

KASPERSKY LAB

Kaspersky[®] Administration Kit
versione 6.0

Per cominciare

KASPERSKY® ADMINISTRATION KIT
VERSIONE 6.0

Per cominciare

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

Data di revisione: Mayo, 2007

Sommario

CAPITOLO 1. INTRODUZIONE.....	4
CAPITOLO 2. PER COMINCIARE	6
2.1. Installazione di MSDE 2000.....	7
2.2. Installazione di Administration Server e Administration Console.....	8
2.3. Avvio rapido	9
2.4. Creazione di un gruppo di amministrazione	11
2.5. Installazione remota di Network Agent.....	12
2.6. Installazione di Kaspersky Anti-Virus.....	13
2.7. Verifica del funzionamento dell'attività di aggiornamento	14
2.8. Configurazione delle notifiche	15
2.9. Collaudo del sistema di notifica e dell'attività di scansione manuale.....	16
2.10. Generazione di report.....	17
CAPITOLO 3. AGGIORNAMENTO DELLA VERSIONE 4.X ALLA 6.X	18
CAPITOLO 4. CONCLUSIONI	20
APPENDICE 1. KASPERSKY LAB	21
A.1.1. Altri prodotti Kaspersky Lab.....	22
A.1.2. Per contattarci	33
APPENDICE 2. CONTRATTO DI LICENZA	34

Capitolo 1. Introduzione

Questo documento illustra i passaggi principali che un amministratore della sicurezza di rete deve attuare per installare in maniera sicura ed efficiente un sistema di protezione antivirus basato sulle applicazioni Kaspersky Lab su una rete aziendale servendosi di **Kaspersky Administration Kit**.

Questo documento presenta uno scenario semplificato nel quale la protezione antivirus è installata su diversi computer senza utilizzare la gerarchia degli Administration Server. Per una corretta installazione, i computer devono utilizzare uno dei seguenti sistemi operativi: Microsoft Windows 2000 con installato il Service Pack 1 o superiore; Microsoft Windows XP Professional con installato il Service Pack 1 o superiore; Microsoft Windows XP Professional x64 o superiore; Microsoft Windows Server 2003 o superiore; Microsoft Windows Server 2003 x64 o superiore; Microsoft Windows NT4 con installato il Service Pack 6a o superiore.

Questo documento descrive inoltre la procedura di aggiornamento delle applicazioni Kaspersky Lab dalla versione 4.x alla versione 6.x.

[Per informazioni dettagliate sulle funzionalità dell'applicazione, vedere la Guida di distribuzione e quella dell'amministratore.](#)

Kaspersky Administration Kit 5 è progettato per la gestione del sistema di protezione antivirus nell'ambito di una rete aziendale. L'applicazione consente all'amministratore di:

- Creare una rete logica che garantisca la protezione antivirus della rete aziendale.
- Installare le applicazioni Kaspersky Lab attraverso la rete.
- Gestire il sistema di protezione antivirus in maniera remota, da una singola postazione.
- Ricevere, attraverso la rete, la notifica di eventi correlati alla protezione antivirus.
- Raccogliere statistiche e rapporti da tutte le installazioni.

Kaspersky Administration Kit 5 include i seguenti componenti:

- **Administration Server** permette all'amministratore di gestire, da una postazione centrale, le applicazioni Kaspersky Lab installate in una rete. Le applicazioni che al momento possono essere gestite in tal modo sono Kaspersky Anti-Virus for Workstations 5.0 e Kaspersky Anti-Virus for File Servers 5.0. Administration Server conserva i dati relativi al sistema di protezione antivirus aziendale in un database, che può essere MSDE 2000 con installato il Service Pack 3 o superiore, MySQL 5.0.22 (code page predefinita UTF-8), Microsoft SQL 2005 o superiore o Microsoft SQL 2005 Express o superiore. I database devono già essere operativi sulla rete aziendale, prima di installare ed iniziare ad utilizzare Administration Server. MSDE 2000 con il Service Pack 3 può essere installato tramite Kaspersky Administration Kit 5.0. Per fare ciò, sul computer deve essere installato Microsoft Data Access Components (MDAC) 2.8 o superiore.
- **Network Agent** viene installato sulle workstation protette dalle applicazioni di Kaspersky Lab che supportano l'amministrazione tramite Kaspersky Administration Kit. Questo componente coordina le interazioni tra le applicazioni Kaspersky Lab presenti sui computer client e l'Administration Server stesso. Network Agent riceve i comandi dell'Administration Server e fornisce informazioni sullo stato della protezione antivirus dei computer client.
- **Administration Console** fornisce un'interfaccia utente per i servizi di amministrazione di Server e Agent. Questo componente si integra con la Microsoft Management Console (MMC).

