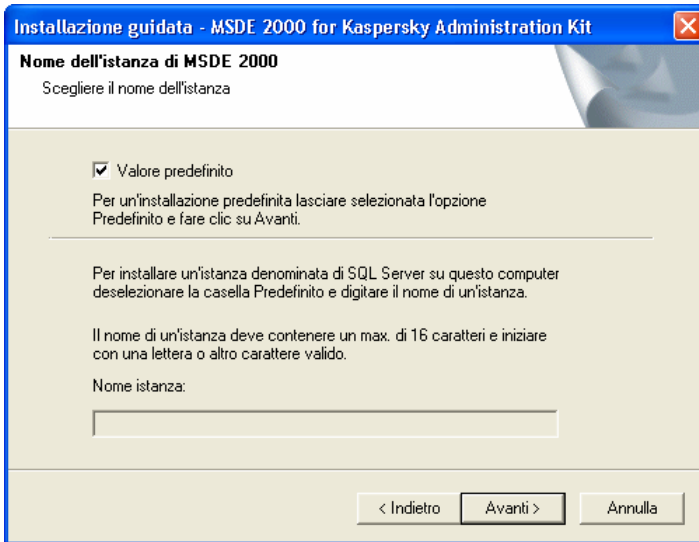


Figura 1. Selezione del nome del server

## 3.2. Installazione di Administration Server e Administration Console

*Per installare Administration Server e/o Administration Console,*

1. Lanciare il file **setup.exe** dal CD d'installazione. L'installazione guidata propone allora di configurare le impostazioni. Attenersi alle istruzioni dell'installazione guidata.
2. Innanzitutto, la procedura guidata decompone i file richiesti dal pacchetto di distribuzione, li copia sul disco rigido del computer e richiede l'accettazione del contratto di licenza e le informazioni sull'utente e l'azienda.
3. Definire quindi la cartella da utilizzare per installare i componenti. La cartella predefinita è: **<Disco:\Programmi\Kaspersky Lab\Kaspersky Administration Kit**. Se questa cartella non esiste, verrà creata automaticamente. Per cambiare cartella, utilizzare il pulsante **Sfogli**.

4. Dopodiché, selezionare i componenti di Kaspersky Administration Kit da installare (vedere la figura 2): **Administration Console** e/o **Administration Server**.

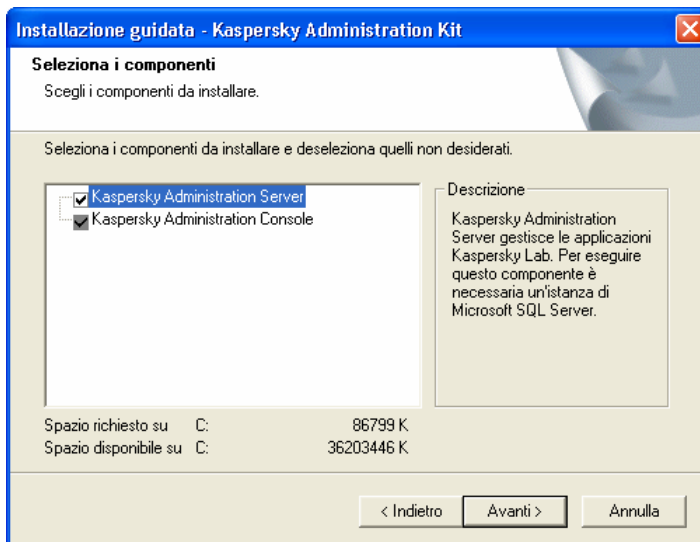


Figura 2. Selezione dei componenti da installare

È possibile selezionare entrambi i componenti o solo la Administration Console. Non è possibile selezionare l'installazione di Administration Server senza installare la Console. L'impostazione predefinita prevede l'installazione di entrambi i componenti.

Con Administration Server verrà installata una versione server di Network Agent. L'installazione congiunta è impossibile utilizzando una versione normale di Network Agent. Se questo componente è già installato sul computer, rimuoverlo e reinstallare Administration Server.

Prestare attenzione alle informazioni visualizzate sulla finestra della procedura guidata:

- il campo **Descrizione** della sezione destra visualizza informazioni sul componente selezionato;
- la sezione in fondo alla pagina visualizza informazioni relative allo spazio richiesto su disco per installare i componenti selezionati e quello disponibile sul disco selezionato per l'installazione.

Se è stata selezionato solo Administration Console, non saranno necessarie ulteriori operazioni per configurare le impostazioni d'installazione e si passerà direttamente a rivedere tali impostazioni, quindi all'avvio dell'installazione.

5. Se è stata selezionata l'installazione di Administration Server, definire durante la fase successiva con quale account verrà avviato come servizio Administration Server su questo computer (vedere la figura 3).

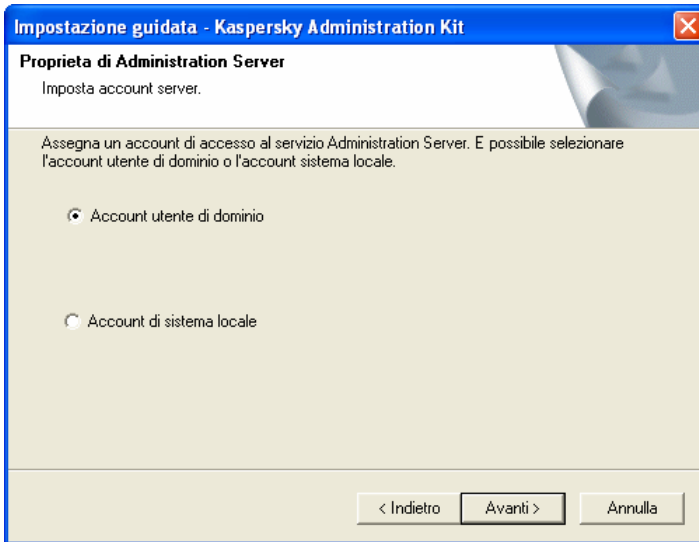


Figura 3. Selezione dell'account

Le due opzioni disponibili sono:

- **Account utente di dominio** - Administration Server verrà avviato con l'account utente incluso nel dominio. In questo caso, l'Administration Server avvierà tutte le operazioni utilizzando i diritti di questo account, e durante la fase successiva verrà richiesto di specificare l'utente proprietario dell'account che verrà utilizzato.

Se è stata creata una struttura di dominio Windows all'interno della rete aziendale, consigliamo di selezionare l'account dell'amministratore di dominio per l'avvio di Administration Server. Ciò eviterà la necessità di configurare ulteriori impostazioni in futuro, quali, ad esempio, l'account di un utente che disponga dei diritti di amministratore di dominio durante la creazione di un'attività di distribuzione (installazione remota) (vedere la sezione 4.1.6 a pagina 51).

- **Account di sistema locale** - Administration Server verrà avviato con l'**account di sistema** con tutti i diritti di questo account. In questo caso non è necessario selezionare un account utente, e si passerà direttamente alla fase in cui sarà necessario specificare il percorso alla memorizzazione del database informativo di Administration Server.

Per un funzionamento corretto di Kaspersky Administration Kit, è necessario che l'account utilizzato per avviare Administration Server disponga dei diritti di amministratore per la risorsa utilizzata per memorizzare il database informativo di Administration Server.

6. Se è stato selezionato un account utente di dominio con cui avviare Administration Server, verrà richiesto di specificare tale utente.

Per fare ciò, nel campo **Nome utente** della finestra della procedura guidata (vedere Figura 4) selezionare il nome utente tramite il pulsante **Sfoglia...** oppure inserire manualmente tale nome, da quelli registrati nel dominio corrente. Dopodiché, inserire la password utilizzata per registrare l'utente nel dominio.

Installazione guidata - Kaspersky Administration Kit

**Proprietà di Administration Server**  
Account servizio

Seleziona l'account utente per il servizio Administration Server.

Nome utente:  
 Sfoglia...

Password:

È possibile creare un nuovo account utente

< Indietro   Avanti >   Annulla

Figura 4. Selezione dell'utente

Se è stato selezionato un utente che non dispone dei diritti di amministratore di dominio, Administration Server verrà lanciato con l'account selezionato, tuttavia la funzionalità di Kaspersky Administration Kit non sarà completa. Ad esempio, potrebbe non disporre dei diritti

necessari per eseguire un'attività di distribuzione utilizzando uno scenario di lancio (vedere la sezione 4.1.6 a pagina 51) ed il polling di alcuni domini della rete Windows.

Per il corretto funzionamento di Administration Server, l'account utilizzato per lanciarlo deve disporre dei seguenti diritti:

- Accedere come servizio;
- Operare come parte del sistema operativo;
- Accedere a questo computer dalla rete;
- Sostituire un token a livello di processo;
- Aumentare/regolare le quote di memoria per un processo.

Se l'utente selezionato è un amministratore di dominio ma non dispone dei diritti summenzionati, tali diritti gli verranno concessi (vedere Figura 5).

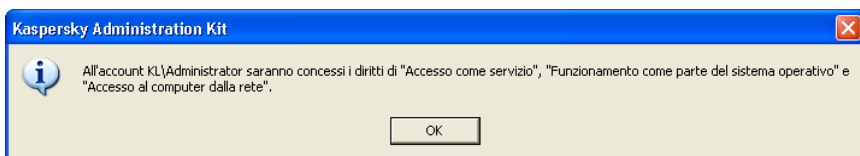


Figura 5. Messaggio relativo ai diritti concessi all'utente.

Se si dispone dei diritti di amministratore di dominio, è possibile creare un utente speciale ed utilizzare tale account per lanciare Administration Server. All'utente verranno concessi i diritti di amministratore di dominio come anche quelli summenzionati.

Per creare un utente speciale, scegliere il pulsante **Crea** ed immettere quanto segue nella finestra di dialogo che viene visualizzata (vedere Figura6):

- nome utente (obbligatorio);
- nome utente completo (facoltativo);
- dettagli supplementari utente. Per impostazione predefinita, verrà immesso **Account per avviare Administration Server** (non richiesto);
- password dell'account (obbligatorio);
- 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

Figura6. Creazione di un nuovo utente

7. Nella fase successiva , verrà richiesto di definire la risorsa **Microsoft SQL server (MSDE)** o **MySQL** (vedere Figura 7), che verrà utilizzata per memorizzare il database informativo di Administration Server.

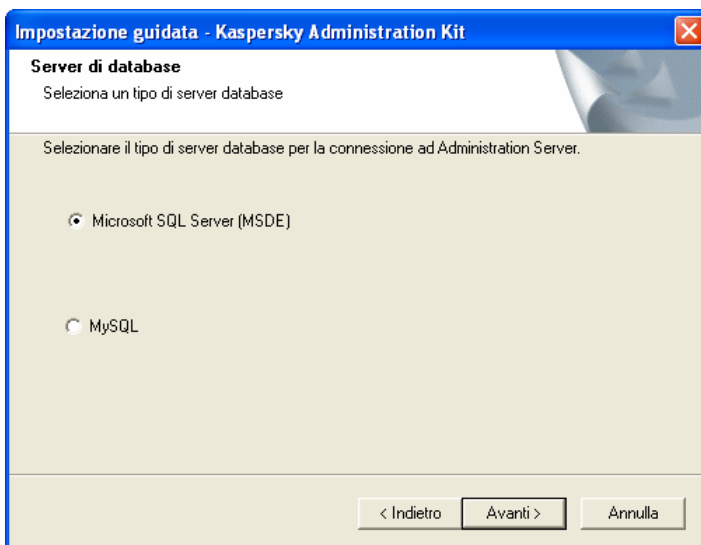


Figura 7. Selezione del database

8. Se durante la fase precedente è stato selezionato MSDE o Microsoft SQL server e si intende utilizzare un server installato nella rete aziendale per lavorare con Kaspersky Administration Kit, indicare il nome di tale server nel campo **Nome server SQL** e specificare il nome del database che verrà creato per memorizzare i dati di Administration Server nel campo **Nome database SQL server** (vedere Figura 8 ). Per impostazione predefinita, il nome del database è **KAV**.

Il valore **(locale)** verrà assegnato automaticamente al campo **Nome server** se viene rilevato un'installazione di SQL server sul computer dal quale si sta installando Kaspersky Administration Kit. Per visualizzare l'elenco di tutte le installazioni di Microsoft SQL server rilevate sulla rete, premere il pulsante **Sfoggia...** .

Se Administration Server verrà avviato con l'account dell'amministratore locale o con l'account di sistema, il pulsante **Sfoggia** non sarà disponibile.

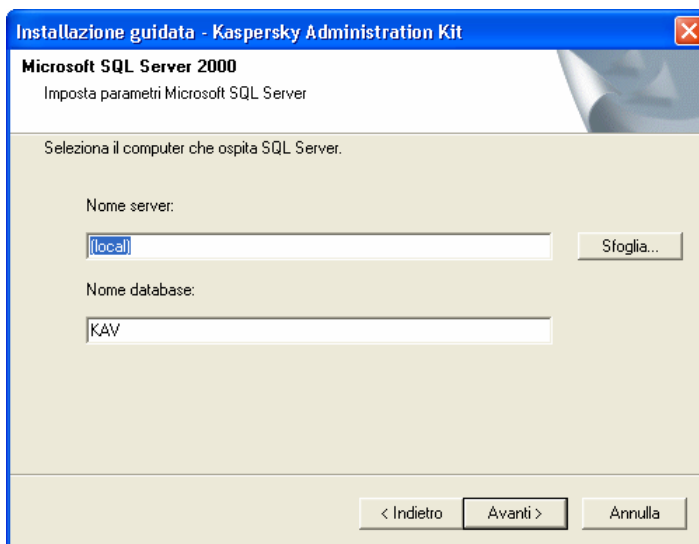


Figura 8. Selezione di SQL server

Se durante la fase precedente è stato selezionato MySQL server, specificare il suo nome in questa finestra (vedere Figura 9) nel campo **Nome MySQL server** (per impostazione predefinita, verrà utilizzato l'indirizzo IP del computer sul quale si sta installando Kaspersky Administration Kit) e specificare la porta da utilizzare per la connessione nel campo **Porta** (la porta predefinita è la 3306). Nel campo **Nome database MySQL server** specificare il nome del database che verrà creato per memorizzare i dati di Administration Server (per impostazione predefinita il database verrà creato col nome **KAV**).

Se durante la fase precedente è stato selezionato MySQL server, specificarlo in questa finestra

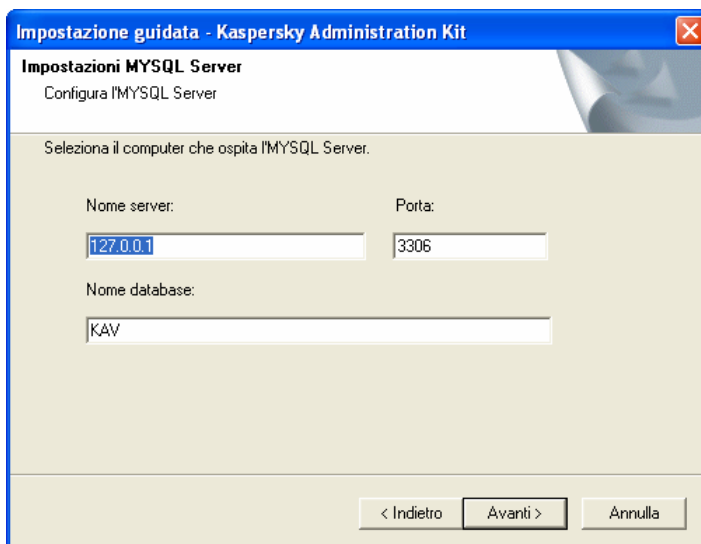


Figura 9. Selezione di MySQL server

Se non ci sono installazioni di SQL server nella rete e non è possibile utilizzarlo, è necessario installarlo (vedere la sezione 3.1a pagina 14).

Per installare SQL server sul computer dal quale si sta installando Kaspersky Administration Kit, è necessario interrompere l'installazione e riavviarla dopo aver installato SQL server.

Se si installa Kaspersky Administration Kit su un computer remoto, non è necessario interrompere l'installazione guidata di Kaspersky Administration Kit. Installare SQL server e tornare all'installazione di Kaspersky Administration Kit.

9. In questa fase è necessario definire la modalità di autenticazione che deve essere utilizzata da Administration Server per connettersi a SQL server.

Per MSDE o Microsoft SQL server è possibile selezionare una delle due seguenti opzioni (vedere Figura 10).

- **Modalità di autenticazione di MS Windows** - in questo caso, i diritti saranno verificati tramite l'account utilizzato per avviare Administration Server;
- **Modalità di autenticazione SQL Server**- scegliendo questa opzione, per verificare i diritti verrà utilizzato l'account

specificato sotto. Compilare i campi **Password dell'account**  
**Conferma password.**

Impostazione guidata - Kaspersky Administration Kit

**Modalità di autenticazione SQL**  
Scegliere una modalità di autenticazione

Scegliere la modalità di sicurezza (autenticazione) da utilizzare per la connessione a Microsoft SQL Server 2000 o 2005. Se si seleziona Autenticazione SQL Server, occorre specificare l'account e confermare la password.

Modalità di autenticazione Microsoft Windows

Modalità di autenticazione SQL Server

Account:

Password:

Conferma password:

< Indietro   Avanti >   Annulla

Figura 10. Modalità di autenticazione SQL server

Per MySQL server, indicare l'account e la password (vedere la figura 11).

**Impostazione guidata - Kaspersky Administration Kit**

**Modalità di autenticazione SQL**  
Scegliere una modalità di autenticazione

Scegliere la modalità di sicurezza (autenticazione) da utilizzare per la connessione a Microsoft SQL Server 2000 o 2005. Se si seleziona Autenticazione SQL Server, occorre specificare l'account e confermare la password.

Modalità di autenticazione Microsoft Windows

Modalità di autenticazione SQL Server

Account:

Password:

Conferma password:

< Indietro   Avanti >   Annulla

figura 11. Modalità di autenticazione SQL server

10. Dopodiché (vedere Figura 12), specificare la posizione della cartella condivisa che verrà utilizzata per:
  - memorizzare i file richiesti per l'installazione remota delle applicazioni (i file saranno copiati sugli Administration Server durante la creazione dei pacchetti d'installazione);
  - memorizzare gli aggiornamenti copiati dalla fonte degli aggiornamenti su Administration Server.

Questa risorsa sarà pubblica per tutti gli utenti solo in lettura.

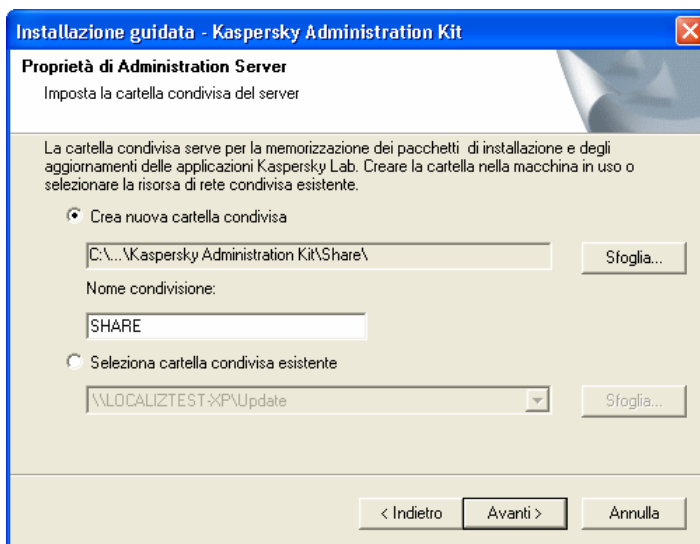


Figura 12. Creazione di una cartella condivisa

È possibile selezionare una delle due seguenti opzioni:

- **Nuova cartella condivisa** - per creare una nuova cartella; sarà necessario specificare il percorso alla cartella nel campo sottostante.
- **Seleziona cartella condivisa esistente** - per selezionare una cartella condivisa dall'elenco di quelle esistenti.

Una cartella condivisa pubblica può essere memorizzata sia localmente, sul computer dal quale si sta eseguendo l'installazione, che in remoto, su qualsiasi computer compreso nella rete aziendale.

Per impostazione predefinita, una **Condivisione** di cartella locale verrà creata nella cartella specificata per l'installazione dei componenti applicativi di Kaspersky Administration Kit.

11. Dopodiché, configurare le impostazioni da utilizzare per la connessione ad Administration Server (vedere Figura 13);
  - numero di porta da utilizzare per la connessione ad Administration Server. Per impostazione predefinita, verrà utilizzata la porta **14000**. Se è già stata assegnata, è possibile sceglierne un'altra.

