

Kaspersky Mobile Security 9

per Microsoft Windows Mobile

KASPERSKY **lab**

Guida dell'utente

VERSIONE DEL PROGRAMMA: 9.0

Gentile Utente!

Grazie per aver scelto il nostro prodotto. Ci auguriamo che questa documentazione possa essere di grande utilità nel lavoro e fornisca sempre risposte ad ogni domanda sul presente prodotto software.

Nota! Il presente documento è di proprietà di Kaspersky Lab ZAO (di seguito denominata Kaspersky Lab): tutti i diritti relativi al documento sono riservati dalle leggi sui diritti d'autore e dalle disposizioni dei trattati internazionali. La riproduzione e la distribuzione non autorizzate del presente documento, interamente o in parte, possono comportare gravi responsabilità civili, amministrative e penali, in conformità alle leggi applicabili.

La riproduzione o distribuzione di qualunque materiale in qualunque formato, incluse le traduzioni, è consentita previo consenso scritto di Kaspersky Lab.

Il presente documento e le immagini in esso contenute può essere utilizzato esclusivamente per scopi informativi non commerciali e personali.

Kaspersky Lab si riserva il diritto di modificare il presente documento senza ulteriore preavviso. È possibile reperire la versione più recente del presente documento sul sito Web di Kaspersky Lab all'indirizzo <http://www.kaspersky.com/docs>.

Kaspersky Lab non potrà essere ritenuta responsabile per il contenuto, qualità, pertinenza o accuratezza di qualunque materiale utilizzato nel presente documento i cui diritti sono di proprietà di terzi o per perdite potenziale o effettive associate all'uso di tali materiali.

Nel presente documento sono utilizzati marchi registrati e marchi di servizio di proprietà dei detentori.

Data di revisione: 20.01.2011

© 1997-2011 Kaspersky Lab ZAO. Tutti i diritti riservati.

<http://www.kaspersky.it>
<http://www.kaspersky.com/it/service>

CONTRATTO DI LICENZA CON L'UTENTE FINALE KASPERSKY LAB

AVVERTENZA LEGALE IMPORTANTE PER TUTTI GLI UTENTI: LEGGERE ATTENTAMENTE IL SEGUENTE CONTRATTO PRIMA DI INIZIARE AD USARE IL SOFTWARE.

FACENDO CLICK SUL PULSANTE ACCETTO NELLA FINESTRA DEL CONTRATTO DI LICENZA O IMMETTENDO IL/I SIMBOLO/I CORRISPONDENTE/I, LEI ACCETTA DI ESSERE VINCOLATO AL RISPETTO DEI TERMINI E DELLE CONDIZIONI DI QUESTO CONTRATTO. **TALE AZIONE EQUIVALE AD APPORRE LA SUA FIRMA E SIGNIFICA CHE ACCETTA DI ESSERE VINCOLATO E DI DIVENTARE UNA PARTE CONTRAENTE DEL PRESENTE CONTRATTO E CHE ACCETTA LA VALIDITÀ LEGALE DEL PRESENTE CONTRATTO COME QUALSIASI ACCORDO STIPULATO PER ISCRITTO E DA LEI FIRMATO.** QUALORA NON SIA D'ACCORDO CON TUTTI I TERMINI E LE CONDIZIONI DEL PRESENTE CONTRATTO, ANNULLI L'INSTALLAZIONE DEL SOFTWARE E NON LO INSTALLI.

DOPO AVER FATTO CLICK SUL PULSANTE ACCETTO NELLA FINESTRA DEL CONTRATTO DI LICENZA O DOPO AVER IMMESSO IL/I SIMBOLO/I CORRISPONDENTE/I LEI HA DIRITTO AD UTILIZZARE IL SOFTWARE SECONDO I TERMINI E LE CONDIZIONI DEL PRESENTE CONTRATTO.