Capitolo 2. Per cominciare

Per realizzare un efficace sistema di protezione di una rete aziendale, è necessario eseguire le seguenti operazioni:

1. Installare Microsoft Data Access Components (MDAC) 2.8 o superiore. Questo non è necessario se il componente è già installato sulla rete aziendale.
2. Installare MSDE 2000 SP 3 (vedere la sezione 2.1 a pagina7), Microsoft SQL 2000 SP 3, MySQL 5.0.22 (codepage predefinita UTF-8), Microsoft SQL 2005 o superiore o Microsoft SQL Express o superiore. Saltare questo passaggio qualora sulla rete sia già stato installato uno di questi server di database.
3. Installare Administration Server e Administration Console (vedere la sezione 2.2 a pagina8).
4. Configurare le impostazioni iniziali del sistema di protezione antivirus utilizzando la Procedura guidata di avvio rapido (vedere la sezione 2.3 a pagina9).
5. Creare i gruppi amministrativi (vedere la sezione 2.4 a pagina 11), se questi non sono stati creati utilizzando la Procedura guidata di avvio rapido. I gruppi amministrativi consentono di gestire i gruppi di computer client come una singola entità, applicando regole ed attività di gruppo.
6. Eseguire l'installazione remota di Network Agent sui computer client, per consentire l'interazione tra le loro applicazioni antivirus e l'Administration Server (vedere la sezione 2.5 a pagina12).
7. Installare in remoto sui computer client selezionati le applicazioni Kaspersky Lab che garantiscono la protezione antivirus della rete aziendale e supportano l'amministrazione tramite Kaspersky Administration Kit (vedere la sezione 2.6 a pagina13). Se tali applicazioni sono già installate, questo passaggio non è necessario.
8. Impostare l'aggiornamento via Internet del database antivirus dall'Administration Server, e verificare che l'operazione venga eseguita correttamente. Verificare che i database dei computer client vengano aggiornati (vedere la sezione 2.7 a pagina14).

9. Impostare le opzioni relative alla notifica all'amministratore di eventi relativi a virus sui computer client (vedere la sezione 2.8 a pagina15).
10. Eseguire una scansione manuale sui computer client e verificare la funzione di notifica sugli stessi (vedere la sezione 2.9 a pagina16).
11. Visualizzare un report sulla protezione antivirus dei computer client e sul numero dei virus rilevati dalle applicazioni Kaspersky Lab (vedere la sezione 2.10 a pagina17).

Completati i passaggi sopra descritti, si è realizzato un sistema di protezione antivirus affidabile e sicuro per la rete aziendale.

Le sezioni seguenti descrivono tali passaggi in maggior dettaglio.

2.1. Installazione di MSDE 2000

È possibile omettere questo passaggio se sulla rete erano stati precedentemente installati MSDE 2000 SP 3, Microsoft SQL 2000 SP 3, MySQL 5.0.22 (codepage predefinita UTF-8), Microsoft SQL 2005 o superiore o Microsoft SQL 2005 Express o superiore.

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).

È possibile omettere questo passaggio se sulla rete erano stati precedentemente installati Microsoft Development Environment (MSDE) 2000 SP 3 o SQL Server 2000 SP 3.

Per installare MSDE 2000 dal pacchetto incluso in Kaspersky Administration Kit,

1. Selezionare un computer su cui installare il database di Administration Server. Normalmente, si tratterà del medesimo computer su cui verrà installato l'Administration Server stesso.
2. Eseguire localmente il file **setup.exe** nella directory **MSDE2KSP3** del CD di installazione di Kaspersky Administration Kit 5.0.
3. Eseguire le istruzioni del programma di installazione guidata.

Al termine di questi passaggi, l'applicazione MSDE 2000 SP 3 risulterà installata sul computer selezionato. MSDE 2000 SP 3 non necessita di amministrazione.

La versione di MSDE qui indicata può essere utilizzata solamente con Kaspersky Administration Kit.