- Numero di porta SSL che verrà utilizzata per la connessione sicura ad Administration Server tramite il protocollo SSL. Per impostazione predefinita, verrà utilizzata la porta **13000**.

Se Administration Server è in esecuzione in Microsoft Windows XP SP 2, il firewall incorporato blocca le porte TCP nr. 13000 e 14000. Per consentire l'accesso ad Administration Server, sarà allora necessario aprire queste porte manualmente.

Installazione guidata - Kaspersky Administration Kit

**Proprietà di Administration Server**  
Imposta porte server.

Definisci porta Administration Server. Il valore deve essere compreso tra 1 e 65535.

Porta server:

Definisci porta SSL Administration Server. Il valore deve essere compreso tra 1 e 65535.

Porta SSL server:

< Indietro   Avanti >   Annulla

Figura 13. Impostazioni utilizzate per la connessione a Administration Server

12. In questa finestra della procedura guidata (vedere Figura 14), indicare il metodo di creazione del certificato da utilizzare per l'autenticazione della copia di Administration Server da installare.

Sono disponibili due opzioni:

- **Crea nuovo certificato** - selezionare questa opzione se si sta installando una nuova copia di Administration Server. Salvare una copia di backup del certificato in modo che, se si rendesse necessario in futuro, sia più facile ripristinare la data e la struttura della rete logica di questo server. Per fare ciò, selezionare la casella **Crea una copia di backup del certificato**.
- **Ripristina certificato** - selezionare questa opzione se si sta ripristinando Administration server senza alcuna copia di

backup disponibile. In questo caso, è possibile ripristinare i dati e la struttura della rete logica della precedente installazione di Administration Server.

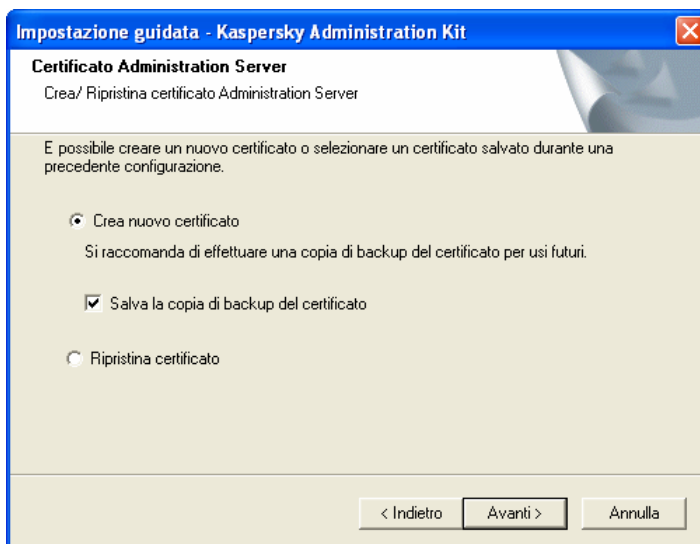


Figura 14. Selezione del metodo da utilizzare per ricevere il certificato Administration Server

13. Se durante la fase precedente è stata selezionata la creazione di un nuovo certificato ed il salvataggio di una sua copia di backup, specificare quanto segue nella relativa finestra (vedere Figura 15):
  - cartella dove salvare la copia di backup del file certificato;
  - password da utilizzare per la crittografia durante la creazione di un nuovo certificato e la sua decriptazione durante il suo ripristino da una copia di backup;
  - conferma della password.

**Per poter ripristinare in seguito i dati di Administration Server, è necessario salvare il certificato del Server.**

Quando si ripristina il certificato è necessario immettere la stessa password utilizzata per la creazione della copia di backup. Se viene immessa una password errata, il certificato non verrà ripristinato.

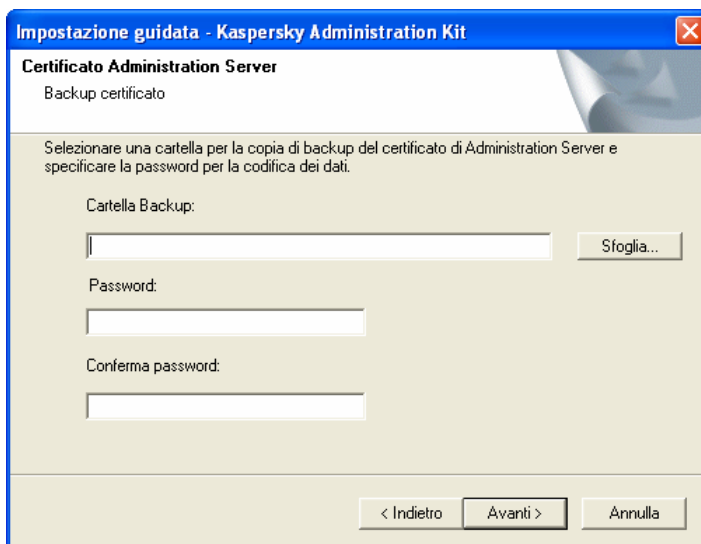


Figura 15. Selezione della cartella per il salvataggio della copia di backup del certificato

Se durante la fase precedente è stata selezionata l'opzione di ripristino del certificato del Server da una copia di backup, specificare quanto segue nella finestra corrispondente (vedere Figura 16):

- cartella in cui salvare la copia di backup del file certificato;
- password utilizzata per la crittografia durante la creazione di una copia di backup del certificato.

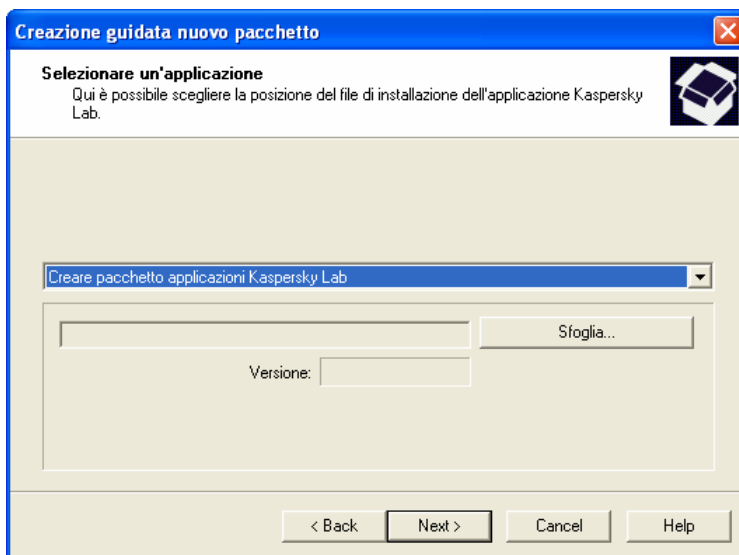


Figura 16. Selezione della cartella dove salvare la copia di backup del certificato.

Una volta terminata la configurazione delle impostazioni di installazione di Kaspersky Administration Kit, è possibile rivederle prima di iniziare l'installazione.

Una volta installata la Administration Console, la relativa icona verrà visualizzata nel menu **Start** → **Tutti i programmi** → **Kaspersky Administration Kit** del computer in uso. Questa icona può essere utilizzata per avviare la Console.

Administration Server sarà installato sul computer come servizio, con i seguenti attributi:

- nome servizio(**CSAdminServer**);
- nome visualizzato **Kaspersky Administration Server**;
- lancio automatico all'avvio del sistema operativo
- account **Sistema locale** oppure un account utente, a seconda della scelta effettuata

Con Administration Server, verrà installata sul computer una versione server di Network Agent. È compresa nella struttura del componente Administration Server e viene installata o rimossa con quest'ultimo; può interagire esclusivamente con l'Administration Server installato localmente. Non è necessario configurare le impostazioni utilizzate da Agent per connettersi a Administration Server, poiché, per impostazione predefinita, questa connessione è implementata in base al presupposto che questi componenti siano installato

sullo stesso computer. Tale configurazione consente di evitare ulteriori configurazioni ed eventuali conflitti nel funzionamento dei componenti se installati separatamente.

Una versione server di Network Agent viene installata con gli stessi attributi, ed esegue le stesse funzioni di amministrazione della versione standard di Network Agent. Opererà in base alla regola del gruppo nel quale è incluso il computer di Administration Server come computer client; verranno create tutte le attività previste per Network Agent, tranne l'attività di cambio server.

Non è necessaria un'installazione separata di Network Agent sul computer di Administration Server. Le sue funzioni verranno eseguite dalla versione server.

È possibile rivedere le proprietà del servizio **Kaspersky Administration Server** e monitorarne il funzionamento tramite gli strumenti di amministrazione standard di Windows - **Gestione computer** → **Servizi**. Le informazioni sul funzionamento del servizio **Kaspersky Administration Server** verranno registrate e salvate nel log di sistema di Windows sul computer sul quale è installato Administration Server, in una sezione separata del **log eventi Kaspersky**.

Inoltre, verranno creati gruppi aggiuntivi di utenti locali **KLAdmins** e **KLOperators** sul computer sul quale è installato Administration Server. Se viene eseguito Administration Server con l'account di un utente incluso nel dominio, allora i gruppi **KLAdmins** e **KLOperators** verranno aggiunti all'elenco di gruppi degli utenti di dominio. La modifica dell'elenco dei gruppi viene eseguita tramite gli strumenti di amministrazione standard di Windows.

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

È possibile rimuovere Kaspersky Administration Kit tramite l'applicazione **Installazione applicazioni** in dotazione con Windows. Ciò disinstallerà dal computer Administration Console, Administration Server e la versione server di Network Agent.

Quando si rimuovono i programmi verrà proposto di salvare una copia di backup di Administration Server.

### 3.4. Aggiornamento della versione dell'applicazione

Per aggiornare la versione 4.x di Kaspersky Administration Kit alla versione 6.0 è necessario disinstallare la versione precedente e installarne una nuova come descritto nella presente guida.

Quando si aggiorna la versione 6.0 ad una versione più recente, ad esempio dalla SP 1 alla SP 2, si consiglia di attenersi alla seguente procedura:

Il ripristino dei dati durante l'upgrade ad una versione più recente dell'applicazione è supportato a partire da Kaspersky Administration Kit versione 5.0 Maintenance Pack 3.

1. Tramite l'utility **klbackup.exe**, creare una copia di backup dei dati dell'Administration Server installato. Questa utility è inclusa nel pacchetto di distribuzione di Kaspersky Administration Kit; una volta installato Administration Server, essa si trova nella cartella root di installazione. Si noti che per poter ripristinare completamente i dati di Administration Server, sarà necessario salvare il certificato del Server. Questa è un'impostazione obbligatoria per l'utility **klbackup.exe**
2. Lanciare l'installazione della versione più recente di Kaspersky Administration Kit 6.0 sul computer sul quale era installata la versione precedente di Administration Server. Aggiornare il componente. Durante l'upgrade, tutti i dati della precedente versione di Administration Server verranno salvati e resi disponibili nella nuova versione. La retrocompatibilità tra la nuova e la vecchia versione di Administration Server è supportata.
3. Per aggiornare la versione di Network Agent installata sui computer della rete, creare un gruppo o un'attività globale per l'installazione di una versione più recente del componente. Eseguire l'attività manualmente o come da pianificazione. Una volta completata questa attività, Network Agent sarà aggiornato alla nuova versione.

In caso di problemi durante l'installazione, è possibile ripristinare la versione precedente di Kaspersky Administration Kit utilizzando la copia di backup dei dati Administration Server creata prima dell'upgrade.

---

# CAPITOLO 4. INSTALLAZIONE E RIMOZIONE DI SOFTWARE SUI COMPUTER

Prima di avviare l'installazione, verificare che il software e l'hardware dei computer soddisfino i relativi requisiti (vedere la sezione 1.3 a pagina 8)

Kaspersky Administration Kit consente l'installazione e la rimozione delle applicazioni di Kaspersky Lab tramite i seguenti metodi:

- in remoto secondo una procedura centralizzata, tramite Administration Console;
- localmente, su ciascun singolo computer.

La connessione di Administration Server coi computer client è garantita dal componente Network Agent. Di conseguenza, tale componente deve essere installato su ciascun computer che verrà connesso al sistema di amministrazione centrale remoto, prima di avviare l'installazione delle applicazioni antivirus. Se si utilizza la procedura centralizzata per installare le applicazioni tramite Administration Console, Network Agent può essere installato insieme ad una delle applicazioni.

Sul computer sul quale è installato Administration Server, è possibile utilizzare solo la versione server di Network Agent. Esso è incluso nella struttura di Administration Server e viene installato e rimosso insieme ad Administration Server (vedere la sezione 3.2 a pagina 16).

Non è necessario installare Network Agent su questo computer.

Network Agent viene installato nella stessa maniera delle applicazioni - vale a dire, in remoto o localmente.

Le copie di Network Agent possono differire in funzione delle applicazioni Kaspersky Lab per le quali sono installate. In alcuni casi, è possibile esclusivamente l'installazione locale di Network Agent (per dettagli, vedere le Guide delle relative applicazioni). Network Agent viene installato solo una volta sul computer client.

L'interfaccia di amministrazione delle applicazioni di Kaspersky Administration Kit viene implementata tramite i corrispondenti plugin di amministrazione. Di conseguenza, per accedere all'interfaccia di amministrazione dell'applicazione, è necessario installare il plugin corrispondente sulla workstation dell'amministratore. In caso di installazione in remoto, l'installazione è automatica alla creazione del primo pacchetto di installazione per la corrispondente applicazione. In caso di installazione locale sul computer client, il plugin di amministrazione deve essere installato manualmente dall'amministratore.

## 4.1. Installazione remota del software

L'installazione remota del software può essere eseguita dalla workstation dell'amministratore nella finestra principale dell'applicazione di Kaspersky Administration Kit.

Alcune applicazioni Kaspersky Lab possono essere installate sui computer client solo in locale (per dettagli vedere le guide delle relative applicazioni). Tuttavia, l'amministrazione remota di tali applicazioni tramite Kaspersky Administration Kit sarà disponibile.

*Per effettuare l'installazione software in remoto:*

1. Creare un pacchetto d'installazione (vedere la sezione 4.1.6 a pagina 51). La struttura di questo pacchetto comprenderà i file richiesti per installare l'applicazione ed i file contenenti le impostazioni del pacchetto d'installazione.

Il pacchetto d'installazione contiene il file setup.exe, che viene utilizzato per eseguire l'installazione locale dell'applicazione in modalità non interattiva.

2. Creare un'attività di installazione remota (vedere la sezione 4.1.6 a pagina 51).

Per installare l'applicazione su tutti i computer della rete logica o diversi gruppi amministrativi o su computer specifici di diversi gruppi, è necessario creare un'attività di distribuzione globale (installazione remota).

Per installare l'applicazione su tutti i computer di un gruppo amministrativo (compresi tutti i gruppi nidificati ed i server slave), è necessario creare un'attività di distribuzione di gruppo (installazione remota).

È possibile utilizzare la procedura di distribuzione guidata (vedere la sezione 4.2 a pagina 65) per creare un gruppo o un'attività globale.

L'attività creata verrà lanciata secondo quanto pianificato. Le impostazioni di funzionamento dell'applicazione sui ciascun computer verranno configurate secondo la regola di gruppo e le impostazioni predefinite dell'applicazione.

È possibile interrompere la procedura d'installazione interrompendo manualmente l'esecuzione dell'attività.

Tutti i pacchetti d'installazione creati per Administration Server saranno ubicati nell'albero della console in una posizione speciale **Installazione remota**. Su

Administration Server, questi pacchetti d'installazione verranno conservati nella cartella condivisa specificata nella cartella di servizio **Pacchetti**.

È possibile rivedere le proprietà del pacchetto d'installazione, modificare il suo nome e le impostazioni tramite la finestra **Proprietà: finestra <nome pacchetto>** (vedere Figura 20). Questa finestra si apre tramite la voce del menu di scelta rapida **Proprietà** o la voce analoga del menu **Azione**.

I pacchetti di installazione creati possono essere distribuiti sui slave di Administration Server (vedere la sezione 4.1.4 a pagina 46) e sui computer di un gruppo tramite gli agenti di aggiornamento (vedere la sezione 4.1.5 a pagina 48).

Un pacchetto di installazione può essere riutilizzato diverse volte per creare attività di distribuzione.

## 4.1.1. Creazione di un pacchetto d'installazione

*Per creare un pacchetto d'installazione:*

1. Connettersi all'Administration Server richiesto.
2. Selezionare nell'albero della console il nodo **Installazione remota**, aprire il menu di scelta rapida e scegliere il comando **Crea**→ **pacchetto d'installazione** o utilizzare la voce analoga dal menu **Azione**. Ciò avvierà la procedura guidata. Seguire le istruzioni.
3. Verrà richiesto di specificare il nome del pacchetto d'installazione, e, durante la fase successiva, di specificare l'applicazione da installare (vedere Figura 17).

Se si sta installando un'applicazione che supporta l'amministrazione remota tramite Kaspersky Administration Kit, sarà necessario selezionare l'opzione **Crea il pacchetto d'installazione per l'applicazione Kaspersky Lab** dal menu a discesa. Tramite il pulsante **Sfoggia...**, selezionare il file che contiene la descrizione dell'applicazione (l'estensione del file è **.kpd**, ed è incluso nel pacchetto di distribuzione per tutte le applicazioni Kaspersky Lab che supportano l'amministrazione remota) o un'archivio autoestraente dell'applicazione Kaspersky Lab (l'estensione del file è **.exe** e può essere scaricato dal sito web di Kaspersky Lab). I campi con il nome dell'applicazione ed il numero di versione verranno allora compilati automaticamente.

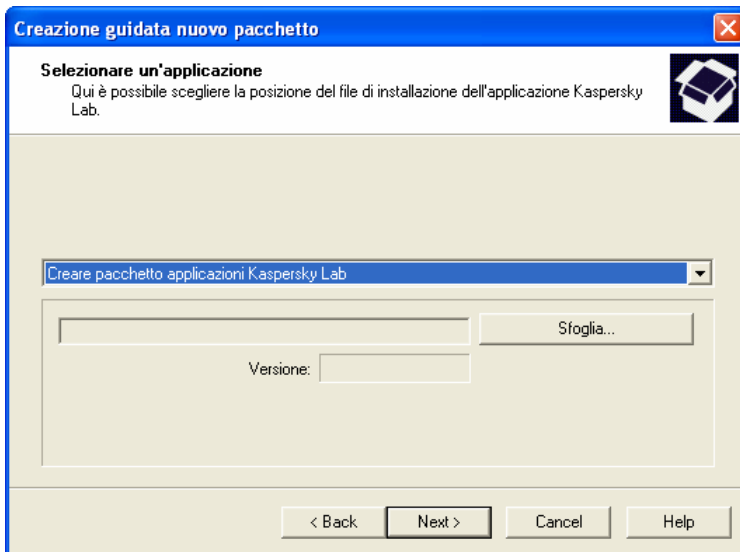


Figura 17. Creazione di un pacchetto d'installazione. Selezione dell'applicazione da installare

Le impostazioni del pacchetto d'installazione verranno create per impostazione predefinita e corrisponderanno all'applicazione selezionata per l'installazione. È possibile modificare le impostazioni dopo aver creato il pacchetto tramite la finestra di revisione delle proprietà del pacchetto (vedere la sezione 4.1.2 a pagina 39).

Se viene creato un pacchetto d'installazione per installare altre applicazioni (vedere la figura 18):

- selezionare Crea pacchetto d'installazione per l'applicazione specificata dall'utente dall'elenco a discesa;
- indicare il percorso al pacchetto di distribuzione dell'applicazione tramite il pulsante **Sfogli**;
- selezionare la casella **Copia intera cartella nel pacchetto d'installazione**, se il pacchetto deve contenere l'intero contenuto della cartella in cui è ubicato il file di distribuzione;
- specificare le impostazioni utilizzate per lanciare il file eseguibile nella riga d'immissione fornita, se tali impostazioni sono richieste per installare l'applicazione (ad esempio, l'esecuzione in modalità non interattiva).

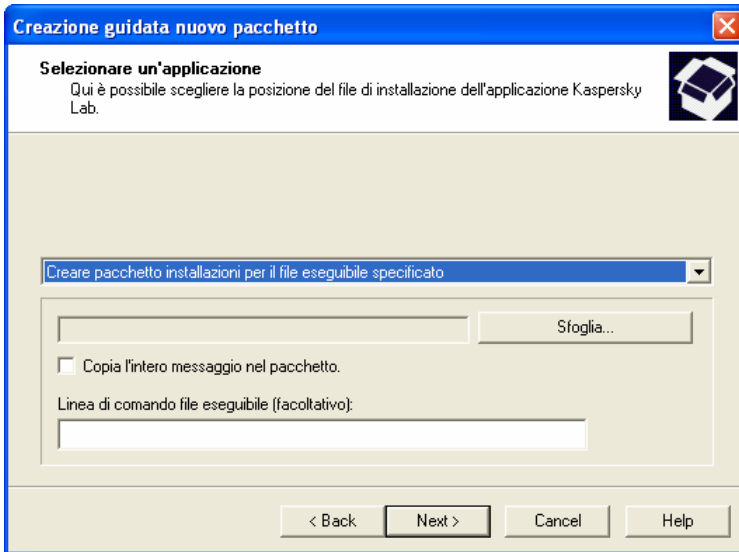


Figura 18. Creazione di un pacchetto d'installazione per installare l'applicazione specificata dall'utente.