1. Definizioni

- 1.1. **Per Software** si intende il software, compresi gli aggiornamenti e i relativi materiali.
- 1.2. **Per Titolare** (titolare di tutti i diritti, sia esclusivi che non, relativi al Software) si intende Kaspersky Lab ZAO, una società regolarmente costituita ai sensi delle leggi della Federazione Russa.
- 1.3. **Per Computer** si intende l'hardware, ivi compresi i personal computer, i laptop, le postazioni di lavoro, i personal digital assistant, gli "smart phone", i dispositivi palmari o gli altri dispositivi elettronici per cui il Software è stato progettato su cui il Software verrà installato e/o utilizzato.
- 1.4. **Per Utente Finale (Lei/Suo)** si intende il soggetto o i soggetti che installano o utilizzano il Software per proprio conto e che sta/stanno utilizzando legalmente una copia del Software; o, se il Software è stato scaricato o installato per conto di un'organizzazione, ad esempio da un dipendente, "Lei" sta a intendere anche l'organizzazione per cui il Software è stato scaricato o installato e si dichiara con il presente che tale organizzazione ha autorizzato quel soggetto ad accettare questo contratto, scaricando e installando il Software per conto dell'organizzazione stessa. Ai fini del presente contratto il termine "organizzazione" include, a titolo esemplificativo e non limitativo, qualsiasi società di persone, società a responsabilità limitata, persona giuridica, associazione, società per azioni, trust, joint venture, organizzazione sindacale, organizzazione non registrata o autorità governativa.
- 1.5. **Per Partner** si intendono le organizzazioni o il soggetto/i soggetti che distribuiscono il Software al Titolare sulla base di un contratto e di una licenza.
- 1.6. **Per Aggiornamento/i** si intendono tutti gli aggiornamenti, le revisioni, le patch, i perfezionamenti, le correzioni, le modifiche, le copie, le aggiunte o i pacchetti di manutenzione, ecc.
- 1.7. **Per Manuale dell'Utente** si intende il manuale dell'utente, la guida per l'amministratore, il libro di riferimento e i relativi materiali di tipo illustrativo o di altro tipo.

2. Concessione della licenza

- 2.1. Con il presente il Titolare Le concede licenza di uso non esclusivo per la memorizzazione, il caricamento, l'installazione, l'esecuzione e la visualizzazione ("uso") del Software su di una quantità specificata di Computer al fine di fornire un supporto per la protezione del Suo Computer, sul quale è installato il Software, contro le minacce descritte nel Manuale dell'Utente, in osservanza di tutti i requisiti tecnici descritti nel Manuale dell'Utente e secondo i termini e le condizioni di questo Contratto (la "Licenza") e Lei accetta questa Licenza: Versione di prova. Se ha ricevuto, scaricato e/o installato la versione di prova del Software e se ha aderito alla licenza di valutazione del Software, può utilizzare il Software solo a scopo dimostrativo e soltanto per il periodo dimostrativo consentito, salvo laddove diversamente indicato, a partire dalla data della prima installazione. È severamente proibito l'uso del Software per scopi diversi o per un periodo più lungo del periodo di valutazione consentito.

Software per ambiente multiplo; Software a linguaggio multiplo; Software a doppio supporto magnetico; Copie multiple; Servizi aggiuntivi. Qualora Lei utilizzi diverse versioni del Software o edizioni del Software di lingua diversa, o riceva il Software su diversi supporti magnetici, o comunque riceva copie multiple del Software, ovvero qualora in cui Lei abbia acquistato il Software insieme a software aggiuntivi, il numero massimo di Computer su cui il Software può essere installato deve corrispondere al numero di computer specificato nelle licenze ricevute dal Titolare *sempre che* ogni licenza acquisita Le dia diritto a installare e utilizzare il Software sulla quantità numero di Computer specificata nei paragrafi 2.2 e 2.3, salvo laddove diversamente stabilito dai termini della licenza.

- 2.2. Se il Software è stato acquisito su un supporto fisico, Lei ha il diritto di utilizzare il Software per proteggere la quantità di Computer specificata nel pacchetto Software o secondo quanto specificato nel contratto aggiuntivo.

- 2.3. Se il Software è stato acquisito via Internet, Lei ha il diritto di utilizzare il Software per la protezione della quantità di Computer specificata all'atto dell'acquisizione della Licenza del Software o secondo quanto specificato nel contratto aggiuntivo.
- 2.4. Lei ha diritto di copiare il Software soltanto a scopo di back-up e solo a titolo di sostituzione della copia di Sua legale proprietà, qualora essa vada persa, distrutta o diventi inutilizzabile. Questa copia di back-up non può essere utilizzata per fini diversi e deve essere distrutta quando viene meno il diritto d'uso del Software o alla scadenza della Sua licenza o qualora questa venga meno per qualsiasi altro motivo, ai sensi della legislazione in vigore nel principale paese di residenza o nel paese in cui Lei fa uso del Software.
- 2.5. Dal momento in cui si procede all'attivazione del Software o dopo l'installazione del file della chiave di licenza (a eccezione della versione di prova del Software), Lei ha diritto di ricevere i seguenti servizi per il periodo di tempo specificato sul pacchetto Software (se il Software è stato acquisito su supporto fisico) o specificato durante l'acquisizione (se il Software è stato acquisito via Internet):
- Aggiornamenti del Software via Internet quando e nel momento in cui il Titolare li pubblica sul suo sito o attraverso altri servizi online. Qualsiasi Aggiornamento di cui Lei possa essere destinatario costituisce parte del Software e a esso si applicano i termini e le condizioni di questo Contratto;
 - Supporto Tecnico via Internet e Hotline telefonica di Supporto Tecnico.