Administration Server si serve di MSDE 2000 SP 3 o SQL Server 2000 SP 3 per salvare i dati relativi alla protezione antivirus in un database centrale.

L'applicazione **klbackup** in dotazione con il pacchetto di distribuzione di Kaspersky Administration Kit crea copie di backup dei dati contenuti nell'Administration Server. Per i dettagli relativi all'uso di questa utility, consultare la Guida dell'Amministratore.

2.2. Installazione di Administration Server e Administration Console

Durante l'installazione, si può scegliere se installare sia Administration Server che Administration Console, o solamente Administration Console. Non è invece possibile installare Administration Server da solo. L'opzione predefinita prevede comunque l'installazione di entrambi i componenti.

Se necessario, è possibile installare l'applicazione Administration Console su un altro computer e gestire Administration Server attraverso la rete.

Per installare Administration Server e/o Administration Console,

1. Selezionare il computer su cui installare i componenti. Se nella rete è presente una struttura di dominio Windows, si raccomanda di installare Administration Server su un componente di tale dominio.

È possibile installare Administration Server 6.x su una macchina in cui sia già presente Administration Server 4.x. Gli Administration Server delle versioni 6.x e 4.x sono indipendenti l'uno dall'altro, e possono operare in maniera concomitante sulla stessa macchina senza problemi di compatibilità.

Ai fini dell'installazione del prodotto è consigliabile disporre dei diritti di amministratore di dominio, che consentono di creare automaticamente i gruppi **KLAdmins** e **KLOperators** e di fornire le necessarie credenziali per gli account in cui Administration Server sarà operativo.

2. Eseguire il file setup.exe dal disco di installazione di Kaspersky Administration Kit 5.
3. Seguire le istruzioni fornite dal programma di installazione.

Selezionare l'account del dominio dell'amministratore quale account di servizio sotto il quale Administration Server sarà avviato su questa macchina.


2.3. Avvio rapido

Per eseguire la configurazione iniziale delle impostazioni della protezione antivirus,

1. Eseguire Administration Console facendo clic su **Start → Tutti i programmi → Kaspersky Administration Kit → Kaspersky Administration Kit**.
2. Connettersi all'Administration Server facendo clic sul nodo corrispondente nella struttura della console. Accettare il certificato del server.
3. Aprire il menu di scelta rapida e selezionare **Avvio rapido**.
4. Attendere che Administration Server abbia rilevato tutti i computer presenti in rete.
5. Creare i gruppi di amministrazione utilizzando uno dei seguenti metodi:
 - Se si sta eseguendo una prova su un numero ridotto di macchine, selezionare l'opzione **Manuale** per aggiungere manualmente i computer client al gruppo.
 - Se si sta allestendo un sistema di protezione antivirus sull'intera rete aziendale, selezionare uno dei seguenti metodi per la creazione di reti logiche:
 - **Aggiunta di computer ad un gruppo per mezzo dei servizi di rete di Windows**. In questo caso, la rete logica sarà basata sulla struttura dei domini e gruppi utente Windows (i gruppi di amministrazione coincideranno con domini e gruppi utente Windows).

- o **Aggiunta di computer ad un gruppo per mezzo della struttura della precedente versione di Kaspersky Administration Kit.** In questo caso, la rete logica si baserà sulla rete di Kaspersky Administration Kit 4.x.
6. Specificare le opzioni per l'invio tramite e-mail di notifiche generate dalle applicazioni Kaspersky Lab. Queste impostazioni possono essere visualizzate come parte delle proprietà di Administration Server. Per maggiori informazioni, vedere la Guida dell'Amministratore.
 7. Lanciare un processo che crei regole per le applicazioni antivirus e più attività che configurino il corretto funzionamento del sistema di protezione antivirus nella rete aziendale. Kaspersky Administration Kit 5 utilizza le regole di gruppo per applicare le impostazioni in modo uniforme a tutte le macchine del gruppo stesso. Le attività sono azioni eseguite dal programma antivirus su tutte le macchine di un gruppo.

Verranno creati i seguenti oggetti:

- Regole di livello superiore per Kaspersky Anti-Virus for Windows Workstations 5.0 e 6.0 con impostazioni predefinite. Successivamente, sarà possibile visualizzare e modificare le impostazioni della regola. Per applicare le regole che sono state apportate alla regola nei computer client e impedire che gli utenti possano modificarne le impostazioni, utilizzare il simbolo .
- Un'attività globale per l'aggiornamento di Administration Server via Internet.