4. Nella successiva finestra della procedura guidata, (vedere Figura 19), è possibile specificare la chiave di licenza che verrà inclusa nel pacchetto d'installazione. Per fare ciò, scegliere il pulsante **Sfoglia...** e selezionare il file della chiave di licenza richiesto (l'estensione del file è **.key**)

Se non si desidera includere la chiave di licenza nel pacchetto d'installazione, scegliere il pulsante **Avanti>** .

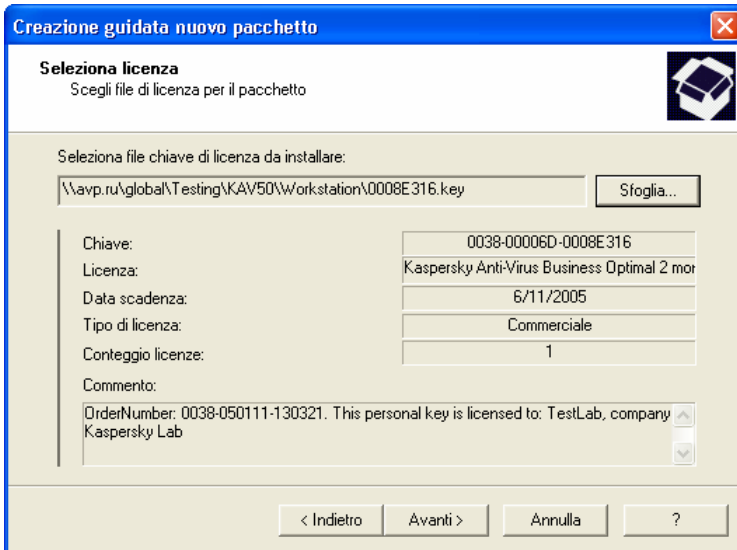


Figura 19. Creazione di un pacchetto d'installazione. Selezione della chiave di licenza

5. Dopodiché, l'insieme di file richiesti per l'installazione dell'applicazione specificata sui computer client viene scaricato nella cartella condivisa di Administration Server; verrà inoltre verificato che il plugin di amministrazione per l'applicazione selezionata sia installato sulla workstation dell'amministratore. Se tale plugin non è installato, o è di versione più vecchia rispetto a quella inclusa nel pacchetto di distribuzione, verrà installato il nuovo plugin a sostituzione di quello vecchio.

Una volta completata la procedura guidata, il pacchetto d'installazione creato verrà aggiunto al nodo **Installazione remota** e visualizzato nel riquadro dei risultati.

#### 4.1.2. Revisione e configurazione delle impostazioni del pacchetto d'installazione

*Per rivedere le proprietà del pacchetto d'installazione o modificarne il nome e le impostazioni:*

nell'albero della console, aprire il nodo **Installazione remota**, selezionare il pacchetto d'installazione richiesto nel riquadro dei risultati ed utilizzare il comando **Proprietà** dal menu di scelta rapida o la voce analoga dal menu **Azione**.

Si aprirà la finestra **Proprietà <Nome del pacchetto d'installazione>** (vedere Figura 20) che comprende le schede **Generale**, **Impostazioni**, **Licenze** e **Reboot SO**.

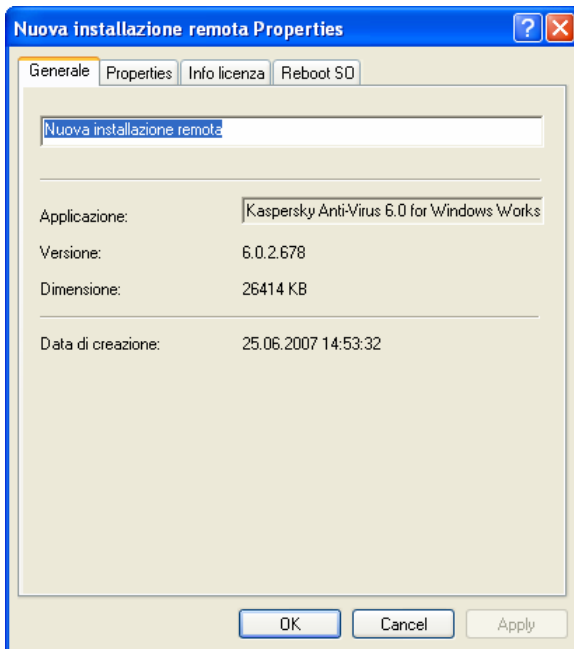


Figura 20. Finestra di revisione delle proprietà del pacchetto d'installazione  
La **scheda** Generale

La scheda **Generale** (vedere Figura 20) contiene informazioni generali sul pacchetto:

- nome pacchetto;
- nome e versione dell'applicazione per la cui installazione è stato creato il pacchetto stesso;
- dimensione del pacchetto;
- data di creazione.

La scheda **Impostazioni** (vedere Figura 21) contiene le impostazioni del pacchetto d'installazione per l'applicazione per la cui installazione è stato

creato il pacchetto stesso; Queste impostazioni vengono create per impostazione predefinita in fase di creazione del pacchetto, e, se richiesto, possono essere modificate.

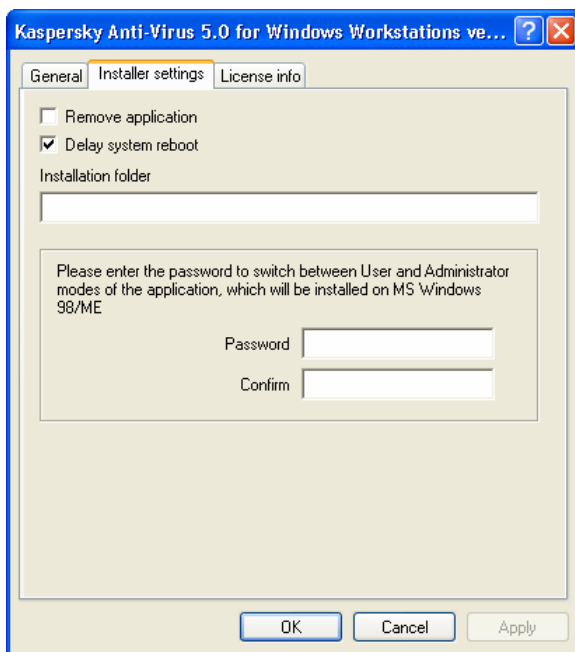


Figura 21. Finestra di revisione delle proprietà del pacchetto d'installazione  
La scheda **Impostazioni**

La scheda **Licenze** (vedere Figura 22) contiene informazioni generali sulla licenza per l'applicazione per la cui installazione è stato creato il pacchetto.

La scheda **Licenze** non è disponibile nelle proprietà del pacchetto d'installazione di Network Agent.

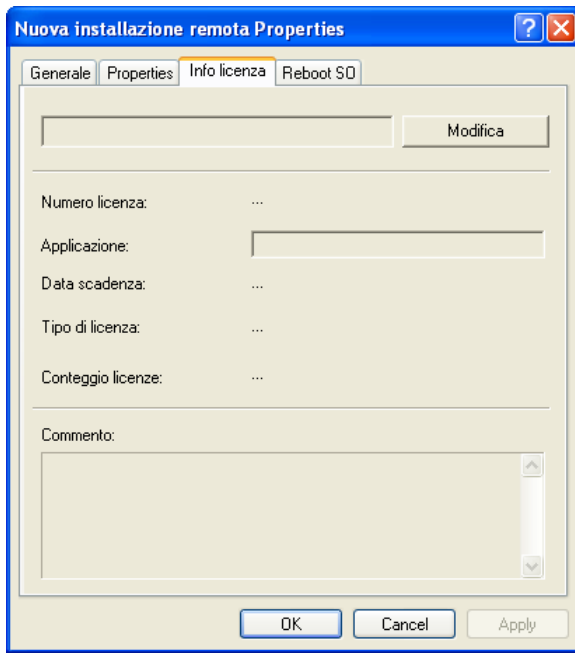


Figura 22. Finestra di revisione delle proprietà del pacchetto d'installazione  
La scheda Licenze

La scheda **Reboot SO** (vedere Figura 23) consente di determinare le azioni da eseguire se il computer deve essere riavviato dopo l'installazione dell'applicazione. È possibile selezionare una delle seguenti opzioni:

- **Non riavviare il sistema operativo**
- **Riavvia automaticamente il sistema operativo**
- **Richiedi l'intervento dell'utente** - se è selezionata questa opzione, è possibile:
  - creare un messaggio informativo che verrà visualizzato in un campo d'immissione per notificare all'utente che è necessario riavviare il sistema operativo.
  - specificare una frequenza per le notifiche relative al riavvio del sistema operativo, se l'utente ha annullato il riavvio, selezionando la casella **Ripeti notifica ogni (min.)** e specificando l'intervallo per la visualizzazione del messaggio;

- o specificare il riavvio automatico del sistema operativo del computer se non eseguito dall'utente entro gli intervalli temporali specificati, a partire dal momento in cui l'applicazione è stata installata. Per fare ciò, selezionare la casella **Forza il riavvio tra (min.)** e specificare l'intervallo temporale.

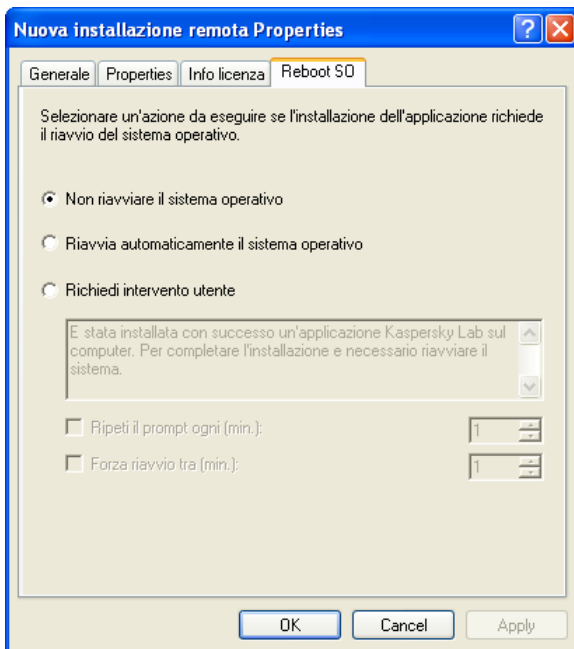


Figura 23. Finestra di revisione delle proprietà del pacchetto d'installazione  
La scheda **Reboot SO**

### 4.1.3. Creazione e configurazione del pacchetto d'installazione di Network Agent

Non è necessario creare manualmente il pacchetto d'installazione per l'installazione remota di Network Agent. Esso viene creato automaticamente durante l'installazione di Kaspersky Administration Kit e ubicato nel nodo **Installazione remota**.

Se il pacchetto per l'installazione remota di Network Agent è stato eliminato, per ricrearlo selezionare il file **knagent.kpd**, ubicato nella cartella NetAgent del pacchetto di distribuzione di Kaspersky Administration Kit, da utilizzare come file contenente la descrizione

Le impostazioni di installazione di Network Agent contengono un insieme minimo di impostazioni richieste per garantire il funzionamento del componente subito dopo la sua installazione. Il valore delle impostazioni è quello delle impostazioni predefinite. Se richiesto, esse possono essere modificate nella scheda **Impostazioni** della finestra di revisione delle proprietà del pacchetto d'installazione (vedere Figura 21).

Il gruppo di campi **Connessione ad Administration Server** contiene le impostazioni utilizzate da Network Agent una volta installato sui computer client per connettersi ad Administration Server (per impostazione predefinita, durante la creazione verranno utilizzati i valori del server corrente).

- Indirizzo del computer sul quale è installato Administration Server.
- Numero di porta utilizzato per la connessione non protetta ad Administration Server. Per impostazione predefinita, viene utilizzata la porta **14000**. Se questa porta è già occupata, si può utilizzarne un'altra.
- Numero della porta utilizzata per la connessione protetta ad Administration Server tramite il protocollo SSL. Per impostazione predefinita, viene utilizzata la porta **13000**.

È consentita solo la rappresentazione decimale.

- File certificato per autenticare l'accesso ad Administration Server. Il valore di questa impostazione è determinato dalla casella **Usa il certificato del server**.

Se la casella non è selezionata per impostazione predefinita, il file certificato verrà ottenuto automaticamente da Administration Server quando Agent si connette ad esso per la prima volta.

Se la casella **Usa il certificato del server** è selezionata, l'autenticazione verrà eseguita in base al file certificato specificato tramite il pulsante **Sfoggia**. L'estensione di questo file è **.cer** ed è ubicato nella cartella **Cert** della cartella d'installazione di Kaspersky Administration Kit. È possibile cambiare file certificato selezionando il file richiesto tramite il pulsante **Sfoggia**.

- La porta che verrà utilizzata da Network Agent per la connessione al Server: semplice o protetta. Il valore di questa impostazione è determinato dalla casella **Usa connessione SSL**. Se la casella è selezionata, la connessione viene eseguita su una porta protetta tramite il protocollo SSL; se la casella non è selezionata, la connessione viene eseguita su una porta non protetta.

- Le impostazioni di connessione del server proxy. Se Network Agent utilizza un server proxy per la connessione al Server, selezionare la casella **Utilizza server proxy**. Dopodiché, scegliere il pulsante **Impostazioni** immettere nella finestra che viene visualizzata l'indirizzo, il nome utente e la password per il server proxy.

Una volta installato Network Agent è possibile modificare il valore delle impostazioni utilizzate per la connessione a Administration Server tramite la regola e le impostazioni dell'applicazione.

Se Network Agent viene reinstallato in remoto sul computer client, i valori delle impostazioni utilizzate per la connessione al Server ed al certificato Administration Server saranno sostituite da quelli nuovi.

Nel gruppo di campi **Assegnazione di computer a gruppi**, verrà definito un sottogruppo del gruppo **Rete** al quale verranno aggiunti i computer dopo che Network Agent sia stato installato su di essi. È possibile selezionare una delle seguenti opzioni:

- aggiungi i computer alle cartelle **Corrispondenti alla posizione del computer nella rete Windows**: dominio o gruppo di lavoro (questa opzione è selezionata per impostazione predefinita);
- aggiungi tutti i computer **Al gruppo** specificato nel campo d'immissione. Se si seleziona questa opzione, immettere il nome della cartella nel campo sottostante. Se il gruppo **Rete** non contiene tale cartella, essa verrà creata (è anche possibile indicare il nome di qualsiasi cartella esistente nel gruppo **Rete**).

La cartella verrà utilizzata per memorizzare solo i computer di nuova rilevazione sulla rete. Se il computer non era stato rilevato da Administration Server ed inserito nella cartella corrispondente alla sua posizione nella rete, prima dell'installazione di Network Agent. I computer rilevati nella rete prima dell'installazione di Network Agent resteranno nella loro vecchia posizione nel gruppo **Rete**.

Dopo l'installazione di Network Agent, non è possibile modificare la cartella per memorizzare i computer nel gruppo **Rete**, poiché questa impostazione non è inclusa nella regola e nelle impostazioni dell'applicazione.

Network Agent viene installato sul computer come servizio, con il seguente insieme di attributi:

- nome servizio **KLNagent**;
- nome visualizzato **Kaspersky Network Agent**;
- avvio automatico all'avvio del sistema operativo;
- con l'account **Sistema locale**.

È possibile rivedere le proprietà del servizio **Kaspersky Network Agent**, avviarlo, arrestarlo e monitorare il suo funzionamento tramite gli strumenti di amministrazione standard di Windows - **Gestione computer** → **Servizi**.

#### 4.1.4. Creazione di un'attività per distribuire il pacchetto d'installazione sugli Administration Server slave

Per creare l'attività di distribuzione del pacchetto d'installazione sugli Administration Server slave:

1. Connettersi all'Administration Server richiesto.
2. Selezionare il nodo **Attività globali** nell'albero della console, aprire il menu di scelta rapida e selezionare il comando **Nuovo** → **Attività**, oppure utilizzare la voce analoga dal menu **Azione**. Ciò avvierà la procedura guidata. Seguire le istruzioni.
3. Per l'applicazione Kaspersky Administration Kit, selezionare il tipo di attività **Distribuzione del pacchetto di installazione**.
4. Nella finestra successiva della procedura guidata (vedere Figura 24), selezionare il pacchetto d'installazione da distribuire. Selezionare una delle seguenti opzioni:
  - **Tutti i pacchetti d'installazione.**
  - **Pacchetti d'installazione selezionati.** In questo caso, selezionare le caselle accanto ai nomi dei pacchetti d'installazione richiesti nella tabella sottostante.

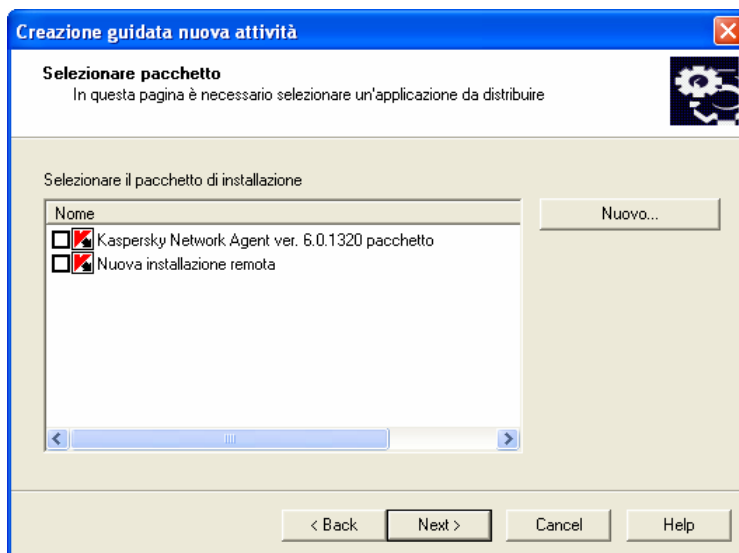


Figura 24. Creazione di un set di pacchetti d'installazione

Specificare il valore richiesto nel campo **Numero massimo di installazioni condivise**.

5. Nella finestra successiva della procedura guidata (vedere Figura 25), selezionare le caselle accanto ai nomi degli Administration Server slave ai quali devono essere distribuiti i pacchetti d'installazione.

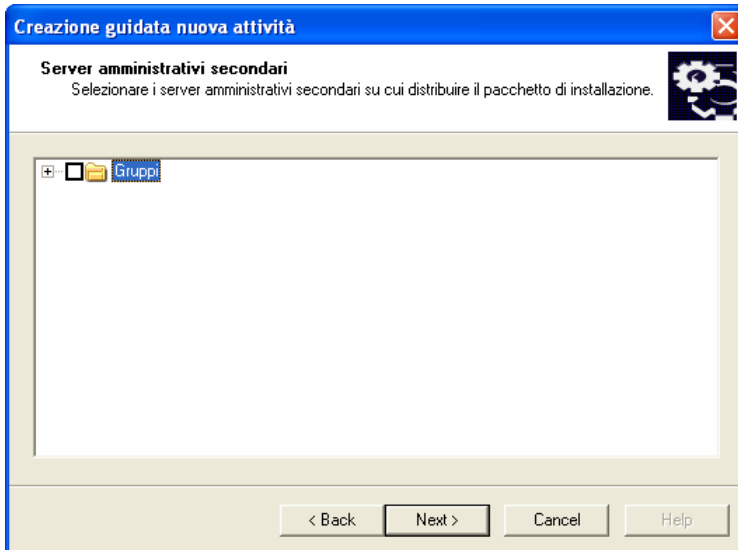


Figura 25. Selezione degli Administration Server slave

6. Determinare quindi con quale account verrà lanciata l'attività sui computer (per dettagli vedere la sezione 4.1.6 a pagina 51).
7. Nelle finestra successiva della procedura guidata, specificare il piano di lancio dell'attività (per dettagli vedere la sezione 4.1.6 a pagina 51).
8. Per uscire dalla procedura guidata una volta terminata, scegliere il pulsante **Fine**.

## 4.1.5. Distribuzione dei pacchetti d'installazione in un gruppo tramite Network Agent

Per distribuire i pacchetti d'installazione in un gruppo, è possibile utilizzare gli agenti di aggiornamento. Gli agenti di aggiornamento ricevono i pacchetti d'installazione da Administration Server e li salvano nella cartella d'installazione delle applicazioni di Kaspersky Lab.