3. Attivazione e validità

- 3.1. Nel caso in cui Lei apportasse modifiche al Suo computer o al software di altri fornitori installato su di esso, il Titolare ha la facoltà di chiederLe di ripetere l'attivazione del Software o l'installazione del file della chiave di licenza. Il Titolare si riserva il diritto di utilizzare qualsiasi mezzo e qualsiasi procedura per verificare la validità della Licenza e/o la validità legale della copia del Software installata e/o utilizzata sul Suo Computer.
- 3.2. Se il Software è stato acquisito su supporto fisico, esso può essere utilizzato previa accettazione del presente Contratto per il periodo specificato sulla confezione a far data dalla data di accettazione del presente Contratto o secondo quanto specificato nel contratto aggiuntivo.
- 3.3. Se il Software è stato acquisito via Internet, il Software può essere utilizzato previa accettazione del presente Contratto per il periodo specificato durante l'acquisizione o secondo quanto specificato nel contratto aggiuntivo.
- 3.4. Lei ha diritto di usare la versione di prova del Software secondo quanto disposto dal Paragrafo 2.1 senza alcun addebito unicamente per il periodo di valutazione (7 giorni) concesso dal momento della sua attivazione ai sensi del presente Contratto, *purché* la versione di prova non dia diritto ad Aggiornamenti e a Supporto Tecnico via Internet e tramite Hotline telefonica. Qualora il Titolare stabilisca una durata diversa per il singolo periodo di valutazione applicabile, Lei ne sarà informato per mezzo di una notifica.
- 3.5. La Sua Licenza d'Uso del Software è limitata al periodo di tempo specificato nei Paragrafi 3.2 o 3.3 (secondo quanto applicabile) e nel periodo restante può essere visionata utilizzando i supporti descritti nel Manuale dell'Utente.
- 3.6. Nel caso in cui Lei abbia acquisito il Software per un utilizzo su più di un Computer, la Sua Licenza d'Uso del Software è limitata al periodo di tempo che ha inizio alla data di attivazione del Software o l'installazione del file della chiave di licenza sul primo Computer.
- 3.7. Fatto salvo qualsiasi altro rimedio previsto dalla legge o basato sui principi di opportunità, giustizia e onesta composizione ("equity") a cui il Titolare possa legittimamente fare ricorso, nel caso di una Sua violazione dei termini e delle condizioni del presente Contratto, il Titolare avrà diritto in ogni momento e senza obbligo di preavviso di rescindere questa Licenza d'uso del Software senza rimborsare il prezzo d'acquisto né parte di esso.
- 3.8. Lei accetta di fare uso del Software e utilizzare qualsiasi rapporto o informazione derivante dall'utilizzo di questo Software in modo conforme a tutte le leggi applicabili internazionali, nazionali, statali, regionali e locali e a qualsiasi normativa, ivi compresa, a titolo esemplificativo e non limitativo, le leggi sulla privacy, sui diritti d'autore, sul controllo delle esportazioni e sulle oscenità.
- 3.9. Fatte salve eventuali disposizioni contrarie specificamente previste in questa sede, Lei non ha la facoltà di trasferire né di assegnare alcuno dei diritti che le sono stati concessi ai sensi del presente Contratto né alcuno degli obblighi che da esso Le derivano.
- 3.10. Se Lei ha acquisito il Software con un codice di attivazione valido per la localizzazione del Software nella lingua della regione in cui è stato acquisito dal Titolare o dai suoi Partner, non può attivare il Software applicando il codice di attivazione destinato alla localizzazione in un'altra lingua.
- 3.11. Se Lei ha acquisito il Software destinato all'utilizzo con uno specifico gestore delle telecomunicazioni, il Software è utilizzabile esclusivamente per il funzionamento con il gestore specificato durante l'acquisizione.
- 3.12. Nel caso delle limitazioni specificate nelle Clausole 3.10 e 3.11, le informazioni relative a tali limitazioni sono riportate sull'imballaggio e/o nel sito Web del Titolare e/o dei suoi Partner.