L'applicazione provvederà a scaricare gli aggiornamenti, sia del database antivirus che dei moduli di programma, dai server di aggiornamento di Kaspersky Lab, salvandoli nella cartella condivisa specificata durante l'installazione di Administration Server. I computer client potranno recuperare tali aggiornamenti da detta cartella. Successivamente, per ottenere una maggiore flessibilità quando i computer client recuperano gli aggiornamenti, è possibile utilizzare la distribuzione degli aggiornamenti agli Administration Server slave e gli Agenti di aggiornamento (per maggiore dettagli, vedere la Guida dell'amministratore). Per configurare l'aggiornamento delle impostazioni di recupero degli aggiornamenti dai server di aggiornamento di Kaspersky Lab, fare clic sul pulsante **Impostazioni aggiornamento**.

- Sarà creata un'attività di gruppo di ordine superiore, con impostazioni predefinite, per l'aggiornamento dei database antivirus sui computer client. I computer client saranno configurati in modo da recuperare gli aggiornamenti dalla cartella condivisa.
 - Sarà creata un'attività di scansione manuale per i computer client, con impostazioni predefinite.
8. Indicare se l'attività di ricezione degli aggiornamenti tramite l'Administration Server debba essere lanciata immediatamente o secondo quanto programmato.
 9. Nell'ultima finestra, indicare se la Procedura di distribuzione guidata debba essere lanciata subito dopo il completamento della Procedura guidata di avvio rapido.

2.4. Creazione di un gruppo di amministrazione

Per aggiungere un nuovo gruppo alla rete logica,

1. Nella struttura ad albero della console o nella cartella **Gruppi** nel riquadro dei dettagli, selezionare un gruppo cui aggiungere un gruppo nuovo. Aprire il menu di scelta rapida e fare clic su **Nuovo → Gruppo** per avviare l'installazione guidata del nuovo gruppo. Seguire le istruzioni fornite dal programma di installazione.
2. Spostare i computer client dal gruppo **Rete** al nuovo gruppo utilizzando i comandi copia-incolla o trascinamento.

Per creare un insieme di computer da includere nel gruppo amministrativo in base a determinati criteri, utilizzare il comando **Trova computer** del menu di scelta rapida (o il comando analogo dal menu **Azione**). Per maggiori dettagli vedere la Guida dell'amministratore.

L'Anti-Virus 4.x di Kaspersky Lab può operare sui computer client selezionati. I sistemi di amministrazione per le versioni 4.x e 6.x lavorano indipendentemente l'uno dall'altro. In caso di installazione di Kaspersky Anti-Virus 6.x sulla versione 4.x, quest'ultima verrà automaticamente eliminata e sovrascritta dalla versione 6.x.

2.5. Installazione remota di Network Agent

Per distribuire (installare in remoto) Network Agent da una postazione remota,

1. Lanciare la Distribuzione guidata dell'applicazione dal menu di scelta rapida di Administration Console in Administration Console.
2. Selezionare il pacchetto di installazione Network Agent creato dalla procedura di avvio rapido. Le impostazioni predefinite di questo pacchetto permettono all'utente di connettersi all'Administration Server subito dopo l'installazione di Network Agent.
3. Selezionare dal gruppo amministrativo di computer quelli sui quali si desidera installare Network Agent.
4. Configurare le impostazioni di installazione remota.
5. Se richiesto, inserire l'account per accedere ai computer client. Se l'account di servizio dell'Administration Server non dispone di diritti amministrativi per i computer client selezionati, utilizzare l'account predefinito.
6. Durante il prossimo passaggio della procedura guidata, verrà creata ed eseguita un'attività di gruppo relativa all'installazione di Network Agent sui computer client selezionati. Nella finestra della procedura guidata, è possibile visualizzare i risultati dell'esecuzione dell'attività in tempo reale.
7. A procedura ultimata, visualizzare il risultato dell'attività ed uscire dal programma di installazione guidata delle applicazioni.
8. Se si desidera controllare la protezione antivirus del computer in tempo reale, per verificare che l'Administration Server sia in grado di stabilire la connessione con Network Agent in qualsiasi momento dato, è necessario aprire la porta UDP nr. 15000 sul computer client. Se non è possibile aprire la porta UDP, selezionare la casella **Non interrompere la connessione con Administration Server** nella scheda **Generale** della finestra di dialogo **Proprietà:<Nome computer>** utilizzata per configurare le impostazioni del computer client.