L'ubicazione della cartella che contiene gli aggiornamenti e i pacchetti d'installazione non può essere modificata; né è possibile limitarne le dimensioni

In seguito, i pacchetti d'installazione verranno distribuiti ai computer client tramite la consegna a più indirizzi. La consegna dei nuovi pacchetti d'installazione in un

gruppo viene eseguita solo una volta. Se al momento della consegna un computer client è scollegato dalla rete logica aziendale, quando viene lanciata l'attività di installazione Network Agent scaricherà automaticamente il pacchetto d'installazione richiesto dall'agente di aggiornamento.

*Per creare l'elenco di agenti di aggiornamento e configurarli per distribuire i pacchetti d'installazione ai computer di un gruppo,*

1. Connettersi all'Administration Server richiesto.
2. Selezionare il gruppo richiesto nell'albero della console, aprire il menu di scelta rapida e selezionare il comando **Proprietà**, oppure utilizzare la voce analoga dal menu **Azione**.
3. Nella finestra delle proprietà del gruppo che si aprirà, sulla scheda **Agenti di aggiornamento** (vedere Figura 26), creare l'elenco di computer che agiranno come agenti di aggiornamento nel gruppo tramite i pulsanti **Aggiungi** e **Rimuovi**.

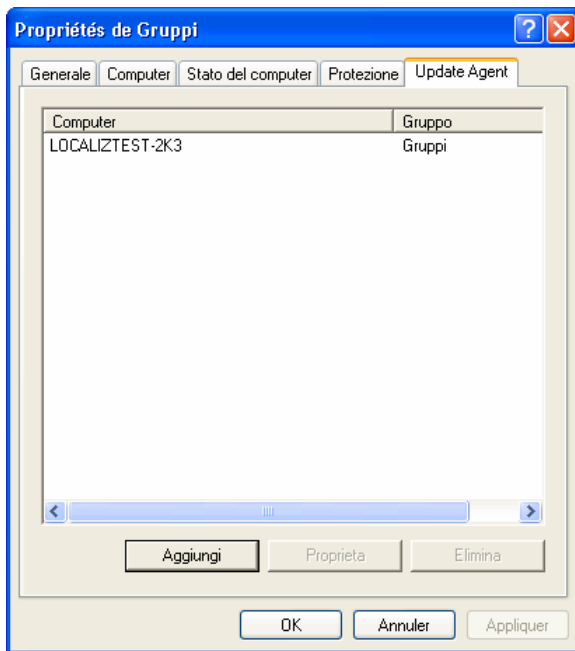


Figura 26. La finestra delle proprietà del gruppo.  
La scheda **Agenti di aggiornamento**

4. Modificare le impostazioni del server di aggiornamento. Per fare ciò, selezionare l'agente dall'elenco e scegliere il pulsante **Proprietà**. Nella

finestra **Proprietà <Nome agente di aggiornamento>** che si aprirà (vedere Figura 27) effettuare le seguenti operazioni:

- specificare il numero della porta che verrà utilizzata dal client per la connessione all'agente di aggiornamento. Il numero predefinito della porta è **14001**. Se questa porta è già utilizzata, si può utilizzarne un'altra.
- specificare il numero della porta utilizzata dal computer client per la connessione protetta all'agente di aggiornamento tramite il protocollo SSL. Il numero predefinito della porta è **13001**;

selezionare la casella **Usa consegna IP a più indirizzi** e compilare i campi **Indirizzo IP di consegna** e **Numero porta IP-MULTICAST**.

5. Scegliere il pulsante **Applica** o quello **OK**.

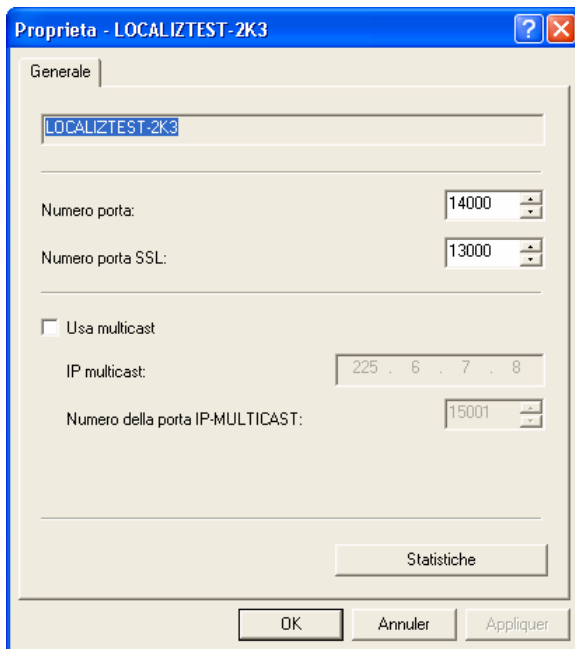


Figura 27. Finestra delle proprietà dell'agente di aggiornamento

---

## 4.1.6. Creazione di un'attività di installazione remota

Quando quest'attività viene eseguita, l'installazione remota del software sul computer client viene eseguita utilizzando uno dei seguenti due metodi: **installazione forzata** oppure **installazione tramite lo scenario di avvio**.

L'**installazione forzata** consente di eseguire l'installazione remota di software sul computer client specifico della rete logica. Quando viene eseguita l'attività, Administration Server copierà dalla cartella condivisa l'insieme di file richiesti per installare l'applicazione su ciascun computer client nella cartella temporanea e lancia il programma d'installazione su ciascun computer. Per eseguire con successo l'attività d'installazione forzata, Administration Server deve disporre dei diritti dell'amministratore locale sul computer client della rete logica. Questo metodo è consigliato per installare applicazioni su computer che eseguono Microsoft Windows NT/2000/2003/XP e che supportano tale capacità, oppure su computer che eseguono Microsoft Windows 98/Me su cui sia installato Network Agent.

Se la connessione tra Administration Server ed il computer client viene stabilita tramite Internet o è protetta da un firewall, le cartelle condivise non possono essere utilizzate per trasferire i dati. In questo caso, i file richiesti per installare l'applicazione sul computer client possono essere trasmessi tramite Network Agent. Network Agent viene installato su ciascuno di questi computer a livello locale.

Il secondo metodo - l'**installazione tramite lo scenario di avvio** - consente di assegnare un'attività d'installazione remota all'account di un utente specifico (o di diversi utenti). In conseguenza dell'esecuzione dell'attività, nello scenario di avvio verrà incluso un record relativo al lancio del programma d'installazione per gli utenti selezionati. Il programma d'installazione è ubicato nella cartella condivisa di Administration Server. Per garantire l'esecuzione dell'attività con successo, l'account utilizzato per lanciarla o Administration Server deve avere il diritto di modificare gli scenari di avvio nel database del controller di dominio. In conseguenza della registrazione dell'utente nel dominio, verrà effettuato un tentativo di installare l'applicazione sul computer client da cui è stato registrato l'utente. Questo metodo è consigliato per l'installazione delle applicazioni Kaspersky Lab sui computer che eseguono MS Windows 98/Me.

Per garantire l'esecuzione con successo dell'attività di installazione remota utilizzando lo scenario di avvio, gli utenti per i quali vengono apportate modifiche agli scenari devono disporre dei diritti di amministratore locale sui rispettivi computer.

Le attività di gruppo per l'installazione remota di software sui computer client vengono eseguite utilizzando esclusivamente l'installazione forzata. Durante la creazione di un'attività globale, è possibile selezionare il metodo richiesto: l'installazione forzata o l'installazione tramite lo scenario di avvio.

*Per creare un'attività globale per l'installazione remota tramite il metodo di installazione forzata:*

Connettersi alla copia di Administration Server richiesta.

1. Selezionare il nodo **Attività globali** nell'albero della console, aprire il menu di scelta rapida e selezionare il comando **Nuovo / Attività** utilizzare la voce analoga dal menu **Azione**. Verrà avviata la creazione guidata di un'attività. Seguire le istruzioni visualizzate.
2. Specificare il nome dell'attività.
3. Quando si seleziona l'applicazione ed il tipo di attività (vedere Figura 28), specificare i valori **Kaspersky Administration Kit** e **Attività gestione del prodotto**.

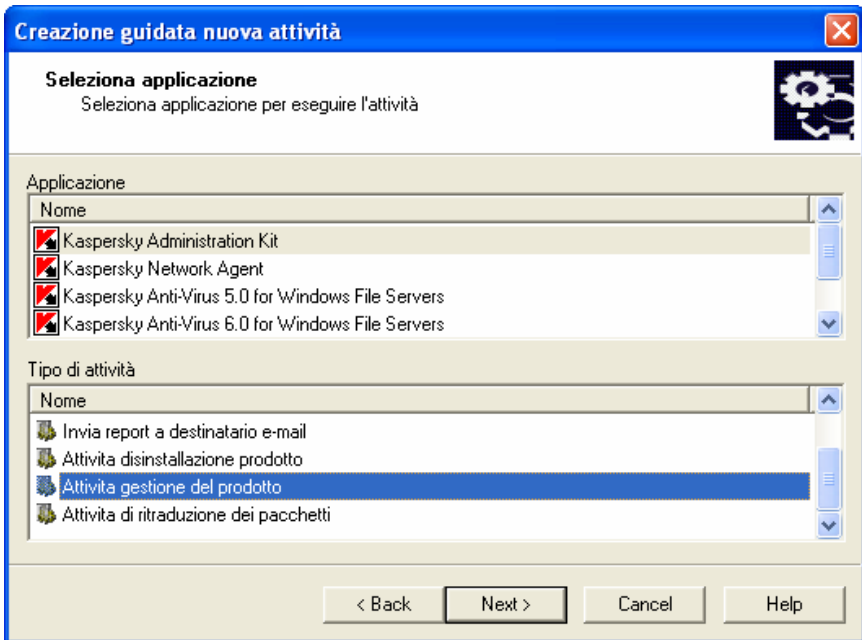


Figura 28. Specificare il tipo di attività

4. Dopodiché, specificare il pacchetto d'installazione che verrà installato durante l'esecuzione dell'attività (vedere Figura 29). Selezionare il

pacchetto richiesto dai pacchetti creati per l'Administration Server specifico, oppure creare un nuovo pacchetto tramite il pulsante **Nuovo....**

Alcune applicazioni che supportano l'amministrazione tramite Kaspersky Administration Kit possono essere installate sui computer solo localmente. Per informazioni dettagliate, vedere le Guide relative alle applicazioni corrispondenti.

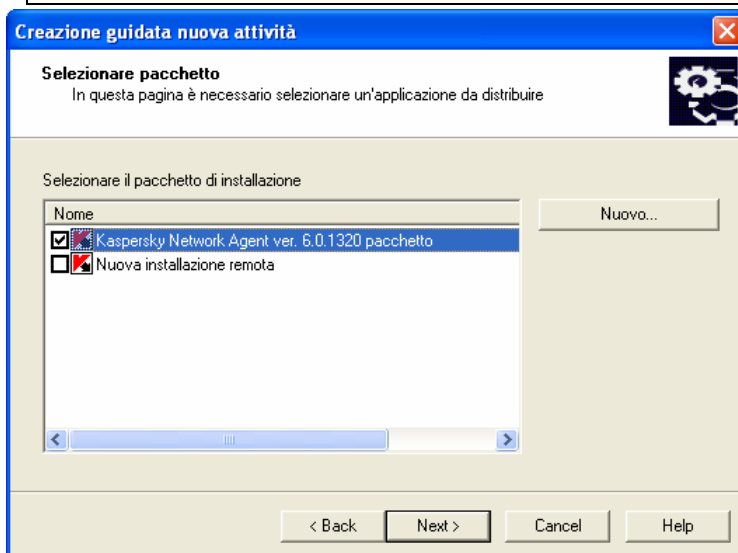


Figura 29. Selezione del pacchetto d'installazione da installare

5. In questa fase, selezionare l'opzione **Installazione Push** (vedere Figura 30)

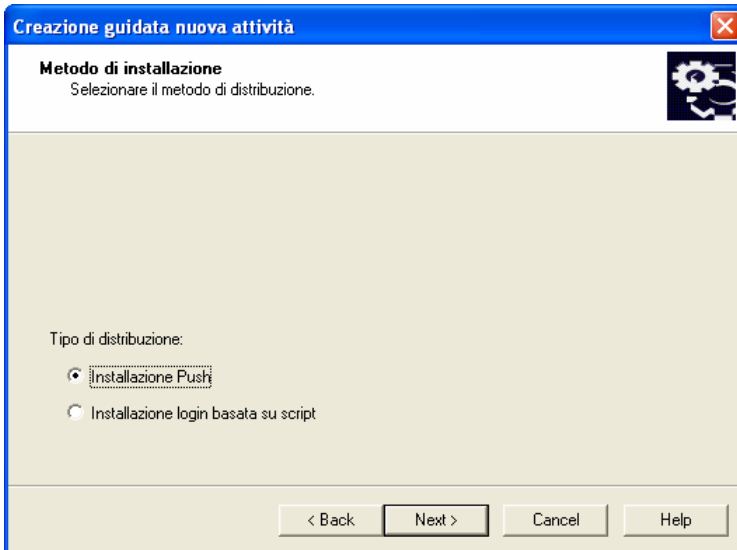


Figura 30. Selezione del metodo d'installazione

6. In questa finestra della procedura guidata (vedere Figura 31), verrà proposto di determinare ulteriori opzioni d'installazione:

- Se l'applicazione debba essere reinstallata se è già stata installata sul computer.

Selezionare la casella **Non reinstallare l'applicazione se è già installata** per prevenire installazioni ripetute (per impostazione predefinita la casella è selezionata). In questo caso, per i computer sui quali l'applicazione è installata localmente o come risultato del lancio dell'attività di installazione remota precedentemente pianificata, l'attività non verrà eseguita.

Se la casella non è selezionata, l'attività di installazione remota verrà lanciata secondo quanto pianificato, fino al raggiungimento del numero massimo di tentativi di installazione dell'applicazione.

- Il metodo di trasmissione dei file richiesti per installare l'applicazione sui computer client.

Per fare ciò, effettuare le seguenti operazioni nel gruppo di campi **Download del pacchetto di installazione**:

- Selezionare la casella **Usando le risorse di Microsoft Windows dalla cartella ad accesso pubblico** se si desidera che il trasferimento dei file richiesti per installare l'applicazione sui computer client venga eseguito utilizzando gli strumenti di Windows e le cartelle condivise (per impostazione predefinita questa casella è selezionata).
- Selezionare la casella **Usando Administration Agent** in modo che i file vengano trasmessi ai computer client tramite la copia di Network Agent installato su ciascun computer (questa casella è selezionata per impostazione predefinita).
- Nel campo **Numero massimo di download simultanei**, specificare il numero massimo di computer client che possono scaricare informazioni da Administration Server.
- Specificare il numero di tentativi di installazione in caso di lancio di un'attività pianificata, inserendo il valore desiderato nel campo **Numero di tentativi**. In caso di errore durante la precedente installazione, verranno ripetuti diversi tentativi.

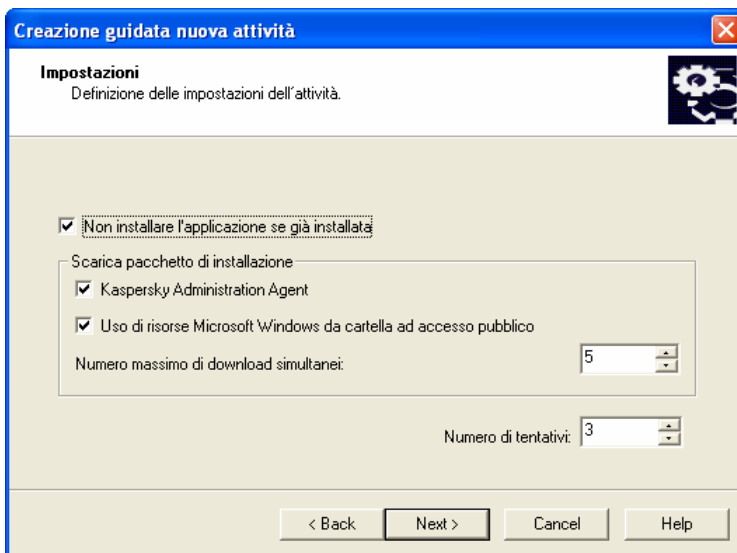


Figura 31. Impostazioni supplementari d'installazione

7. Durante questa fase verrà proposto di installare Network Agent unitamente all'applicazione.

Si consiglia di utilizzare l'installazione congiunta per ridurre il carico su Administration Server. Per fare ciò, selezionare la casella **Installa con Administration Agent** e selezionare la casella accanto al nome del pacchetto d'installazione richiesto. Se richiesto, creare un nuovo pacchetto d'installazione tramite il pulsante **Crea**.

Determinare il metodo di selezione dei computer sui quali verrà creata l'attività (vedere Figura 32):

- **Selezionare i computer tramite le funzioni di rete di Windows.** In tal caso, i computer per l'installazione verranno selezionati in base ai dati ricevuti da Administration Server, secondo il polling della rete aziendale di Windows.
- **Definire gli indirizzi IP dei computer.** In tal caso, i computer per l'installazione verranno selezionati manualmente.

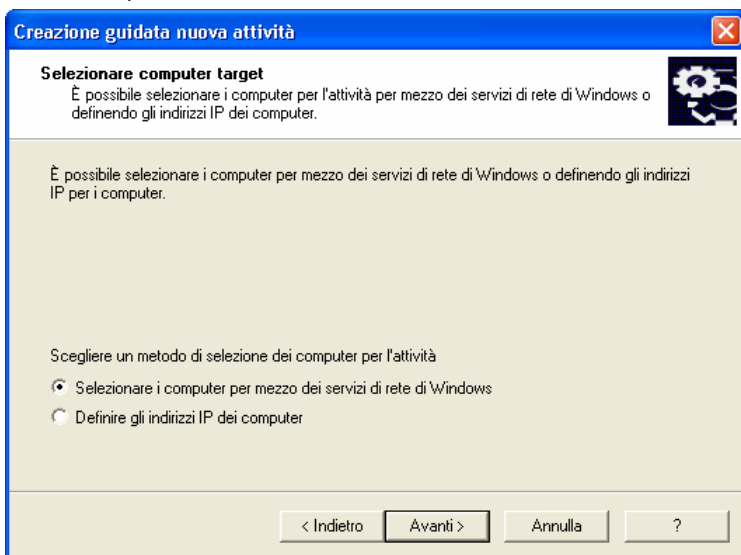


Figura 32. Selezione del metodo da utilizzare per scegliere i computer client

Se la selezione dei computer avviene in base ai dati risultanti dal polling di rete di Windows, l'elenco verrà creato nella finestra della procedura guidata (vedere Figura 33) e tale selezione verrà eseguita come quando si aggiungono computer alla rete logica (per dettagli, vedere il Manuale di riferimento per Kaspersky Administration Kit). È possibile selezionare i computer della rete logica (la cartella **Gruppi**) o i computer che non sono ancora stati inclusi nella rete logica (la cartella **Rete**).

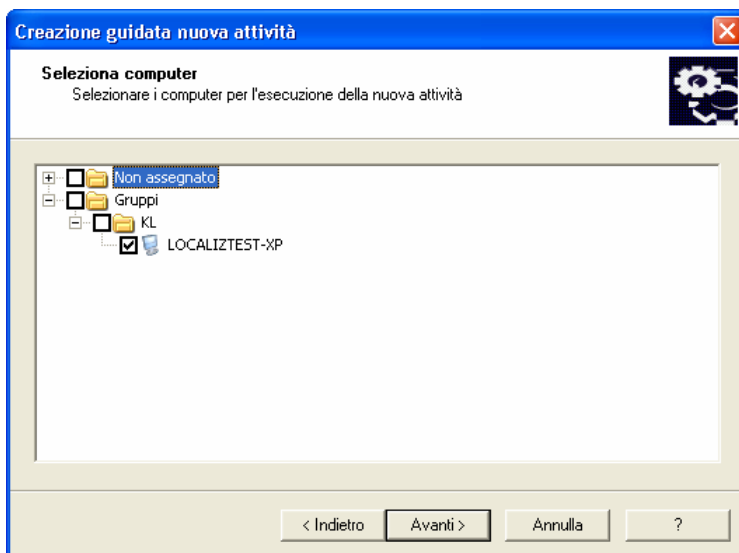


Figura 33. Creazione dell'elenco di computer per l'installazione sulla base dei dati della rete Windows

Se si selezionano i computer manualmente, l'elenco viene creato immettendo i nomi NETBIOS o DNS, gli indirizzi IP (o un intervallo di indirizzi IP) dei computer, o importando l'elenco da un file *txt* nel quale ciascun indirizzo deve essere inserito in una nuova riga (vedere Figura 34).