4. Supporto Tecnico

Il Supporto Tecnico descritto al Paragrafo 2.5 del presente Contratto Le viene fornito quando è stato installato l'Aggiornamento più recente del Software (a eccezione della versione di prova del Software).

Servizio di assistenza tecnica: <http://support.kaspersky.com>

5. **Restrizioni**

- 5.1. Le è fatto divieto di emulare, clonare, locare, dare in prestito, noleggiare, vendere, modificare, decompilare o reingegnerizzare il Software, disassemblarlo o creare opere accessorie basate sul Software o su una porzione di esso con la sola eccezione di diritti non rinunciabili previsti dalla legislazione applicabile, e Le è fatto comunque divieto di ridurre parte del Software in forma decifrabile o trasferire il Software tutelato da licenza o qualsivoglia sottoinsieme dello stesso, o permettere a terzi di fare quanto sopra, salvo nella misura in cui le limitazioni sopra illustrate siano espressamente proibite dal diritto applicabile. È fatto divieto di utilizzare o reingegnerizzare qualsivoglia codice binario o origine del Software allo scopo di ricreare l'algoritmo del programma, che è proprietario. Tutti i diritti non espressamente concessi attraverso il presente Contratto sono riservati al Titolare e/o ai suoi fornitori, secondo quanto applicabile. L'uso non autorizzato del Software produrrà la rescissione immediata e automatica del presente Contratto e della Licenza concessa in virtù dello stesso e può determinare l'apertura di un procedimento legale nei Suoi confronti.
- 5.2. Fatto salvo quanto disposto in un contratto aggiuntivo, Lei non ha diritto di trasferire i diritti d'uso del Software a terzi.
- 5.3. Le è fatto divieto di mettere a conoscenza di terzi il codice di attivazione e/o il file chiave della licenza o di consentire l'accesso al codice di attivazione e/o di licenza, i quali rappresentano dati riservati del Titolare; Lei sarà inoltre tenuto a usare ogni ragionevole cautela per la protezione del codice di attivazione e/o di licenza riservati, qualora Lei abbia la facoltà di trasferire il codice di attivazione e/o di licenza a terzi secondo quanto illustrato in un contratto aggiuntivo.
- 5.4. Non è consentito concedere a noleggio, in locazione o in prestito a terzi il Software.
- 5.5. Non è consentito utilizzare il Software per la creazione di dati o di software che servono a individuare, bloccare o gestire le minacce descritte nel Manuale dell'Utente.
- 5.6. In caso di violazione dei termini e delle condizioni del presente Contratto, il Titolare ha il diritto di bloccare il file di codice o di annullare la Sua licenza d'uso del Software senza obbligo di rimborso.
- 5.7. Se si usa la versione di prova del Software non si ha il diritto di ricevere il Supporto Tecnico specificato al Paragrafo 4 del presente Contratto, né il diritto di trasferire la licenza o i diritti d'uso del software a terzi