Per verificare il successo dell'operazione, fare clic sull'opzione **Proprietà** del menu di scelta rapida di uno dei computer su cui Network Agent è stato appena

installato. Verificare che lo stato dell'applicazione Kaspersky Network Agent, nella scheda **Applicazioni**, corrisponda a **In corso**.

Se l'installazione è riuscita, ma Network Agent non è riuscito a connettersi all'Administration Server, utilizzare l'utility kinagchik.exe. Questa utility è inclusa nel kit di distribuzione di Network Agent e sarà disponibili nella cartella root d'installazione dopo aver installato questo componente. Quando viene seguita dalla riga di comando, questa utility consente la diagnostica dettagliata delle impostazioni di connessione di Administration Server. L'utility è descritta dettagliatamente nel Manuale di riferimento.

2.6. Installazione di Kaspersky Anti-Virus

Questa sezione descrive l'installazione di Kaspersky Anti-Virus for Windows Workstations da una postazione remota. L'installazione di altre applicazioni Kaspersky Lab procede in maniera analoga a quella sotto illustrata.

Alcune applicazioni di Kaspersky Lab che supportano l'amministrazione tramite Kaspersky Administration Kit possono essere installate sui computer client solo localmente (per dettagli, vedere la Guida specifica per l'applicazione).

Per installare Kaspersky Anti-Virus for Windows Workstations da una postazione remota su computer collegati in rete,

1. Creare un pacchetto di installazione per Kaspersky Anti-Virus for Workstations 5 usando il programma di installazione guidata. Esso si avvia tramite il nodo **Installazione remota** del menu di scelta rapida.

Il file **.kpd** necessario per creare il pacchetto di installazione è situato nella directory principale del file di distribuzione di Kaspersky Anti-Virus for Workstations. In tale directory si trova anche il file chiave della licenza dell'antivirus. Specificare il file della chiave di licenza utilizzato per il funzionamento di Kaspersky Anti-Virus for Windows Workstations.

Se necessario, configurare le impostazioni del pacchetto di installazione. Si raccomanda, per esempio, di abilitare il riavvio automatico per i computer client.

2. Avviare il programma di installazione guidata delle applicazioni dal menu di scelta rapida di Administration Server.

3. Installare Kaspersky Anti-Virus for Workstations dal pacchetto di installazione, analogamente a quanto visto per Network Agent (vedere la sezione 2.5 a pagina 12). È anche possibile installare Network Agent con Kaspersky Anti-Virus for Windows Workstation.

È possibile installare Kaspersky Anti-Virus 5.x su computer sui quali siano già presenti applicazioni della versione 4.x. In questo caso, le applicazioni 4.x saranno automaticamente sovrascritte dalla successiva versione 6.x.

Per verificare che l'installazione sia avvenuta correttamente, selezionare un computer client su cui l'applicazione sia stata appena installata, ed aprire la sua finestra Proprietà. Selezionare la scheda **Applicazioni** e verificare che lo stato dell'applicazione Kaspersky Anti-Virus for Workstations 5 corrisponda a **In corso**. La scheda **Attività** deve visualizzare l'attività di protezione in tempo reale eseguita da Kaspersky Anti-Virus for Workstations 5.

2.7. Verifica del funzionamento dell'attività di aggiornamento

Per verificare che i computer client recuperino correttamente gli aggiornamenti,

1. Eseguire l'attività di aggiornamento su Administration Server dal nodo **Attività** nella parte superiore della struttura ad albero della console. Questa attività viene creata automaticamente dal programma di installazione guidata. L'applicazione scaricherà gli aggiornamenti dai server preposti Kaspersky Lab e li salverà nella cartella condivisa specificata durante l'installazione dell'Administration Server. Attendere che l'operazione sia completata.

Fare clic sul pulsante **Cronologia** per visualizzare il risultato dell'operazione.

Per un elenco degli aggiornamenti scaricati, fare clic sul nodo **Aggiornamenti** nella struttura ad albero della console.