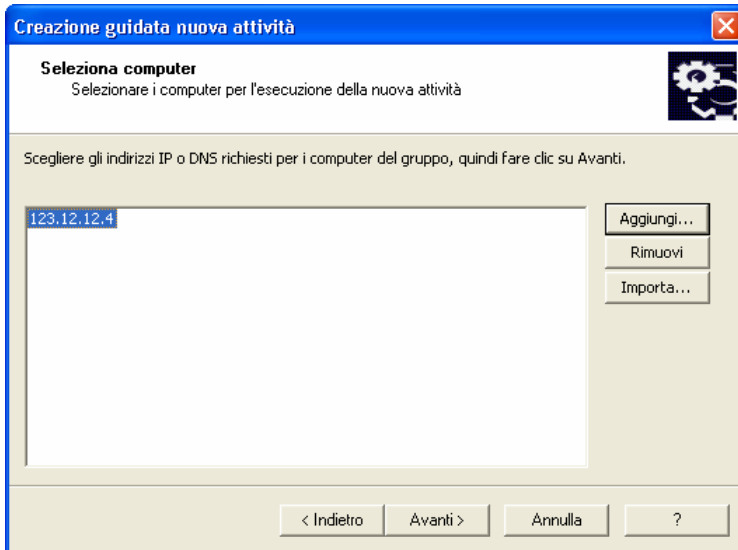


Figura 34. Creazione dell'elenco di computer per l'installazione in base agli indirizzi IP

8. Nella successiva finestra della finestra guidata, specificare con che account l'attività di distribuzione deve essere lanciata sui computer (vedere Figura 35).

L'account deve disporre di diritti di amministratore per tutti i computer sui quali s'intende eseguire l'installazione remota di software.

Quando il software viene installato su computer facenti parte di diversi domini, tra tali domini ed il dominio nel quale opera Administration Server deve sussistere una relazione di affidabilità.

Selezionare una delle seguenti opzioni:

- **Account predefinito** - se Administration Server viene eseguito con l'account dell'utente di dominio (vedere la sezione 3.2 a pagina 16) e tale account dispone dei diritti richiesti per installare il software.
- **Account specificato**- se Administration Server viene eseguito con l'account di sistema o se l'account di Administration Server non dispone dei diritti richiesti per lanciare l'attività di distribuzione.

Per installare in remoto il software sui computer non inclusi nel dominio, lanciare l'attività di installazione remota con l'account di un utente che disponga dei diritti di amministratore su tali computer.

Specificare nei campi forniti sotto gli attributi dell'utente il cui account è conforme ai requisiti richiesti.

Creazione guidata nuova attività

**Account**  
In questa pagina è possibile definire l'account utente in cui avviare l'attività

Account predefinito

Account specificato

Esegui come utente:

Password:

Conferma password:

< Indietro   Avanti >   Annulla   ?

Figura 35. Selezione dell'account

9. Quindi, pianificare il lancio dell'attività (vedere Figura 36).
  - Selezionare la modalità di esecuzione dell'attività dall'elenco a discesa **Esecuzione pianificata**:
    - **Manuale**
    - **Ogni N ore**
    - **Giornaliera**
    - **Settimanale**
    - **Mensile**
    - **Una sola volta** (in tal caso, l'attività di distribuzione verrà eseguita solo una volta sul computer, a prescindere dai risultati della sua esecuzione).

- **Immediatamente** (subito dopo la creazione dell'attività ed il completamento della procedura guidata).
- Configurare le impostazioni di pianificazione nel gruppo di campi in base alla modalità selezionata (per dettagli, vedere la guida di riferimento di Kaspersky Administration Kit).

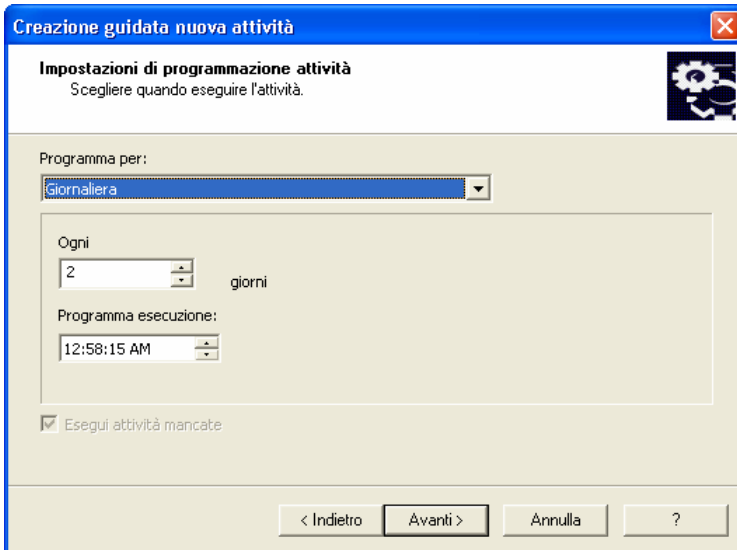


Figura 36. Esecuzione quotidiana dell'attività

*Per creare un'attività di distribuzione globale tramite lo scenario di avvio:*

1. Connettersi all'Administration Server richiesto.
2. Selezionare il nodo **Attività globali** nell'albero della console, aprire il menu di scelta rapida e selezionare il comando **Nuovo / Attività** o utilizzare la voce analoga dal menu **Azione**. Verrà avviata la creazione guidata di un'attività. Seguire le istruzioni.
3. Specificare il nome dell'attività.
4. Quando si seleziona l'applicazione ed il tipo di attività (vedere Figura 28), selezionare rispettivamente **Kaspersky Administration Kit** e **Installazione remota applicazione**.
5. Nella finestra successiva (vedere Figura 29), specificare il pacchetto d'installazione da utilizzare per l'installazione. Ciò viene eseguito come nel caso dell'installazione forzata (vedere sopra).

6. Dopodiché, selezionare l'opzione **Installazione tramite lo scenario di avvio** (vedere Figura 30)
7. Nella successiva finestra della procedura guidata (vedere Figura 34), selezionare gli account degli utenti per i quali è necessario modificare lo scenario di avvio.

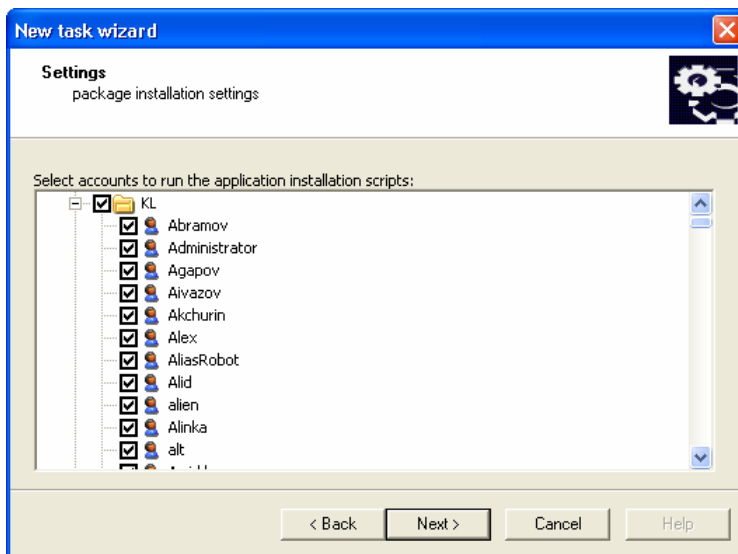


Figura 37. Selezione degli account

8. Durante la fase successiva della procedura guidata (vedere Figura 35), analogamente all'utilizzo del metodo di installazione forzata (vedere sopra),
9. Pianificando l'esecuzione dell'**Attività** (vedere Figura 36) creare un piano nello stesso modo in cui viene creato per l'installazione forzata (vedere sopra).

Al termine della procedura guidata, l'attività di distribuzione creata verrà aggiunta al nodo **Attività globali** e visualizzata nel riquadro dei risultati. Se richiesto, è possibile modificare le sue impostazioni (per dettagli, vedere la sezione 4.1.7 a pagina 62).

*Per fare ciò,*

selezionare il nodo **Installazione remota** nell'albero della console, selezionare il pacchetto d'installazione richiesto nel riquadro dei risultati e selezionare il comando **Installa** o utilizzare il comando analogo dal menu

**Azione.** Ciò lancerà la creazione guidata dell'attività di distribuzione descritta sopra, tuttavia, essa non includerà le fasi relative alla selezione del tipo di attività e del pacchetto d'installazione. Seguire le istruzioni.

In alternativa, è possibile lanciare la creazione guidata di un'attività di distribuzione di gruppo.

*Per fare ciò,*

selezionare il nodo **Gruppi** nell'albero della console, aprire il menu di scelta rapida e selezionare il comando **Installa** oppure utilizzare il comando analogo dal menu **Azione**. Ciò lancerà la creazione guidata dell'attività di distribuzione di gruppo descritta sopra, tuttavia, essa non includerà le fasi relative alla selezione del tipo di attività e del gruppo di computer. Seguire le istruzioni.

## 4.1.7. Configurazione dell'attività di distribuzione

Le attività di distribuzione vengono configurate in maniera analoga a qualsiasi altra attività (per dettagli, vedere il Manuale di riferimento per Kaspersky Administration Kit). Di seguito verranno trattate in dettaglio le impostazioni specifiche per questo tipo di attività offerte dalla scheda **Impostazioni**.

Se si sta modificando un'attività che prevede l'installazione forzata (vedere la figura 38), è possibile:

- determinare se reinstallare l'applicazione in caso essa sia già installata sul computer client;
- specificare il metodo da utilizzare per trasmettere i file richiesti per installare l'applicazione sul computer client, nonché il numero massimo di connessioni simultanee;
- specificare il numero di tentativi di installazione se l'attività viene eseguita secondo quanto pianificato.

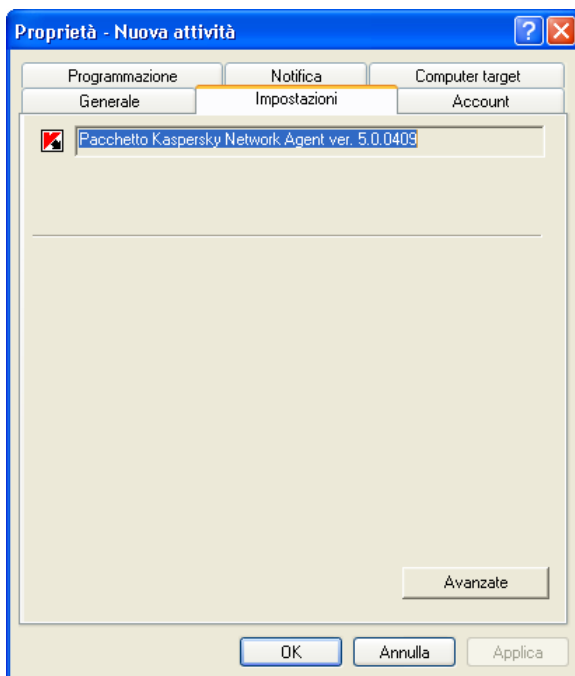


Figura 38. Configurazione di un'attività di distribuzione  
Metodo d'installazione forzata

Quando si configura un'attività di distribuzione utilizzando uno scenario di avvio, è possibile utilizzare la scheda **Impostazioni** per modificare l'elenco di account utente per i quali verrà modificato lo scenario di avvio (vedere Figura 39). Per modificare l'elenco, usare i pulsanti **Aggiungi** e **Rimuovi**.

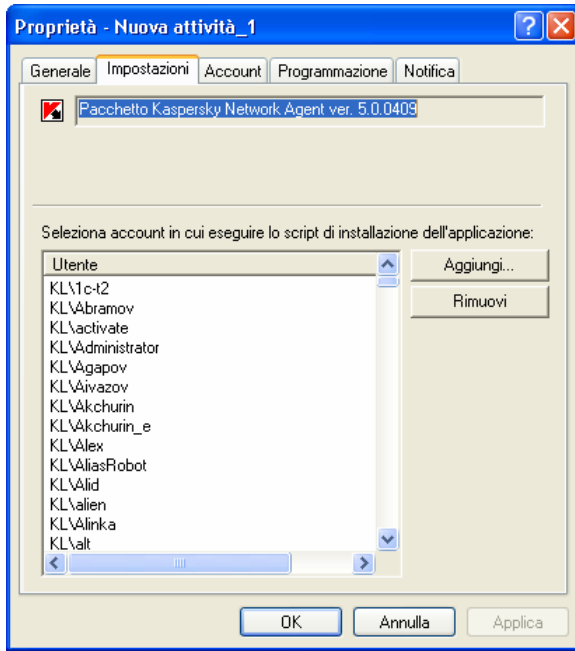


Figura 39. Configurazione di un'attività di distribuzione tramite lo scenario di avvio.

## 4.1.8. Rimozione remota di software

*Per rimuovere software in remoto:*

Creare un'attività in maniera analoga alla creazione di un'attività di distribuzione (vedere la sezione 4.1.6 a pagina 51); selezionare **Rimozione remota applicazione** come tipo di attività e selezionare l'applicazione Kaspersky Lab desiderata dall'elenco a discesa **Applicazione da rimuovere** nella finestra **Applicazione** (vedere la figura 40). Per rimuovere un'applicazione di terzi, selezionare la casella **Applicazione di terze** selezionare l'applicazione da rimuovere.

L'elenco a discesa contiene l'elenco di applicazioni rilevate sui computer delle reti logiche dopo l'installazione di Network Agent su tali computer.

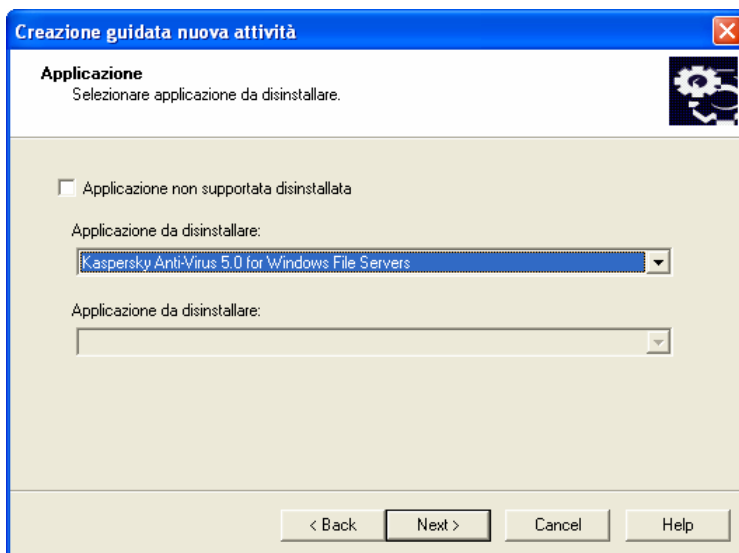


Figura 40. Selezione di un'applicazione da rimuovere

L'attività creata verrà eseguita secondo quanto pianificato.

## 4.2. Distribuzione guidata

La distribuzione guidata può essere utilizzata per installare le applicazioni Kaspersky Lab. Essa consente di implementare le applicazioni tramite il metodo di installazione forzata, utilizzando un pacchetto di installazione creato o direttamente dal pacchetto di distribuzione.

La procedura guidata esegue le seguenti operazioni:

- creazione di un pacchetto d'installazione per installare l'applicazione (se tale pacchetto non è stato creato in precedenza). Il pacchetto viene memorizzato nel nodo **Installazione remota** con un nome corrispondente al nome ed alla versione dell'applicazione, e può essere utilizzato per installare l'applicazione in seguito.
- creazione ed esecuzione di attività di distribuzione globali e di gruppo. L'attività creata verrà ubicata nella cartella **Attività globali** o **Attività di gruppo** del gruppo per il quale l'attività è stata creata, e può essere eseguita manualmente in seguito. Il nome dell'attività corrisponde al nome del pacchetto per l'installazione dell'applicazione: **Installazione <Nome del pacchetto d'installazione selezionato>**.

Per installare l'applicazione tramite la distribuzione guidata:

1. Connettersi all'Administration Server richiesto.
2. Nell'albero della console della finestra principale dell'applicazione Kaspersky Administration Kit, selezionare il nodo corrispondente all'Administration Server richiesto, aprire il menu di scelta rapida e selezionare il comando **Distribuzione guidata**, oppure utilizzare il comando analogo dal menu **Azione**. Ciò avvierà la procedura guidata. Seguire le istruzioni.
3. Nella finestra che si aprirà (vedere Figura 41), specificare il pacchetto d'installazione che verrà installato. Se si sta installando l'applicazione da un pacchetto di distribuzione e/o se il pacchetto d'installazione non è stato creato, crearne uno nuovo. Per fare ciò, scegliere il pulsante **Nuovo...**; si aprirà la creazione guidata di un pacchetto d'installazione (vedere la sezione 4.1.1 a pagina 36).

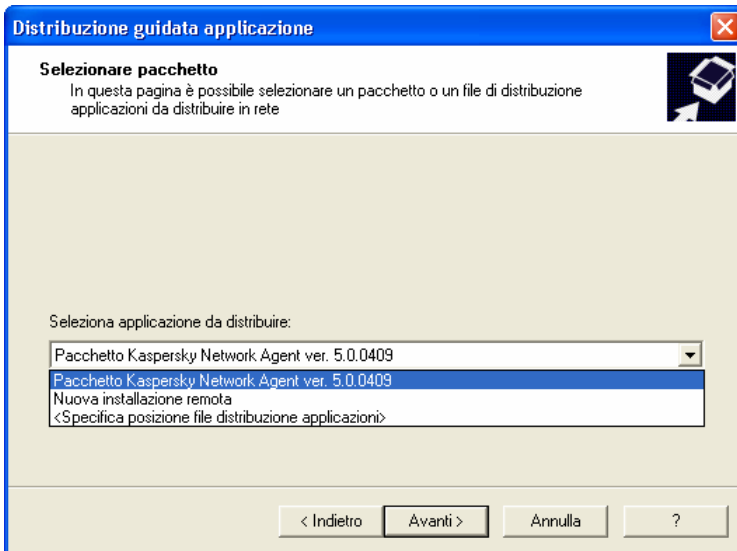


Figura 41. Selezione di un pacchetto d'installazione

4. Nella finestra successiva della procedura guidata, se richiesto, specificare il pacchetto d'installazione di Network Agent da installare congiuntamente (per dettagli vedere la sezione 4.1.6 a pagina 51).
5. Nella finestra della procedura guidata, determinare su quali computer verrà installata l'applicazione. Per fare ciò, selezionare una delle seguenti opzioni:

- **Installa l'applicazione sui computer selezionati**, se si seleziona questa opzione, una volta completata la procedura guidata verrà creata una attività globale di distribuzione dell'applicazione.
  - **Installa l'applicazione sui computer del gruppo amministrativo**- in conseguenza del lavoro della procedura guidata, verrà creata un'attività di gruppo.
6. Quindi, se si sta creando un'attività di gruppo, specificare il gruppo sui cui computer verrà installata l'applicazione in remoto (vedere Figura 42), oppure selezionare i computer per l'installazione. Se l'applicazione deve essere installata su tutti i computer client della rete logica, selezionare il gruppo **Gruppi**.