6. **Garanzia limitata e clausola di esclusione della responsabilità**

- 6.1. Il Titolare garantisce che il Software eseguirà sostanzialmente le prestazioni illustrate nelle specifiche e descritte nel Manuale dell'Utente *fermo restando, tuttavia, che tale garanzia limitata non si applica a quanto segue: (w) lacune del Suo Computer e relative violazioni per le quali il Titolare declina espressamente qualsiasi responsabilità di garanzia; (x) malfunzionamenti, difetti o guasti conseguenti a cattivo uso, abuso, incidente, negligenza, difetti di installazione, funzionamento o manutenzione, furto, atto vandalico, evento di forza maggiore, atti di terrorismo, interruzione di tensione o momentanea sovratensione, infortunio, alterazione, modifica non consentita o riparazioni eseguite da soggetti diversi dal Titolare o qualsiasi azione o causa, a opera Sua o di qualsiasi altro soggetto terzo, ragionevolmente fuori del controllo del Titolare; (y) qualsiasi difetto da Lei tenuto nascosto al Titolare anche dopo la comparsa della prima anomalia; e (z) incompatibilità provocata da componenti hardware e/o software installati sul Suo computer.*
- 6.2. Lei riconosce, accetta e concorda che nessun software è esente da errori e che Lei è stato informato che è necessario fare il back-up del Computer, con la frequenza e secondo le modalità per Lei più indicate.
- 6.3. Lei riconosce, accetta e concorda che il Titolare non è responsabile né perseguibile per l'eliminazione di dati da Lei autorizzata. I dati in questione possono includere qualsiasi informazione di natura personale o riservata.
- 6.4. Il Titolare non garantisce che il Software funzionerà correttamente se Lei non scarica regolarmente gli Aggiornamenti specificati nel Paragrafo 2.5 del presente Contratto.
- 6.5. Il Titolare non garantisce la protezione dalle minacce descritte nel Manuale dell'Utente una volta scaduto il periodo specificato nei Paragrafi 3.2 or 3.3 del presente Contratto o una volta scaduta, per qualsiasi motivo, la Licenza d'uso del Software.
- 6.6. IL SOFTWARE VIENE FORNITO "COSÌ COM'È" E IL TITOLARE NON FA ALCUNA DICHIARAZIONE E NON FORNISCE ALCUNA GARANZIA IN QUANTO A USO O PRESTAZIONI. FATTE SALVE LE GARANZIE, LE CONDIZIONI, LE DICHIARAZIONI O I TERMINI CHE NON POSSONO ESSERE ESCLUSI O LIMITATI DAL DIRITTO APPLICABILE, IL TITOLARE E I SUOI PARTNER, NON FORNISCONO ALCUNA GARANZIA, CONDIZIONE, DICHIARAZIONE O TERMINE (NÉ ESPlicitO NÉ IMPLICITO NÉ PREVISTO DALLA LEGGE, DALLA *COMMON LAW*, DALLE CONSUETUDINI O DAGLI USI O ALTRO) IN MERITO A QUALSIVOGLIA QUESTIONE, IVI COMPRESSE, A TITOLO ESEMPLIFICATIVO E NON LIMITATIVO, LA NON VIOLAZIONE DEI DIRITTI DI TERZI, LA COMMERCIALIZZABILITÀ, LA QUALITÀ SODDISFACENTE, L'INTEGRAZIONE O L'APPLICABILITÀ PER UN FINE SPECIFICO. LEI SI ASSUME LA RESPONSABILITÀ DI TUTTI GLI ERRORI E TUTTI I RISCHI RELATIVI ALLE PRESTAZIONI NONCHÉ LA RESPONSABILITÀ DI AVER SCELTO IL SOFTWARE ALLO SCOPO DI RAGGIUNGERE I RISULTATI DESIDERATI NONCHÉ DELL'INSTALLAZIONE DEL SOFTWARE, DEL RELATIVO USO E DEI RISULTATI OTTENUTI DALLO STESSO. SENZA LIMITARE LE DISPOSIZIONI DI CUI SOPRA, IL TITOLARE NON FORNISCE ALCUNA DICHIARAZIONE E NON FORNISCE ALCUNA GARANZIA CHE IL SOFTWARE SARÀ ESENTE DA ERRORI O ESENTE DA INTERRUZIONI O ALTRI DIFETTI DI FUNZIONAMENTO NÉ CHE IL SOFTWARE SARÀ IN GRADO DI SODDISFARE IN TOTO O IN PARTE LE SUE ESIGENZE, SIANO ESSE STATE COMUNICATE AL TITOLARE O MENO.