Dettagli relativi alla procedura di aggiornamento sono disponibili presso il sito web di Kaspersky Lab (<http://www.kaspersky.ru/avupdates>).

2. Eseguire l'attività di aggiornamento dei gruppi sui computer client. Questa attività è generata dalla procedura di Avvio rapido guidato ed è

accessibile dalla cartella **Attività** del nodo **Gruppo**. Attendere che l'operazione sia completata.

Fare clic sul pulsante **Cronologia** per visualizzare il risultato dell'operazione.

L'attività creata dalla procedura guidata di Avvio rapido aggiorna i computer client mediante la connessione tra Network Agent e Administration Server. Sono supportati inoltre i seguenti metodi di aggiornamento dei computer client:

- Dalla cartella condivisa del server amministrativo;
- Dalla cartella condivisa dell'Administration Server principale (se si utilizza la gerarchia Server).
- Dai server di aggiornamento di Kaspersky Lab.
- Tramite un server FTP o HTTP;
- Mediante il server FTP.


Per copiare l'aggiornamento più recente dalla cartella condivisa, il computer client deve poter accedere in lettura alla cartella stessa. Se ciò non è possibile per qualsiasi ragione, è possibile scaricare l'aggiornamento sul computer client tramite un server FTP o HTTP. Creare una directory FTP o HTTP collegata alla sottocartella **Aggiornamenti** nella cartella condivisa in cui Administration Server salverà gli aggiornamenti scaricati (ad esempio, ftp://admserver/updates). Specificare questa cartella (ftp://admserver/updates) quale sorgente dell'aggiornamento per la funzione di aggiornamento eseguita sui computer client.

2.8. Configurazione delle notifiche

Per configurare la notifica di eventi relativi alla protezione antivirus,

1. Selezionare la scheda **Elaborazione eventi** dalle proprietà delle regole di livello superiore per un'applicazione antivirus (per esempio, Kaspersky Anti-Virus for Workstations).
2. In questa scheda, selezionare gli eventi di cui si desidera avere notifica ed il modo in cui si desidera che questa sia inviata.

Per collaudare il sistema di notifica (vedere la sezione 2.9 a pagina 16), abilitare la notifica dell'**individuazione di un virus**.

3. Utilizzare il simbolo  per tutte le impostazioni configurate per estenderle a tutti i computer client. Per applicare le modifiche scegliere il pulsante **Applica**.
4. È possibile verificare le impostazioni configurate inviando manualmente un messaggio. Per fare ciò, scegliere il pulsante **Prova**. In conseguenza, si aprirà una finestra di notifica della prova. In caso di errori, verranno visualizzate informazioni dettagliate su di essi.

2.9. Collaudo del sistema di notifica e dell'attività di scansione manuale

Per collaudare il sistema di notifica e l'attività di scansione manuale,

1. Provare a copiare il virus di prova **Eicar** sul computer protetto. La copia non andrà a buon fine se è attiva la funzione di protezione in tempo reale. Si dovrebbe ricevere la notifica dell'intercettazione del virus, e questo evento verrà registrato anche nel nodo **Eventi** della struttura ad albero della console.

Il "virus di prova" Eicar non è a tutti gli effetti un virus, poiché non contiene alcun codice potenzialmente dannoso per la macchina in esame. Comunque, la maggior parte dei prodotti antivirus lo segnala come tale. È possibile scaricare il "virus di prova" dal sito web ufficiale dell'organizzazione **EICAR** all'indirizzo http://www.eicar.org/anti_virus_test_file.htm.

2. Interrompere l'attività di protezione in tempo reale sul computer client. Copiare il virus di prova **Eicar** sul computer client ed abilitare nuovamente l'attività di protezione in tempo reale.
3. Avviare l'attività di gruppo di scansione manuale per un gruppo di computer client. Come risultato, l'applicazione individuerà il file eicar.com ed invierà la relativa notifica. Nel nodo **Eventi** della struttura ad albero della console comparirà la registrazione di tale evento.

2.10. Generazione di report

L'applicazione è in grado di generare report sullo stato corrente del sistema di protezione antivirus dai dati del registro eventi di Kaspersky Administration Kit salvati nell'Administration Server. È possibile accedere ai modelli predefiniti dei report dal nodo **Report** della struttura della console.