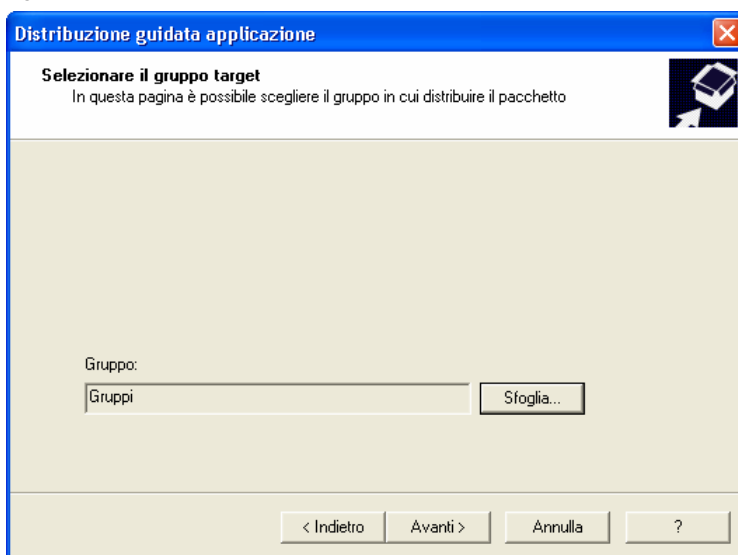
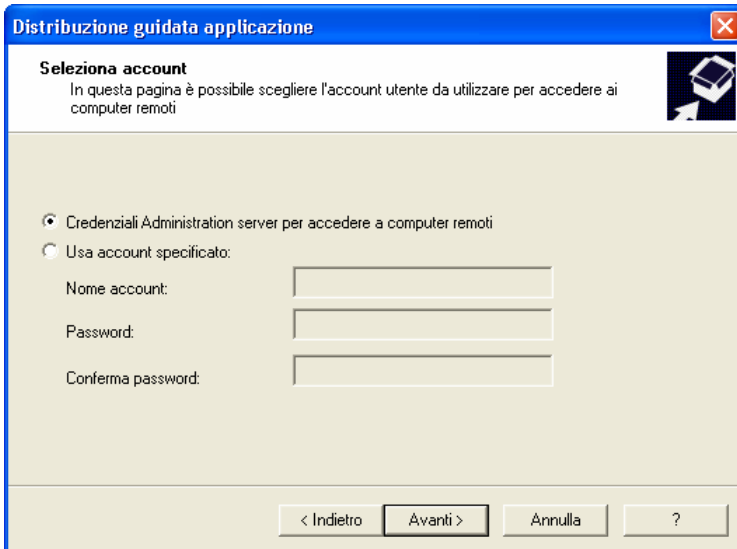


Figura 42. Selezione di un gruppo

7. Determinare quindi l'account per l'esecuzione dell'attività di distribuzione sui computer (per dettagli vedere la sezione 4.1.6a pagina 51).



The image shows a Windows-style dialog box titled "Distribuzione guidata applicazione" with a close button in the top right corner. The main heading is "Selezione account". Below it, a subtitle reads: "In questa pagina è possibile scegliere l'account utente da utilizzare per accedere ai computer remoti". To the right of this text is a small icon of a computer monitor with a mouse cursor pointing at it. There are two radio button options: the first is "Credenziali Administration server per accedere a computer remoti" (selected), and the second is "Usa account specificato:". Below the second option are three text input fields labeled "Nome account:", "Password:", and "Conferma password:". At the bottom of the dialog, there are four buttons: "< Indietro", "Avanti >", "Annulla", and "?".

Figura 43. Selezione di un account utente

8. Dopodiché, si aprirà una finestra che visualizzerà il processo di distribuzione ed esecuzione dell'attività di distribuzione sui computer del gruppo selezionato (vedere la figura 44). È possibile passare alla finestra finale della procedura guidata senza attendere il completamento del processo. Per fare ciò, premere il pulsante **Avanti**. È possibile visualizzare informazioni dettagliate sui risultati dell'esecuzione dell'attività tramite il pulsante **Cronologia**.

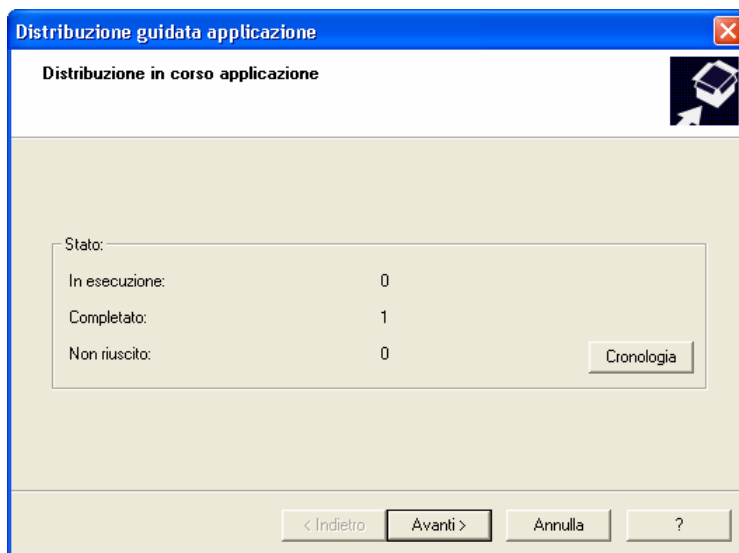


Figura 44. Esecuzione dell'attività di distribuzione

## 4.3. Installazione locale del software

L'installazione locale del software viene eseguita individualmente su ciascun computer. Per eseguire l'installazione locale, è necessario disporre dei diritti di amministratore per il computer locale.

Alcune applicazioni che supportano l'amministrazione tramite Kaspersky Administration Kit possono essere installate solo a livello locale. Per dettagli, vedere la guida per l'applicazione corrispondente.

La procedura generale per l'installazione di software durante la distribuzione locale del sistema di protezione antivirus può essere la seguente:

- Installare Network Agent e configurare la connessione tra il computer client e l'Administration Server (vedere la sezione 4.3.1 a pagina 70);
- installare le applicazioni richieste sul computer che verrà incluso nel sistema di protezione antivirus secondo quanto descritto nella corrispondente guida;
- installare il plugin di amministrazione per ciascuna delle applicazioni Kaspersky Lab installate sulla workstation dell'amministratore (vedere la sezione 4.3.2 a pagina 75).

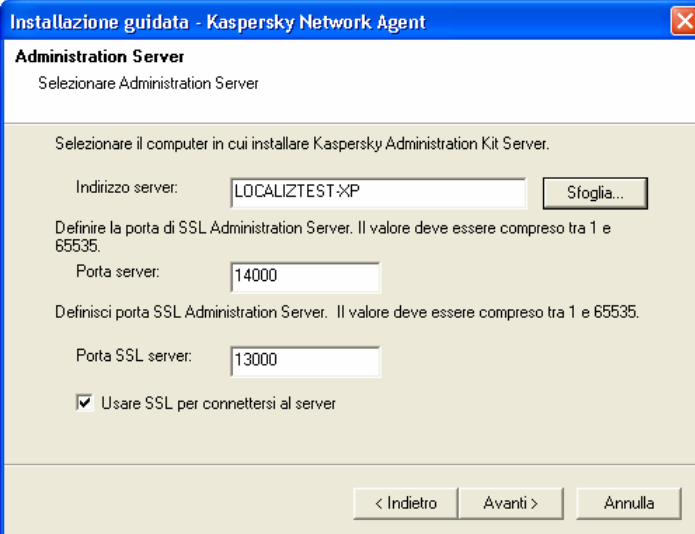
Kaspersky Administration Kit supporta l'installazione locale delle applicazioni in modalità non interattiva sulla base dei file creati durante la creazione del pacchetto d'installazione (vedere la sezione 4.3.3 a pagina 76).

## 4.3.1. Installazione locale di Network Agent

*Per installare localmente Network Agent sul computer:*

1. Eseguire il file **setup.exe** (o **setup.msi**) ubicato sul CD di distribuzione dell'applicazione Kaspersky Administration Kit nella cartella **NetAgent**. Il processo di installazione è reso più semplice da una procedura guidata. Quest'ultima propone di configurare le impostazioni di installazione. Seguire le istruzioni.
2. I primi passi del processo d'installazione consistono nella solita procedura, ed implicano la decompressione dei file richiesti dal pacchetto di distribuzione e la loro copiatura sul disco rigido del computer, l'accettazione del contratto di licenza e l'inserimento delle informazioni sull'utente e l'azienda.
3. Quindi, è necessario definire la cartella d'installazione di Network Agent. La cartella d'installazione predefinita è **Programmi\Kaspersky Lab\NetworkAgent**. Se questa cartella non esiste, verrà creata automaticamente. Per cambiare cartella, utilizzare il pulsante **Sfoglia...**
4. Nella finestra successiva dell'installazione guidata (vedere Figura 45), sarà necessario configurare le impostazioni utilizzate da Network Agent per connettersi a Administration Server. Per fare ciò, definire quanto segue:
  - Indirizzo del computer sul quale è o sarà installato Administration Server. Come indirizzo del computer si può utilizzare l'indirizzo IP o il nome del computer nella rete Windows. In alternativa, è possibile selezionare il computer tramite il pulsante **Sfoglia**.
  - il numero della porta utilizzata da Network Agent per connettersi a Administration Server. Per impostazione predefinita, verrà utilizzata la porta **14000**. Se è già stata assegnata, è possibile sceglierne un'altra. È consentita solo la rappresentazione decimale.
  - il numero della porta utilizzata per la connessione protetta all'Administration Server tramite il protocollo SSL. Per impostazione predefinita, verrà utilizzata la porta **13000**. Se è già stata assegnata, è possibile sceglierne un'altra. È

consentita solo la rappresentazione decimale. Per fare in modo che la connessione utilizzi una porta protetta (tramite il protocollo SSL), selezionare la casella **Usa SSL per la connessione al server**.



Installazione guidata - Kaspersky Network Agent

**Administration Server**

Selezionare Administration Server

Selezionare il computer in cui installare Kaspersky Administration Kit Server.

Indirizzo server: LOCALIZTEST-XP Sfoggia...

Definire la porta di SSL Administration Server. Il valore deve essere compreso tra 1 e 65535.

Porta server: 14000

Definisci porta SSL Administration Server. Il valore deve essere compreso tra 1 e 65535.

Porta SSL server: 13000

Usare SSL per connettersi al server

< Indietro Avanti > Annulla

Figura 45. Configurazione delle impostazioni utilizzate per connettersi ad Administration Server

- Se Network Agent si connette al Server tramite un server proxy (vedere la figura 46), configurare le corrispondenti impostazioni di connessione:
  - Selezionare la casella **Utilizza server proxy per la connessione a Administration Kit Server** ed immettere l'indirizzo ed il nome della porta per la connessione al server proxy. È consentita solo la rappresentazione decimale (ad esempio: **Indirizzo proxy:** proxy.test.com; **Porta:** 8080).
  - Se si utilizza una password per accedere al server proxy, compilare i campi **Login proxy** e **Password proxy**.
  - Se non si utilizza alcun server proxy, saltare questa fase tramite il pulsante **Avanti**.

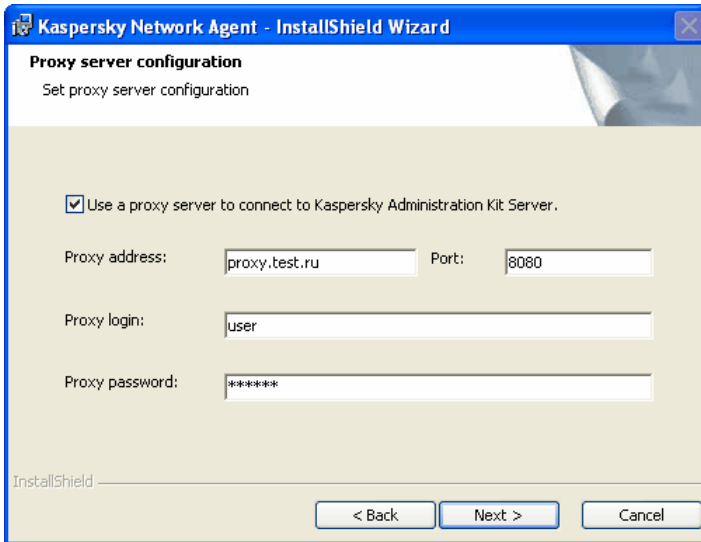


Figura 46. Configurazione della connessione tramite un server proxy

6. Dopodiché, determinare a quale cartella del gruppo **Rete** debba essere aggiunto il computer, una volta rilevato da Administration Server durante il polling della rete Windows. Selezionare una delle seguenti opzioni: (vedere la figura 47):
  - **Nome predefinito gruppo** - il computer verrà aggiunto alla cartella corrispondente alla sua posizione nella rete Windows network: dominio o workgroup (questa è l'opzione predefinita).
  - **Definire nome di gruppo** - il computer verrà aggiunto alla cartella specificata nel campo **Nome gruppo**. Se si seleziona questa opzione, immettere il nome della cartella. Se tale cartella non esiste nel gruppo **Rete**, verrà creata (è possibile specificare il nome di qualsiasi cartella esistente nel gruppo **Rete**).

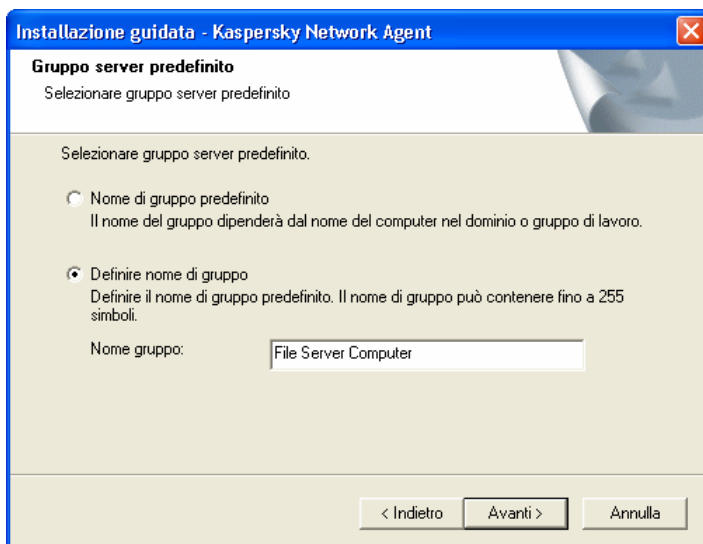


Figura 47. Selezione del gruppo nella cartella **Rete** per memorizzare i computer

7. Nella fase successiva (vedere Figura 48), specificare il metodo da utilizzare per ricevere il certificato dell'Administration Server al quale si collegherà Network Agent. Selezionare una delle seguenti opzioni:
- **Certificato predefinito** - il certificato di Administration Server verrà ricevuto quando Network Agent si connette ad esso per la prima volta (questa è l'opzione predefinita);
  - **Seleziona file certificato**- l'autenticazione su Administration Server verrà eseguita in base al certificato specificato dall'amministratore. Se si seleziona questa opzione, specificare il certificato di Administration Server da utilizzare.

Il file certificato ha estensione **.cer** ed è ubicato sull'Administration Server nella cartella **Cert** della cartella d'installazione di Kaspersky Administration Kit .

È possibile copiare il file certificato nella cartella condivisa o su un disco ed utilizzarne una copia per installare Network Agent.

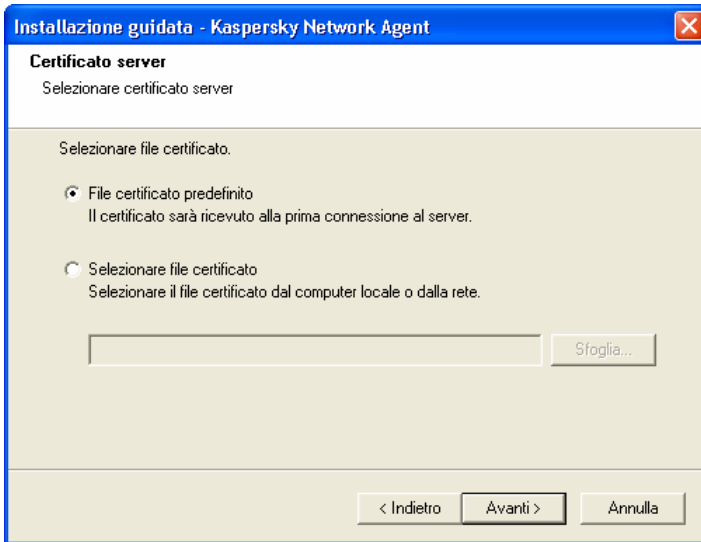


Figura 48. Selezione del metodo da utilizzare per ricevere il certificato Administration Server.

8. Nell'ultima finestra della procedura guidata (vedere Figura 49) verrà proposto di eseguire Network Agent subito dopo la chiusura della procedura guidata. Se si desidera eseguirlo successivamente, deselegionare la casella **Avvia Network Agent** selezionata per impostazione predefinita.

Se s'intende utilizzare il disco rigido del computer sul quale è installato Network Agent per creare un'immagine del disco e implementarla su altri computer, la casella **Avvia Network Agent** deve essere deselegionata.

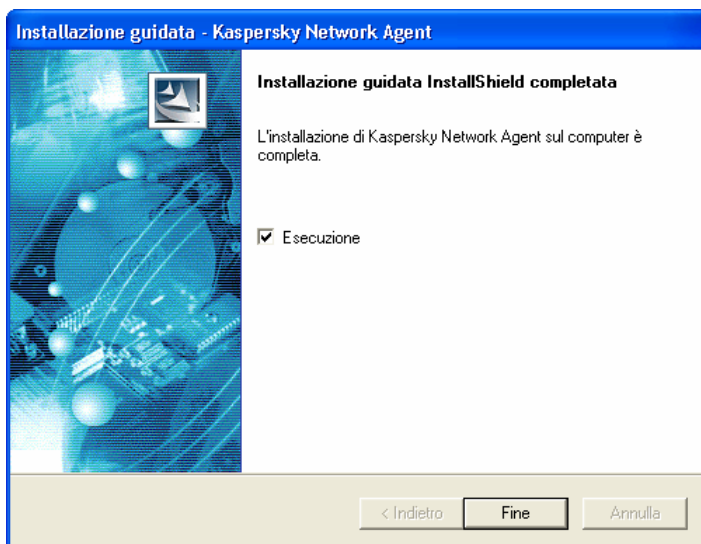


Figura 49. Configurazione dell'avvio di Network Agent

Al termine della procedura guidata, Network Agent sarà installato sul computer.

È possibile rivedere le proprietà del servizio **Kaspersky Network Agent**, avviarlo, arrestarlo o monitorarlo tramite gli strumenti standard di amministrazione di Windows - **Gestione computer**→ **Servizi**.

### 4.3.2. Installazione locale del plugin di amministrazione dell'applicazione

*Per installare il plugin di amministrazione dell'applicazione*

sul computer sul quale è installata la Administration Console, lanciare il file eseguibile **klcfginst.exe**, ubicato sul CD di distribuzione dell'applicazione. Questo file è incluso in tutte le applicazioni che possono essere amministrate tramite Kaspersky Administration Kit. L'installazione è facilitata da una procedura guidata. Essa proporrà di configurarne le impostazioni di installazione ed avviarla.

Il file del plugin di amministrazione per Network Agent **klcfginst.exe** è ubicato nella cartella **NetAgent** del pacchetto di distribuzione di Kaspersky Administration Kit

### 4.3.3. Installazione delle applicazioni in modalità non interattiva

*Per installare un'applicazione in modalità non interattiva:*

1. Creare il pacchetto d'installazione richiesto (vedere la sezione .1.1xx), se quello per l'applicazione che si desidera installare non è ancora stato creato.
2. Lanciare il file eseguibile **setup.exe** col modificatore **/s** incluso nel pacchetto di distribuzione dell'applicazione da installare, sul computer sul quale s'intende installare l'applicazione in modalità non interattiva.

I pacchetti d'installazione sono memorizzati su Administration Server nella cartella condivisa specificata durante la fase d'installazione di Administration Server, nella cartella di servizio **Pacchetti**.

---

# APPENDICE A. GLOSSARIO

Questa Guida utilizza alcuni termini specifici legati alla protezione antivirus. Il glossario è un elenco di definizioni di questi termini. Le voci del glossario sono disposte in ordine alfabetico per facilitare l'uso del glossario.

## A

**Aggiornamenti disponibili** – Service pack contenenti aggiornamenti urgenti accumulatisi nel tempo nonché le più recenti modifiche all'architettura dell'applicazione.

**Gruppo amministrativo**– Computer raggruppati secondo le loro applicazioni Kaspersky Lab funzionali ed installate. Il raggruppamento facilita significativamente la gestione e consente all'amministratore di gestire tutti i computer come un'entità singola. Un gruppo può comprendere altri gruppi. Le regole e le attività di gruppo possono essere create per ciascuna applicazione installata sui membri di un gruppo.

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

**Database antivirus** - database creato dagli specialisti di Kaspersky Lab, contenente descrizioni dettagliate di tutti i virus esistenti al momento della compilazione e dei metodi per la loro individuazione ed eliminazione. Le applicazioni antivirus utilizzano il database per rilevare e disinfectare con successo i virus. Il database antivirus disponibile sui siti Web di Kaspersky Lab viene regolarmente aggiornato alla comparsa di nuovi virus. Gli utenti registrati delle applicazioni Kaspersky Lab hanno accesso agli aggiornamenti del database. Per mantenere il computer costantemente protetto dai virus, si consiglia fortemente di scaricare gli aggiornamenti regolarmente.

**Workstation dell'amministratore** – Un computer sul quale è installata la Administration Console di Kaspersky Administration Kit. Tramite la Console, l'amministratore può costruire e gestire il sistema di protezione antivirus basato sulle applicazioni Kaspersky Lab.

**Stato della protezione antivirus** - Stato attuale della protezione antivirus, che caratterizza il livello di sicurezza del computer.