7. Esclusione e limite della responsabilità

NELLA MASSIMA MISURA CONSENTITA DAL DIRITTO APPLICABILE, IN NESSUN CASO IL TITOLARE O I SUOI PARTNER SARANNO RESPONSABILI DI DANNI SPECIALI, MARGINALI, PUNITIVI, INDIRETTI O DI DANNI INDIRETTI DI QUALSIASI TIPO (IVI COMPRESI, A TITOLO ESEMPLIFICATIVO E NON LIMITATIVO, I DANNI PER PERDITA DI UTILI O PER PERDITA DI INFORMAZIONI RISERVATE O DI ALTRE INFORMAZIONI, PER INTERRUZIONE DELL'ATTIVITÀ LAVORATIVA, PER PERDITA DI PRIVACY, PER CORRUZIONE, DANNO E PERDITA DI DATI O DI PROGRAMMI, PER MANCATA OSSERVANZA DI UN OBBLIGO IVI COMPRESO QUALSIASI ONERE IMPOSTO PER LEGGE, DOVERE DI BUONA FEDE O DOVERE DI RAGIONEVOLE DILIGENZA, PER NEGLIGENZA, PER PERDITA ECONOMICA E PER QUALSIASI ALTRA PERDITA PECUNIARIA O ALTRA PERDITA DI SORTA) DERIVANTE DA O IN QUALSIASI MODO COLLEGATO ALL'USO O ALL'IMPOSSIBILITÀ DI USARE IL SOFTWARE, ALLA FORNITURA O MANCATA FORNITURA DEL SERVIZIO DI SUPPORTO O DI ALTRI SERVIZI, INFORMAZIONI, SOFTWARE E RELATIVI CONTENUTI ATTRAVERSO IL SOFTWARE O COMUNQUE DERIVANTI DALL'USO DEL SOFTWARE O COMUNQUE AI SENSI O IN RELAZIONE A QUALSIASI DISPOSIZIONE DEL PRESENTE CONTRATTO, O DERIVANTI DA UNA VIOLAZIONE DEL PRESENTE CONTRATTO O DA QUALSIVOGLIA ILLECITO (IVI COMPRESA LA NEGLIGENZA, LA FALSA TESTIMONIANZA, QUALSIASI OBBLIGO O DOVERE RELATIVI ALLA RESPONSABILITÀ) O DA UNA VIOLAZIONE DI UN OBBLIGO DI LEGGE O DA UNA VIOLAZIONE DELLA GARANZIA DA PARTE DEL TITOLARE O DI UNO DEI SUOI PARTNER, ANCHE QUALORA IL TITOLARE O UNO DEI SUOI PARTNER SIA STATO INFORMATO DELLA POSSIBILITÀ DI TALI DANNI.

LEI ACCETTA CHE NEL CASO IN CUI IL TITOLARE E/O SUOI PARTNER VENISSERO TROVATI RESPONSABILI, LA RESPONSABILITÀ DEL TITOLARE E/O DEI SUOI PARTNER SI LIMITERÀ AL COSTO DEL SOFTWARE. IN NESSUN CASO LA RESPONSABILITÀ DEL TITOLARE E/O DEI SUOI PARTNER POTRÀ SUPERARE LE SOMME VERSATE PER IL SOFTWARE AL TITOLARE O AL PARTNER (SECONDO QUANTO APPLICABILE).

NULLA IN QUESTO CONTRATTO ESCLUDE O LIMITA LA QUALSIVOGLIA RICHIESTA DI DANNI IN CASO DI MORTE E LESIONI PERSONALI. INOLTRE IN CASO IN CUI UNA MANLEVA, ESCLUSIONE O LIMITAZIONE CONTEMPLATE DAL PRESENTE CONTRATTO NON POSSA ESSERE ESCLUSA O LIMITATA AI SENSI DEL DIRITTO APPLICABILE, QUELLA MANLEVA, ESCLUSIONE O LIMITAZIONE NON SARÀ VALIDA NEI SUOI CONFRONTI E LEI DOVRÀ CONTINUARE A OSSERVARE TUTTE LE RESTANTI MANLEVE, ESCLUSIONI E LIMITAZIONI.

8. GNU e altre licenze di Terzi

Il Software può comprendere alcuni programmi software sottoposti a licenza (o a sublicenza) dell'utente ai sensi della GNU Licenza Pubblica Generica (General Public License, GPL) o ad altra licenza software di analoga natura che, tra gli altri, concede all'utente il diritto di copiare, modificare e ridistribuire certi programmi o porzioni di essi e di avere accesso al codice source ("Software Open Source"). Se tali licenze prevedono che per un software distribuito in formato binario eseguibile anche il codice source venga reso disponibile ai suoi utenti, il codice source deve essere reso accessibile inviando la richiesta all'indirizzo source@kaspersky.com, altrimenti il codice source verrà fornito insieme al Software. Se le licenze dei Software Open Source prevedono che il Titolare fornisca diritti d'uso, di copia e modifica del programma Software Open Source più ampi dei diritti concessi in virtù del presente Contratto, tali diritti avranno la priorità sui diritti e sulle restrizioni contemplati da questo documento.