Vi sono sei modelli standard, che corrispondono ai seguenti tipi di report:

- **Report della versione dei database dell'antivirus**
- **Report errori**
- **Report autorizzazioni**
- **Report dei desktop più infettati**
- **Report protezione**
- **Report versione software**
- **Report dell'attività antivirus**
- **Report delle applicazioni di terzi**
- **Report degli attacchi di rete.**

Per esempio, un report dell'attività antivirus creato attraverso il modello corrispondente conterrà informazioni relative a tutti i rilevamenti di virus registrati da Kaspersky Administration Kit.

Aggiungendo un computer sprovvisto di Network Agent ad un gruppo di amministrazione, il report della protezione conterrà un'informazione relativa alla presenza, nel gruppo, di un computer non protetto.

Capitolo 3. Aggiornamento della versione 4.x alla 6.x

Questa sezione illustra la procedura di aggiornamento delle applicazioni Kaspersky Lab versione 4.x a Kaspersky Anti-Virus for Workstations versione 6.x o Kaspersky Anti-Virus for Windows Server versione 6.x. Alcuni particolari sono già stati descritti in precedenza. Qui troverete istruzioni passo-passo per una transizione senza problemi.

Kaspersky Administration Kit 6.x funziona indipendentemente da Kaspersky Administration Kit 4.x. Il sistema di amministrazione per la versione 5.x gestisce solo le applicazioni della versione 5.x e 6.x, mentre il sistema di amministrazione 4.x gestisce la versione 4.x. Di conseguenza, durante la transizione i due sistemi di amministrazione possono operare parallelamente sui computer collegati alla rete.

Di seguito viene fornita una panoramica di una tipica transizione:

1. Installare la versione 6.x di Administration Server. È possibile installarla sullo stesso computer della versione 4.x.
2. Creare una rete logica di gruppi di amministrazione per le applicazioni 6.x. Tale struttura può essere importata dal sistema di amministrazione 4.x.
3. Creare privilegi e attività di gruppo sulla rete logica per le applicazioni 5.x e 6.x. Configurare le impostazioni richieste per la protezione antivirus e stabilire le regole per l'elaborazione degli eventi relativi a tale protezione.
4. Specificare quali computer passeranno dalla versione 4.x alla 5.x e 6.x.
5. Creare un pacchetto di installazione per le applicazioni della versione 5.x e 6.x, ed installare le applicazioni 5.x e 6.x sui computer selezionati. Nel corso del processo, le applicazioni 4.x saranno automaticamente sovrascritte dalle versioni 5.x e 6.x.
6. I computer su cui si installa la versione 5.x del software antivirus vengono annessi alla rete logica della versione 5.x dell'Administration Server, mentre gli altri computer continueranno ad essere gestiti dall'Administration System 4.x.

In questo modo, il sistema di protezione antivirus dell'azienda, basato sulla versione precedente, si trasferirà progressivamente alle versioni 5.x e 6.x delle applicazioni gestite dalla versione 6.x del sistema di amministrazione.

Capitolo 4. Conclusioni

Kaspersky Administration Kit 5 offre una grande varietà di strumenti di amministrazione, oltre a quelli menzionati in questo documento. La presente guida ha lo scopo di descrivere Kaspersky Administration Kit 5 e di introdurre l'utente all'utilizzo delle sue applicazioni e all'allestimento di un sistema di protezione antivirus per i computer collegati in rete. Questa semplice panoramica affronta gli aspetti di base relativi all'approntamento di un sistema di protezione efficace, permettendo all'amministratore di:

- Installare e configurare il sistema di amministrazione della protezione antivirus
- Installare le applicazioni antivirus sui computer client da una singola postazione
- Definire un sistema di protezione antivirus
- Creare e valutare sul piano operativo un'attività di aggiornamento per i computer client
- Collaudare la funzionalità della funzione di protezione in tempo reale
- Creare e collaudare la funzione di scansione manuale dei computer client
- Impostare i parametri per l'invio delle notifiche dopo gli eventi critici
- Generare e visionare rapporti creati dal sistema di protezione antivirus

Appendice A. 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.A.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 progettato 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 (incluse le liste nere DNS e le caratteristiche della posta formale) e una raccolta esclusiva di servizi che consentono agli utenti di individuare ed eliminare fino al 95% del traffico indesiderato.