**Administration Server** – Un componente di Kaspersky Administration Kit che conserva in posizione centralizzata le informazioni sulle applicazioni Kaspersky Lab installate sui client e le gestisce.

**Certificato Administration Server**– Un certificato utilizzato per autenticare Administration Server alla connessione della Administration Console al server e trasmettere i dati tra i server e i client. Il certificato Administration Server viene creato durante l'installazione di

Administration Server. Si trova nella cartella **Cert** della cartella d'installazione.

## **B**

**Blocco di un oggetto** – Impedisce alle applicazioni esterne di accedere ad un oggetto. L'oggetto bloccato non può essere letto, eseguito, modificato o eliminato.

**Backup** – la copiatura dei dati di Administration Server per la memorizzazione ed il successivo ripristino, eseguito dall'utility di backup. L'utility consente di salvare:

- Il database di Administration Server che conserva le regole e le attività, le impostazioni delle applicazioni e gli eventi registrati su Administration Server
- Le informazioni relative alle configurazioni delle reti logiche e dei client
- I file d'installazione per l'installazione remota delle applicazioni (contenuti delle cartelle Pacchetti, Disinstalla, Aggiornamenti)
- Certificato Administration Server

**Cartella di backup** – Una directory contenente i backup degli oggetti eliminati e disinfettati.

**Chiave di licenza di riserva** – Una chiave di licenza installata per un'applicazione Kaspersky Lab ma non ancora attivata. In funzione delle impostazioni, l'attivazione della chiave può essere eseguita automaticamente alla scadenza della chiave corrente, oppure manualmente.

**Memoria di backup**– Una cartella contenente le copie di backup dei dati di Administration Server create dall'apposita utility.

## **C**

**Plugin Console (gestione)** – Un componente speciale che fornisce un'interfaccia per la gestione remota di un'applicazione tramite Administration Console. I plugin sono specifici per ciascuna applicazione e sono inclusi in tutte le applicazioni Kaspersky Lab che possono essere gestite tramite Kaspersky Administration Kit.

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

**Client, Administration Server (o computer client)** – un computer, un server, oppure una workstation con installato Network Agent nonché le applicazioni Kaspersky Lab gestite.

**Chiave di licenza in uso** – una chiave di licenza installata ed attualmente utilizzata per lavorare con un'applicazione Kaspersky Lab. Questa chiave determina il periodo di licenza nonché la politica di licenza applicata al prodotto.

**D**

**Disinfezione** - Un metodo di trattamento degli oggetti infetti. 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 eseguita, ad esempio dopo l'individuazione di un oggetto sospetto, il programma crea una copia di backup del file in questione. Qualora alcuni dati vadano perduti durante la riparazione, il backup può essere utilizzato per il loro recupero.

**Eliminazione di un oggetto** - Metodo di gestione di un oggetto. Eliminare un oggetto significa rimuoverlo fisicamente dal computer. È il metodo raccomandato per il trattamento degli oggetti infetti. Se l'eliminazione è la prima opzione per un oggetto, è necessario creare una copia di backup dello stesso prima di procedere. Il backup consente l'eventuale ripristino dell'oggetto eliminato.

**E**

**Esclusioni** - Impostazioni definite dall'utente, che escludono dalla scansione certi oggetti. È possibile personalizzare le regole di esclusione dalla *protezione in tempo reale* e dalla *scansione manuale*. Si possono ad esempio escludere gli archivi da una scansione completa, o utilizzare maschere per escludere singoli file.

**Database di posta** - Database contenenti i messaggi di posta elettronica salvati 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.

**F**

**Installazione forzata** – Un metodo di installazione remota delle applicazioni Kaspersky Lab che consente di eseguire l'installazione remota su computer client specifici della rete logica. Per garantire l'esecuzione con successo di un'attività d'installazione forzata, l'account utilizzato per lanciarla deve disporre dei diritti per il lancio remoto delle applicazioni sui computer client della rete logica. Questo metodo è consigliato per installare applicazioni su computer che eseguono Microsoft Windows NT/2000/2003/XP e che supportano tale funzione, oppure su computer che eseguono Microsoft Windows 98/Me su cui sia installato Network Agent.

**G**

**Attività globali** – Un'attività definita per l'esecuzione su diversi client di diversi gruppi amministrativi.

**Attività di gruppo** – Un'attività definita per l'esecuzione su tutti i client di un gruppo.

**Regola di gruppo** – Un'insieme di impostazioni di un'applicazione in un gruppo amministrativo, gestito tramite Kaspersky Administration Kit. Le regole di gruppo possono essere diverse per ciascun gruppo. Le regole di gruppo sono specifiche per le singole applicazioni. La regola richiede la configurazione di tutti i parametri delle applicazioni.

## I

**Tecnologia IChecker** – Una tecnologia che esclude gli oggetti non modificati rispetto all'ultima scansione dalle future scansioni. La tecnologia IChecker viene implementata tramite il database delle checksum degli oggetti.

**Tecnologia IStreams** – Una tecnologia che esclude dalla scansione i file memorizzati su un disco formattato in NTFS che non sono stati modificati dall'ultima scansione. La tecnologia IStreams viene implementata utilizzando un metodo di memorizzazione delle checksum dei file nei flussi NTFS.

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

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

**Installazione tramite lo scenario di avvio** – un metodo di installazione remota delle applicazioni Kaspersky Lab che consente di assegnare un'attività di installazione remota all'account specifico di un utente (o di diversi utenti). Quando un utente è registrato con un dominio, verrà fatto un tentativo di installare l'applicazione sul computer client per cui è registrato l'utente. Questo metodo è consigliato per l'installazione delle applicazioni Kaspersky Lab sui computer che eseguono Microsoft Windows 98/Me.

## K

**Server di aggiornamento di Kaspersky Lab** – Un elenco di siti web http e ftp di Kaspersky Lab dai quali è possibile copiare gli aggiornamenti sul computer.

**Kaspersky Administration Kit** – Un'applicazione per l'esecuzione centralizzata di importanti attività di amministrazione. Offre il controllo completo sulla politica antivirus aziendale basata sulle applicazioni di Kaspersky Lab .

**L**

**Chiave di licenza** – Un file con estensione *.key* che funziona da "chiave" personale. Questo file è necessario per il corretto funzionamento delle applicazioni Kaspersky Lab. La chiave di licenza è inclusa nel kit di distribuzione se la copia dell'applicazione è stata acquistata dai distributori Kaspersky Lab. Se l'applicazione è stata acquistata online, la chiave di licenza viene inviata via posta elettronica. Senza la chiave di licenza, Kaspersky Anti-Virus NON FUNZIONA.

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

**Gestione locale**– Gestione di un'applicazione tramite un'interfaccia locale.

**Attività locale**– Un'attività creata per l'esecuzione su un solo client.

**Periodo di licenza** – Un periodo entro il quale si ha diritto a beneficiare della funzionalità completa di Kaspersky Anti-Virus. Di regola, il periodo di licenza definito dalla chiave di licenza dura un anno dalla data d'acquisto. Una volta scaduta la licenza, l'applicazione funziona ma non sarà più possibile aggiornare il *database antivirus*.

**Amministratore di rete locale**– Un utente che installa, configura e mantiene Kaspersky Administration Kit e gestisce in remoto le applicazioni Kaspersky Lab installate sui computer della rete logica.

**M**

**Protezione massima** – Un livello di protezione che garantisce una protezione totale ma diminuisce leggermente le prestazioni.

**Massima velocità** – Un livello di protezione che garantisce la massima velocità di funzionamento ma un livello di protezione inferiore.

**N**

**Network Agent** – Un componente di Kaspersky Administration Kit che garantisce le comunicazioni tra Administration Server e le applicazioni Kaspersky Lab installate su specifici nodi di rete (workstation o server). Questo componente è comune a tutte le applicazioni incluse in Kaspersky Lab Business Optimal e Corporate Suite.

**O**

**Oggetto OLE** – Un oggetto collegato o incorporato in altri file tramite la tecnologia OLE.

**Scansione manuale completa** – Una modalità definita dall'amministratore che esamina tutti i file del computer alla ricerca di virus e disinfecta/elimina gli oggetti infetti una volta rilevati.

**P**

**Regola** – vedere **Regola di gruppo**

**Installazione Push** – Un metodo di installazione remota che consente di installare software Kaspersky Lab sui computer specificati della rete

logica. Per eseguire con successo l'attività tramite un'installazione Push, l'account utilizzato per lanciare questa attività deve disporre dei diritti per eseguire applicazioni sui client remoti. Questo metodo è consigliato per i computer che eseguono MS Windows NT/2000/2003/XP, che supportano questa funzione, oppure per i computer che eseguono MS Windows 98/Me ed hanno installato Network Agent.

**Q**

**Mettere in quarantena**– Un metodo di gestione degli oggetti *sospetti*. L'accesso a tali oggetti viene bloccato, ed essi vengono spostati in quarantena per ulteriore elaborazione.

**Quarantena**– Una memoria speciale dove isolare gli oggetti infetti e sospetti.

**R**

**Protezione in tempo reale**– Una modalità di scansione in cui un'applicazione antivirus è residente in memoria. Nella modalità di protezione in tempo reale, l'applicazione esamina tutti gli oggetti quando vengono aperti per la lettura, la scrittura o l'esecuzione. Prima di consentire l'accesso ad un oggetto, Kaspersky Anti-Virus lo esamina alla ricerca di virus e, se ne rileva, blocca l'accesso ad esso, lo disinfetta o lo elimina (in funzione delle impostazioni definite dall'utente).

**Livello raccomandata** – Il livello di protezione antivirus in base alle impostazioni predefinite raccomandate dagli esperti di Kaspersky Lab, che garantisce la protezione ottimale del computer. Questo è il livello predefinito.

**Installazione remota**– Installazione delle applicazioni Kaspersky Lab tramite i servizi offerti da Kaspersky Administration Kit.

**Ripristino** - Ripristino dei dati di Administration Server tramite un'utility di backup. Le informazioni di ripristino sono disponibili nella memoria di backup. L'utility consente di ripristinare:

- Il database di Administration Server che conserva le regole, le attività, le impostazioni delle applicazioni e gli eventi registrati su Administration Server
- Le informazioni relative alle configurazioni delle reti logiche e dei client
- I file d'installazione per l'installazione remota delle applicazioni (contenuti delle cartelle Pacchetti, Disinstalla, Aggiornamenti)
- Il Certificato Administration Server

**S**

**Installazione basata su script** – Un metodo d'installazione che pone in relazione l'attività di installazione remota con un account utente

specificato (o con diversi account). Quando l'utente specificato accede al dominio, l'applicazione verrà installata sul client sul quale l'utente ha effettuato l'accesso. Questo metodo è consigliato per i computer che eseguono MS Windows 95/98/Me

**Impostazioni, attività** – Impostazioni specifiche dell'applicazione per ciascun tipo di attività.

**Impostazioni, applicazioni** - Impostazioni specifiche dell'applicazione per tutti i tipi di attività eseguiti da questa applicazione.

**Livello di criticità** – Un parametro che classifica un evento registrato durante le attività di Kaspersky Anti-Virus. Vi sono quattro livelli di criticità:

- **Critico**
- **Errore**
- **Avviso**
- **Informazioni**

Gli eventi dello stesso tipo possono essere di criticità diversa, in funzione della situazione specifica.

**Oggetti di avvio**– Insieme di programmi necessari per l'esecuzione e il corretto funzionamento del sistema operativo e di altro software installato sul computer. Il sistema operativo li esegue ad ogni avvio. Alcuni virus cercano di infettarli e possono provocare un errore di avvio.

**Oggetto sospetto** - oggetto contenente una variante del codice di un virus noto o un codice somigliante a quello di un virus ma ancora sconosciuto agli esperti di Kaspersky Lab.

**Scansione dei file per formato**– In questa modalità di scansione, il programma analizza i contenuti di un file, più precisamente l'identificatore del formato nell'intestazione dei file.

**Scansione dei file per estensione**– In questa modalità di scansione, il programma prende in considerazione l'estensione del file esaminato.

## T

**Attività** – Un'azione con nome che viene eseguita da un'applicazione di Kaspersky Lab.

**Applicazione di terzi**– Un'applicazione antivirus di terzi, oppure un'applicazione Kaspersky Lab che non supporta l'amministrazione tramite Kaspersky Administration Kit.

## U

**Virus sconosciuto** – Un nuovo virus non registrato nel *database antivirus*. Di regola, Kaspersky Anti-Virus rileva i virus sconosciuti tramite un *analizzatore di codice euristico* e gli oggetti contenenti tali virus vengono identificati come *sospetti*.

**Aggiornamento** – Una funzione di Kaspersky Anti-Virus che aggiorna/aggiunge nuovi file (database antivirus o moduli del programma) recuperati dai server di aggiornamento Kaspersky Lab.

**Agenti di aggiornamento** - computer che operano da centri intermedi per la distribuzione degli aggiornamenti e dei pacchetti d'installazione tra i gruppi amministrativi.

## V

**Unità virtuali (RAM drive)** – Una parte di RAM che emula un disco fisico normale di un personal computer.

**Soglia di attività dei virus** – Numero di virus rilevati su un intervallo di tempo specifico. Quando questo numero viene superato, la situazione viene considerata un **Attacco di virus**. Questo parametro è importante per definire le epidemie di virus, poiché l'amministrazione può rispondere per tempo alle nuove minacce ed attuare misure preventive per proteggere la sua rete.

## APPENDICE B. 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 550 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 15 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 25 ore su 25, disponibile in diverse lingue per soddisfare le esigenze di una clientela internazionale.

## A.B.1. Altri prodotti Kaspersky Lab

### **Kaspersky Lab News Agent**

News Agent è progettato per comunicare tempestivamente le notizie pubblicate da Kaspersky Lab, per le notifiche relative allo status corrente dell'attività dei virus e per notizie fresche. Il programma legge l'elenco dei canali news disponibili e il loro contenuto dai server di notizie di Kaspersky Lab con la frequenza specificata.

Il programma permette all'utente le seguenti funzioni:

- Visualizza nella barra di sistema il giudizio sul virus corrente.

- Iscriviti ad un canale di news.

- Recupera le news da ogni canale selezionato con la frequenza specificata e ricevi una notifica sulle ultime notizie.

- Rivedi le notizie sui canali selezionati.

- Rivedi l'elenco dei canali e il loro status.

- Apri nel browser il testo completo di un articolo.

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 tuo browser. Gli utenti hanno così la possibilità di esaminare velocemente 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 che richiede una iscrizione 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 tuo browser. 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® Internet Security 7.0**

Kaspersky Internet Security 7.0 è una soluzione integrata progettata per proteggere i personal computer dalle più diffuse minacce (virus, hackers, spam e spyware). Una singola interfaccia abilita gli utenti a configurare tutti i componenti del programma.

### **La protezione anti-virus include:**

**Scansione Anti-Virus del traffico e-mail** a livello del protocollo di trasmissione dati (POP3, IMAP e NNTP per posta in arrivo e SMTP per messaggi in uscita), indipendentemente dal client mail che viene utilizzato. Il programma include plug-in per conosciuti client e-mail (come Microsoft Office Outlook, Microsoft Outlook Express/Windows Mail e The Bat) e supporta la disinfezione dei loro database delle e-mail.

Scansione anti-virus real-time del traffico Internet trasferito via HTTP.

**Protezione del file system:** scansione anti-virus di file individuali, cartelle o drives. In aggiunta l'applicazione può condurre il controllo anti-virus solo per le aree critiche del sistema operativo e gli oggetti di avvio di Microsoft Windows.

**Protezione Proattiva:** il programma monitorizza costantemente l'attività dell'applicazione e dei processi lavorando sulla RAM, prevenendo modifiche importanti al file system ed al registro e ripristinando il system.

**Protezione contro le frodi Internet:** viene assicurata dal riconoscimento dagli attacchi phishing, evitando la sottrazione di dati riservati (soprattutto password, numeri dei conti bancari e delle carte di credito), e bloccando l'esecuzione di script pericolosi sulle pagine web, finestre di pop-up e banner pubblicitari. La caratteristica **di blocco degli autodialer** aiuta ad identificare software che tentano di usare il tuo modem per connessioni nascoste e non autorizzate a numerazioni telefoniche a pagamento e blocca tali attività.

Kaspersky Internet Security 7.0 **registra i tentativi di scansionare le porte del tuo computer** che frequentemente precedono gli attacchi sul network e con successo difende contro i tipici attacchi al network. Il programma utilizza **come base regole definite** per il controllo delle transazioni sulla rete tracciando tutti i pacchetti di dati in ingresso ed uscita. La **Modalità Stealth** (di proprietà di SmartStealth™ technology) **previene gli attacchi dall'esterno**. Quando ti sposti su Modalità Stealth il sistema blocca tutta l'attività di rete escluse poche transazioni permesse nelle regole definite dall'utente.

Il programma impiega un approccio tutto compreso per filtrare gli spam in ingresso con i messaggi di posta:

Verifica contro liste bianche e nere del destinatario (compresi indirizzi dei siti di phishing)

Ispezione delle frasi contenuto nel corpo del messaggio

Analisi del testo dei messaggi utilizzando un algoritmo di apprendimento

Riconoscimento di spam inviato nei file immagine

### **Kaspersky Anti-Virus Mobile**

Kaspersky® Anti-Virus Mobile fornisce una protezione per apparati mobili funzionanti con Symbian OS e Microsoft Windows Mobile. Il programma assicura una scansione esaustiva comprendente:

**Scansione su richiesta** della memoria dell'apparato, memory cards o cartelle individuali o uno specifico file; se viene rilevato un file infetto questo viene spostato in Quarantena o eliminato

**Scansione real-time** – tutti i file in ingresso ed uscita sono scansionati automaticamente, come pure i file oggetti di tentativi di accesso

**Protezione da spam** contenuto nei messaggi di testo

### **Kaspersky Anti-Virus per Servers File**

Questo pacchetto fornisce una affidabile protezione da tutti i tipi di malware per i file di sistema su server che operano con Microsoft Windows, Novell NetWare, Linux e Samba. La suite include le seguenti applicazioni Kaspersky Lab:

[Kaspersky Administration Kit.](#)

[Kaspersky Anti-Virus for Windows Server.](#)

[Kaspersky Anti-Virus for Linux File Server.](#)

[Kaspersky Anti-Virus for Novell Netware.](#)

[Kaspersky Anti-Virus for Samba Server.](#)

Caratteristiche e funzionalità:

Protegge i file system dei server in real-time. Tutti i file dei server sono scansionati quando aperti o salvati sul server

Evita l'epidemia virus

Scansione su richiesta dell'intero file system o di file o cartelle individuali

Usa tecnologie di ottimizzazione nella scansione degli oggetti nel file system del server

Possibilità di rollback dopo un attacco virus

Scalabilità del pacchetto software in accordo con la capacità delle risorse disponibili di sistema

Monitoraggio del sistema di cattivo bilanciamento

Creazione di un elenco di processi sicuri la cui attività sul server non è soggetta a controllo dal pacchetto software

Amministrazione remota del pacchetto software, compreso installazione, configurazione ed amministrazione centralizzata

Salvataggio di copie di backup degli oggetti infettati o cancellati nel caso tu abbia bisogno di ripristinarle

Messa in Quarantena degli oggetti sospetti

Invio di notifiche degli eventi nell'esecuzione del programma all'amministratore di sistema

Registrazione di dettagliati report

Aggiornamento automatico dei database del programma

### **Sicurezza Kaspersky Open Space**

Kaspersky Open Space Security è un pacchetto software con un nuovo approccio alla sicurezza per le rete aziendali attuali di qualsiasi dimensione assicurando un sistema informativo di protezione centralizzato ed il supporto per uffici remoti e utenti in movimento.

La suite comprende quattro programmi:

Kaspersky Work Space Security

Kaspersky Business Space Security

Kaspersky Enterprise Space Security

Kaspersky Total Space Security

Specifiche per ogni programma sono fornite di seguito.

**Kaspersky WorkSpace Security** è un programma per la protezione centralizzata di workstation interne ed esterne alla rete aziendale contro tutte le minacce attuali di Internet (virus, spyware, attacchi di hacker e spam)

Caratteristiche e funzionalità:

Affidabile protezione da virus, spyware, attacchi hacker e spam

Difesa Proattiva da nuovi programmi maligni le cui firme non sono ancora state aggiunte al database

Firewall personale con sistema di rilevamento intrusione e avviso circa gli attacchi alla rete

Rollback per modifiche pericolose del sistema

Protezione dagli attacchi phishing mail indesiderate

- Redistribuzione dinamica delle risorse durante la completa scansione del sistema
- Amministrazione Remota del pacchetto software, comprendente installazione, configurazione ed amministrazione centralizzata
- Supporto per Cisco® NAC (Network Admission Control)
- Scansione e-mail e traffico Internet in real-time e, blocco delle finestre pop-up e banner pubblicitari su Internet
- Operatività sicura in qualsiasi tipo di Network compreso Wi-Fi
- Creazione del disco di ripristino per permetterti di ripristinare il tuo sistema dopo una invasione virus
- Ampio sistema di reportistica sugli stati della protezione
- Aggiornamento automatico dei database
- Supporto completo per sistemi operativi a 64-bit
- Ottimizzazione delle prestazioni del programma su laptops (tecnologia Intel® Centrino® Duo)
- Capacità di disinfezione remota (Intel® Active Management, Intel® vPro™).

**Kaspersky Business Space Security** fornisce una ottima protezione alle risorse informative aziendali dalle odierne minacce Internet. Kaspersky Business Space Security protegge workstations e file server da tutti i tipi di virus, Trojan e worms, impedisce la diffusione dei virus ed assicura le informazioni mentre garantisce un accesso immediato alle risorse di rete per l'utente.

#### Caratteristiche e funzionalità

- Amministrazione Remota del pacchetto software, comprendente installazione, configurazione ed amministrazione centralizzata
- Supporto per Cisco® NAC (Network Admission Control)
- Protezione di workstations e file server da tutti i tipi di minacce
- tecnologia iSwift per evitare la ripetizione della scansione file internamente alla rete
- Distribuzione del carico tra i server
- Oggetti sospetti in Quarantena da workstation
- Rollback per modifiche pericolose del sistema
- Scalabilità del pacchetto software in accordo con la capacità delle risorse disponibili di sistema

Difesa Proattiva per workstation da programmi maligni le cui firme non sono ancora state aggiunte ai database

Scansione e-mail e traffico internet in real-time

Firewall personale con sistema di rilevamento intrusione e avviso circa gli attacchi alla rete

Protezione mentre si usa un network Wi-Fi

Auto-Difesa da programmi maligni

Oggetti sospetti in Quarantena

Aggiornamento automatico dei database

### **Kaspersky Enterprise Space Security**

Questo programma comprende componenti per la protezione dalle attuali minacce Internet collegati a workstations e servers. Cancella i virus dalle email, rendendo sicura l'informazione mentre fornisce un accesso sicuro alle risorse di rete per l'utente.

Caratteristiche e funzionalità

Protezione delle workstation e file server da virus, Trojan e worm

Protezione di Sendmail, Qmail, Postfix e Exim mail servers

*Scansione di tutte le e-mail su microsoft Exchange Server compreso le cartelle condivise*

*Processo di tutte le e-mail, database ed altri oggetti per i server Lotus Domino*

*Protezione dagli attacchi phishing e junk mail*

*Prevenzione infezione virus e mass mailing*

Scalabilità del pacchetto software in accordo con la capacità delle risorse disponibili di sistema

Amministrazione Remota del pacchetto software, comprendente installazione, configurazione ed amministrazione centralizzata

Supporto per Cisco® NAC (Network Admission Control)

Difesa Proattiva per workstation da programmi maligni le cui firme non sono ancora state aggiunte ai database

Firewall personale con sistema di rilevamento intrusione e avviso circa gli attacchi alla rete

Protezione sicura mentre si usa un network Wi-Fi

Scansione traffico Internet in real-time

- Rollback per modifiche pericolose del sistema
- Redistribuzione dinamica delle risorse durante la completa scansione del sistema
- Oggetti sospetti in Quarantena
- Ampio sistema di reportistica sugli stati della protezione
- Aggiornamento automatico dei database

### **Kaspersky Total Space Security**

Questo programma esegue il monitoraggio del flusso dati in ingresso ed uscita (e-mail, Internet e tutte le interazioni di rete). Comprende i componenti per la protezione di workstation ed apparati mobili, mantenendo sicura l'informazione mentre fornisce per l'utente un accesso sicuro alle risorse informative della rete aziendale e di Internet e una sicura comunicazione via e-mail.

#### Caratteristiche e funzionalità

- Protezione completa da virus, spyware, attacchi hacker e spam a qualsiasi livello della rete aziendale da workstation a gateways Internet
- Difesa Proattiva per workstation da programmi maligni le cui firme non sono ancora state aggiunte ai database
- Protezione dei server di posta e server collegati
- Scansione del traffico Internet (HTTP/FTP) in real-time sull'area del network locale
- Scalabilità del pacchetto software in accordo con la capacità delle risorse disponibili di sistema
- Blocco degli accessi da workstation infettate
- Prevenzione epidemia virus
- Reportistica centralizzata sugli stati di protezione
- Amministrazione Remota del pacchetto software, comprendente installazione, configurazione ed amministrazione centralizzata
- Supporto per Cisco® NAC (Network Admission Control)
- Supporto per hardware server proxy
- Filtraggio del traffico Internet usando elenchi di server, tipi di oggetto e gruppi utenti sicuri
- Tecnologia iSwift per evitare la ripetizione della scansione di file nella rete
- Redistribuzione dinamica delle risorse durante la completa scansione del sistema

Firewall personale con sistema di rilevamento intrusione e avviso circa gli attacchi alla rete

Sicura operatività per gli utenti in qualsiasi tipo di Network compreso Wi-Fi

*Protezione dagli attacchi phishing e junk mail*

Capacità di disinfezione remota (Intel® Active Management, Intel® vPro™)

Rollback per modifiche pericolose del sistema

Auto-Difesa da programmi maligni

Completo supporto per sistemi operativi a 64-bit

Aggiornamento automatico dei database

### **Kaspersky Security per Server di Posta**

Questo programma è per proteggere i server di posta ed i server collegati da programmi pericolosi e da spam. Il programma comprende l'applicazione per proteggere tutti server di posta standard (Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix ed Exim) e ti abilita a configurare un gateway e-mail dedicato. La soluzione include:

[Kaspersky Administration Kit.](#)

[Kaspersky Mail Gateway.](#)

[Kaspersky Anti-Virus for Lotus Notes/Domino.](#)

[Kaspersky Anti-Virus for Microsoft Exchange.](#)

[Kaspersky Anti-Virus for Linux Mail Server.](#)

Le sue caratteristiche comprendono

Affidabile protezione contro programmi maligni op potenzialmente pericolosi

Filtraggio di junk mail

Scansione di tutti i messaggi ed si Microsoft Exchange Server per virus compreso le cartelle condivise

Controllo di e-mail, database ed altri oggetti per server Lotus Notes/Domino

Filtraggio delle e-mail per tipo di allegato

Oggetti sospetti in Quarantena

Semplice sistema di gestione del programma

Prevenzione epidemia virus

Monitoraggio stato protezione a mezzo notifiche

Sistema di reportistica per l'operatività del programma

Scalabilità del pacchetto software in accordo con la capacità delle risorse disponibili di sistema

Aggiornamento automatico dei database

### **Kaspersky® Anti-Spam**

Kaspersky® Anti-Spam è un'innovativa suite di software progettata per assistere le aziende con reti di piccole e medie dimensioni nella difesa contro i sempre più numerosi messaggi di posta elettronica non desiderati (spam). Il prodotto combina 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 (includere 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, dove controlla le e-mail in arrivo dallo spam, Kaspersky® Anti-Spam funziona come barriera alle e-mail indesiderate. Il prodotto è compatibile con qualsiasi sistema di posta e può essere installato sia su server di posta esistente 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 l'aggiunta di campioni forniti specialisti del laboratorio linguistico della Società. I database vengono aggiornati ogni 20 minuti.

### **Kaspersky Anti-Virus® for MIMESweeper**

Kaspersky Anti-Virus® per MIMESweeper assicura una elevata velocità di scansione del traffico sui server funzionanti con Clearswift MIMESweeper per SMTP / Clearswift MIMESweeper per Exchange / Clearswift MIMESweeper per Web.

Il programma è un plug-in e scansiona contro i virus e processa in real-time il traffico e-mail in ingresso ed in uscita.

## A.B.2. Per contattarci

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.

Supporto Tecnico	<a href="http://www.kaspersky.com/supportinter.html">Trovi le informazioni di supporto tecnico su http://www.kaspersky.com/supportinter.html</a> Helpdesk: <a href="http://www.kaspersky.com/helpdesk.html">http://www.kaspersky.com/helpdesk.html</a>
Informazio	<a href="http://www.kaspersky.com">WWW: http://www.kaspersky.com</a>

---

ni generali	<a href="http://www.viruslist.com">http://www.viruslist.com</a> E-mail: <a href="mailto:info@kaspersky.com">info@kaspersky.com</a>
-------------	---

---

# APPENDICE C. CONTRATTO DI LICENZA

AVVERTENZA PER TUTTI GLI UTENTI: SI RACCOMANDA DI LEGGERE ATTENTAMENTE IL SEGUENTE CONTRATTO DI LICENZA ("CONTRATTO"), PER LA LICENZA DEL SOFTWARE SPECIFICATO ("SOFTWARE") PRODOTTO DA KASPERSKY LAB. ("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 DOVRA ASTENERSI DAL ROMPERE IL SIGILLO DELLA BUSTA DEL CD, SCARICARE, INSTALLARE O UTILIZZARE QUESTO SOFTWARE. SE IL SIGILLO DELLA BUSTA DEL CD O DELLA SCATOLA È STATO ROTTO, IL DIRITTO ALLA RESTITUZIONE AI FINI DEL RIMBORSO DECADE. IL SOFTWARE PER USO DOMESTICO (KASPERSKY ANTI-VIRUS PERSONAL, KASPERSKY ANTI-VIRUS PERSONAL PRO, KASPERSKY ANTI-HACKER, KASPERSKY SECURITY FOR PDA) ACQUISTATO MEDIANTE SCARICAMENTO DA INTERNET PUÒ ESSERE RESTITUITO PER IL RIMBORSO COMPLETO ENTRO 14 GIORNI DALL'ACQUISTO PRESSO KASPERSKY LAB O UN SUO DISTRIBUTORE O RIVENDITORE AUTORIZZATO. ALTRI PRODOTTI NON SONO RIMBORSABILI. 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 chiave di attivazione ("File di identificazione chiave") fornita da Kaspersky Lab come parte integrante del Software.

1. Concessione della licenza. Previo pagamento dei canoni di licenza applicabili, e in base ai termini e alle condizioni del presente Contratto, Kaspersky Lab conferisce all'utente il diritto non esclusivo e non trasferibile di usare una copia della versione specificata del Software e della documentazione che lo accompagna (la "Documentazione") per il periodo di validità del presente Contratto, esclusivamente per scopi interni. L'utente può installare una copia del

Software su un computer, workstation, agenda elettronica o altro dispositivo elettronico per il quale il Software è stato progettato (ciascuno denominato "Dispositivo del cliente"). Se il Software è concesso su licenza come suite o pacchetto contenente più di un prodotto Software specificato, tale licenza si applica a tutte le applicazioni software specificate, ed è soggetta alle restrizioni o alle condizioni d'uso specificate sul listino prezzi applicabile o sull'imballo di ciascuna singola applicazione Software.

1.1 Uso. Il Software è concesso in licenza in qualità di singola applicazione; non può essere utilizzato su più di un Dispositivo client o da più di un utente per volta, salvo diversamente specificato nella presente Sezione.

1.1.1 Il Software è "in uso" su un Dispositivo del cliente 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 Dispositivo del cliente. 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 Dispositivo del cliente 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 È fatto divieto all'utente di effettuare o consentire a terzi di effettuare copie (oltre a quelle espressamente consentite ai sensi del presente contratto), correggere errori o altrimenti modificare, adattare o tradurre il Software, oppure derivare altre applicazioni dal Software stesso.

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.

1.2 Uso in modalità server. Il Software può essere usato su un Dispositivo del cliente o su o come server ("Server") in un ambiente multiutente o di rete ("Modalità server") solo se tale uso è consentito in base al listino prezzi applicabile o alla confezione del Software. È necessaria una licenza a parte per ogni Dispositivo del cliente o "postazione" che possa collegarsi al Server in qualsiasi momento, a prescindere dal fatto che tali Dispositivi del cliente o postazioni autorizzati mediante licenza siano Collegati simultaneamente o accedano o facciano effettivamente uso del Software. L'uso di software o di hardware che riducano il numero dei Dispositivi del cliente o postazioni che accedono direttamente a o fanno uso del Software (per esempio software o hardware "multiplexing" o "pooling") non riduce il numero delle licenze necessarie (vale a dire, il numero delle licenze necessarie corrisponde al numero di input distinti al "front end" del software o hardware multiplexing o pooling). Se il numero di Dispositivi Client o di postazioni che possono connettersi al Software è maggiore del numero di licenze ottenute, l'utente deve disporre di un meccanismo ragionevole che garantisca che l'uso del Software non supera i limiti di utilizzo specificati per la licenza ottenuta. La presente licenza autorizza l'utente a effettuare o scaricare il numero di copie della Documentazione per ogni Dispositivo Client o postazioni concessi in licenza necessario per il suo utilizzo ai termini di legge, a condizione che ogni copia contenga tutte le informazioni sui diritti di proprietà della Documentazione.

1.3 Licenze per volume di acquisto. Se il Software è concesso dietro una licenza per volume le cui condizioni sono specificate nella fattura applicabile del prodotto o sull'imballo del Software, l'utente può effettuare, utilizzare o installare tante copie supplementari del software sul numero di Dispositivi Client quante sono specificate nelle condizioni della licenza per volume. L'utente deve applicare meccanismi ragionevoli per garantire che il numero di Dispositivi Client su cui è stato installato il Software non superi il numero di licenze ottenute. La presente licenza autorizza l'utente a effettuare o scaricare una copia della Documentazione per ogni copia supplementare autorizzata dalla licenza per volume, a condizione che ogni copia contenga tutte le informazioni sui diritti di proprietà della Documentazione.

2. Durata. Il presente Contratto è valido per il periodo specificato nel file chiave (l'unico file necessario per abilitare completamente il Software; cfr. la Guida/Informazioni sul Software; per la versione Unix/Linux del Software vedere l'avviso sulla data di scadenza del file chiave) salvo risoluzione anticipata e in tal caso fino alla data di tale risoluzione, come esposto nel presente documento. Il presente Contratto terminerà automaticamente in caso di mancata osservanza da parte dell'utente di una delle condizioni, limitazioni o altri requisiti descritti nel presente. Al momento della rescissione o alla scadenza del presente Contratto, l'utente è tenuto a distruggere immediatamente tutte le copie del Software e della

Documentazione. E' possibile recedere dal presente Contratto in qualsiasi momento distruggendo tutte le copie del Software e della Documentazione.

### 3. Assistenza.

(i) Kaspersky Lab mettera a disposizione dell'utente i servizi di assistenza ("Servizi di assistenza") specificati di seguito, per la durata di un anno, 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 File di identificazione chiave 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.

(ii) 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 .

(iii) 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 allegata al presente Contratto, e acconsente esplicitamente al trasferimento dei propri dati in paesi esterni a quello di residenza, come specificato nella politica di tutela della riservatezza.

(iv) Per "Servizi di assistenza" si intendono

(a) Aggiornamenti quotidiani del database antivirus;

(b) Aggiornamenti gratuiti del software, inclusi gli aggiornamenti della versione;

(c) Assistenza tecnica estesa via e-mail e numero verde fornita dal distributore e/o dal rivenditore;

(d) Rilevamento virus e aggiornamenti per l'eliminazione entro 24 ore.

4. Diritti di proprieta. Il Software e protetto dalle leggi sul copyright. Kaspersky Lab e i relativi fornitori possiedono e mantengono tutti i diritti, l'autorita e gli interessi del Software e ad esso correlati, inclusi tutti i diritti di proprieta, i brevetti, i marchi commerciali e gli altri diritti di proprieta intellettuale ad esso connessi. Il possesso, l'installazione o l'utilizzo del Software non trasferiscono all'utente alcun diritto relativo alla proprieta intellettuale del Software e non determinano l'acquisizione di diritti sul Software salvo quelli espressamente indicati nel presente Contratto.

5. Riservatezza. L'utente riconosce che il Software e la Documentazione, inclusa la specifica configurazione e la struttura dei singoli programmi e il File di identificazione chiave costituiscono informazioni proprietarie riservate di Kaspersky Lab. L'utente non dovra divulgare, fornire o altrimenti rendere disponibili tali informazioni riservate in qualsivoglia forma a terzi senza previo

consenso scritto di Kaspersky Lab. Dovra inoltre applicare ragionevoli misure di sicurezza volte a proteggere tali informazioni riservate ma, senza tuttavia limitarsi a quanto sopra espresso dovra fare quanto in suo potere per tutelare la sicurezza del File di identificazione chiave.

#### 6. Garanzia limitata

(i) Kaspersky Lab garantisce che per un periodo di [90] giorni a decorrere dal primo caricamento o installazione il Software operera sostanzialmente in conformita 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 responsabilita 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 ne 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 ne 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 responsabilita di Kaspersky Lab per la violazione della garanzia di cui al paragrafo (i) saranno a discrezione di Kaspersky Lab, che decidera se riparare, sostituire o rimborsare il Software in caso di reclamo a Kaspersky Lab o suoi fornitori durante il periodo di garanzia. L'utente dovra fornire tutte le informazioni ragionevolmente necessarie per agevolare il Fornitore nel ripristino dell'articolo difettoso.

(v) La garanzia di cui al punto (i) non e applicabile qualora l'utente (a) apporti modifiche al presente Software o determini la necessita 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 specificate in questo Contratto sostituiscono qualsiasi altra condizione, garanzia o termine relativi alla fornitura o alla presunta fornitura, all'impossibilita di fornire o al ritardo nella fornitura del Software o della Documentazione che, se non fosse per questo paragrafo (v), potrebbero verificarsi tra Kaspersky Lab e voi o sarebbero altrimenti impliciti o incorporati nel presente Contratto o in qualsiasi altro contratto collaterale, per disposizione statutaria, legislazione vigente o altro, che con cio sarebbero esclusi (inclusi, senza limitazione, le condizioni implicite, le garanzie o altri termini relativi all'adeguatezza della qualita, all'idoneita allo scopo o all'uso di competenza e cura ragionevoli).

#### 7. Responsabilita limitata

(i) Nessun elemento nel presente Contratto deve escludere o limitare la responsabilita di Kaspersky Lab relativamente a (i) responsabilita civile per frode, (ii) 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, (iii) eventuali violazioni degli obblighi stabiliti dalla sezione 12 del Sale of Goods Act del 1979 o della sezione 2 del Supply of Goods and Services Act del 1982 o (iv) eventuali responsabilità che non possono essere escluse ai termini di legge.

(ii) Ai sensi del paragrafo (i), il Fornitore 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 scanso di dubbi, i danni o le perdite del tipo specificato nel paragrafo (ii), da (a) a (ii), (i).

(iii) Ai sensi del paragrafo (i), la responsabilità di Kaspersky Lab (relativamente al contratto, per responsabilità civile, restituzione o altro) derivante o collegata alla fornitura del Software non deve in alcun caso superare un ammontare pari alla stessa somma corrisposta dall'utente per il software.

8. La costituzione e l'interpretazione del presente Contratto devono essere effettuate in conformità alle leggi dell'Inghilterra e del Galles. Con il presente, le parti si rimettono alla giurisdizione dei tribunali di Inghilterra e Galles fatto salvo che, in caso di ricorso, Kaspersky Lab detiene il diritto di intentare un'azione legale in qualsiasi tribunale della giurisdizione competente.

9. (i) 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. Fatta eccezione per quanto disposto nei paragrafi (ii) - (iii), non si riconosce all'utente alcun rimedio per

affermazioni non veritiere su cui l'utente stesso abbia fatto affidamento alla stipula del presente Contratto ("Dichiarazione erronea") e Kaspersky Lab declina qualsiasi responsabilita oltre a quella derivante dalle condizioni esplicite del presente Contratto.

(ii) Nessun elemento nel presente Contratto esclude o limita la responsabilita di Kaspersky Lab per eventuali false dichiarazioni rilasciate intenzionalmente.

(iii) La responsabilita di Kaspersky Lab per eventuali false dichiarazioni relativamente ad aspetti fondamentali, incluso un aspetto fondamentale relativo alla capacita del fabbricante di adempiere ai propri obblighi ai sensi del presente Contratto, sara soggetta alla clausola di responsabilita limitata di cui al paragrafo 7 (iii).

#### 1.

---

Quando si utilizza il Software demo, l'utente non può usufruire del Servizio Tecnico specificato nella Clausola 2 di questo EULA e neppure ha diritto di vendere la copia in possesso a terze parti.

All'utente è concesso l'uso del software a scopi dimostrativi per il periodo riportato nel file della chiave di avvio dal momento dell'attivazione (questo periodo può essere visto nella finestra Servizio del GUI del software).