Installato all'ingresso di una rete, 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.A.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	Trovi le informazioni di supporto tecnico su http://www.kaspersky.com/supportinter.html Helpdesk: http://www.kaspersky.com/helpdesk.html
Informazio ni generali	WWW: http://www.kaspersky.com http://www.viruslist.com E-mail: info@kaspersky.com

Appendice B. 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 E 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 e 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 modalita server. Il Software puo essere usato su un Dispositivo del cliente o su o come server ("Server") in un ambiente multiutente o di rete ("Modalita server") solo se tale uso e consentito in base al listino prezzi applicabile o alla confezione del Software. E 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 e 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 postazione concessi in licenza necessario per il suo utilizzo ai termini di legge, a condizione che ogni copia contenga tutte le informazioni sui diritti di proprieta della Documentazione.

1.3 Licenze per volume di acquisto. Se il Software e concesso dietro una licenza per volume le cui condizioni sono specificate nella fattura applicabile del prodotto o sull'imballo del Software, l'utente puo 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 e 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 proprieta della Documentazione.

2. Durata. Il presente Contratto e 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. È possibile recedere dal presente Contratto in qualsiasi momento distruggendo tutte le copie del Software e della Documentazione.

3. Assistenza.

(i) Kaspersky Lab metterà a disposizione dell'utente i servizi di assistenza ("Servizi di assistenza") specificati di seguito, per la durata di un anno, 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 proprietà. Il Software è protetto dalle leggi sul copyright. Kaspersky Lab e i relativi fornitori possiedono e mantengono tutti i diritti, l'autorità e gli interessi del Software e ad esso correlati, inclusi tutti i diritti di proprietà, i brevetti, i marchi commerciali e gli altri diritti di proprietà intellettuale ad esso connessi. Il possesso, l'installazione o l'utilizzo del Software non trasferiscono all'utente alcun diritto relativo alla proprietà intellettuale del Software e non determinano l'acquisizione di diritti sul Software salvo quelli espressamente indicati nel presente Contratto.

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 dovrà divulgare, fornire o altrimenti rendere disponibili tali informazioni riservate in qualsivoglia forma a terzi senza previo consenso scritto di Kaspersky Lab. Dovrà inoltre applicare ragionevoli misure di sicurezza volte a proteggere tali informazioni riservate ma, senza tuttavia limitarsi a quanto sopra espresso dovrà fare quanto in suo potere per tutelare la sicurezza del 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 opererà sostanzialmente in conformità alle funzioni descritte nella Documentazione, a condizione che sia utilizzato in modo corretto e nella maniera specificata nella Documentazione.

(ii) L'utente si assume ogni responsabilità relativamente al fatto che il presente Software soddisfi i propri requisiti. Kaspersky Lab non garantisce che il Software e/o la Documentazione siano idonei a soddisfare le esigenze dell'utente né che il suo utilizzo sia esente da interruzioni o privo di errori.

(iii) Kaspersky Lab non garantisce che il Software identifichi tutti i virus noti né esclude che possa occasionalmente eseguire il report erroneo di un virus in un titolo non infettato da quel virus.

(iv) L'indennizzo dell'utente e la completa responsabilità di Kaspersky Lab per la violazione della garanzia di cui al paragrafo (i) saranno a discrezione di Kaspersky Lab, che deciderà se riparare, sostituire o rimborsare il Software in caso di reclamo a Kaspersky Lab o suoi fornitori durante il periodo di garanzia. L'utente dovrà fornire tutte le informazioni ragionevolmente necessarie per agevolare il Fornitore nel ripristino dell'articolo difettoso.

(v) La garanzia di cui al punto (i) non è applicabile qualora l'utente (a) apporti modifiche al presente Software o determini la necessità di modificarlo senza il consenso di Kaspersky Lab, (b) utilizzi il Software in modo difforme

dall'uso previsto o (c) impieghi il Software per usi diversi da quelli permessi ai sensi del presente Contratto.

(vi) Le garanzie e le condizioni specificate in questo Contratto sostituiscono qualsiasi altra condizione, garanzia o termine relativi alla fornitura o alla presunta fornitura, all'impossibilit  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 responsabilita 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 responsabilita 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 liquidita;
- (d) perdita di risparmi presunti;
- (e) perdita di affari;
- (f) perdita di opportunita;
- (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 responsabilita di Kaspersky Lab (relativamente al contratto, per responsabilita 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 conformita 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).

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).