9. Proprietà Intellettuale

9.1 Lei accetta che il Software e il fatto di esserne autori, i sistemi, le idee e i metodi operativi, la documentazione e altre informazioni contenute nel Software, sono proprietà intellettuale esclusiva e/o preziosi segreti commerciali del Titolare o dei suoi partner e che il Titolare e i suoi partner, secondo quanto applicabile, sono protetti dal diritto civile e penale e dalla legge sul copyright, sul segreto commerciale, sul marchio di fabbrica e sui brevetti della Federazione Russa, dell'Unione Europea e degli Stati Uniti e da altri trattati internazionali o di altri paesi. Il presente Contratto non Le concede alcun diritto di proprietà intellettuale né alcun diritto sui marchi o sui marchi di servizio del Titolare e/o dei suoi partner ("Marchi di fabbrica"). Lei ha la facoltà di usare i marchi di fabbrica solo nella misura in cui essi permettono di identificare le stampe prodotte dal Software in conformità con la pratica sui marchi generalmente accettata, ivi compresa l'identificazione del nome del proprietario del Marchio di fabbrica. Tale uso di un Marchio di fabbrica non Le conferisce alcun diritto di proprietà sul Marchio stesso. Il Titolare e/o i relativi partner possiedono e conservano ogni diritto, titolo e interesse relativo e collegato al Software, ivi comprese, senza alcuna limitazione, le correzioni d'errore, i perfezionamenti, gli Aggiornamenti o altre modifiche del Software, sia apportate dal Titolare che da Terzi nonché tutti i diritti d'autore, i brevetti, i diritti su segreti commerciali, i marchi di fabbrica e qualsiasi altro diritto di proprietà intellettuale ivi contemplato. Il possesso, l'installazione o l'uso del Software da parte Sua non Le trasferisce alcun titolo nella proprietà intellettuale del Software e Lei non acquisirà alcun diritto sul Software, salvo nella misura espressamente indicata nel presente Contratto. Tutte le copie del Software eseguite ai sensi del presente documento devono contenere le stesse avvertenze proprietarie che compaiono sul e nel Software. Fatto salvo quanto disposto in questo documento, il presente Contratto non Le conferisce alcun diritto di proprietà intellettuale sul Software e Lei riconosce che la Licenza, secondo la definizione data in seguito, concessa ai sensi del presente Contratto

Le conferisce soltanto il diritto di uso limitato ai termini e alle condizioni del presente Contratto. Il Titolare si riserva tutti i diritti che non Le sono espressamente concessi ai sensi del presente Contratto.

- 9.2 Lei riconosce che il codice source, il codice di attivazione e/o il file di codice di licenza per il Software sono proprietari del Titolare e che essi costituiscono segreto commerciale del Titolare. Lei accetta di non modificare, adattare, reingegnerizzare, decompilare, disassemblare, né comunque tentare di scoprire il codice source del Software.
- 9.3 Lei accetta di non modificare, né alterare in alcun modo il Software. Lei non ha la facoltà di rimuovere, né di alterare alcuna delle avvertenze in materia di diritti d'autore o altre avvertenze proprietarie sulle copie del Software.

10. Diritto applicabile; Arbitrato

Il presente Contratto sarà regolamentato dalle leggi della Federazione Russa e interpretato conformemente a esse, senza riferimento a conflitti fra stato di diritto e principi. Il presente Contratto non sarà regolamentato dalla Convenzione delle Nazioni Unite sui Contratti per la Vendita Internazionale di Merci, la cui applicazione è espressamente esclusa. Qualsiasi vertenza derivante dall'interpretazione o dall'applicazione dei termini del presente Contratto o dalla sua violazione dovrà essere regolata tramite trattativa diretta oppure dal Tribunale dell'Arbitrato Commerciale Internazionale avente sede presso la Camera di Commercio e dell'Industria della Federazione Russa di Mosca, Federazione Russa. Qualsiasi lodo arbitrale emesso dall'arbitro sarà definitivo e vincolante per le parti e qualsiasi giudizio su tale lodo può essere fatto valere in ogni foro competente. Nulla nel presente Paragrafo 10 può impedire a una delle Parti di ricercare e ottenere equo indennizzo presso un foro competente, sia prima, durante sia dopo il processo d'arbitrato.

11. Periodo di validità per la presentazione di azioni legali

A prescindere dalla forma, nessuna azione derivante dalle transazioni commerciali eseguite ai sensi del presente Contratto può essere presentata dalle due parti contrattuali a più di un (1) anno dal momento in cui è accaduto o si è scoperto che è accaduto l'evento su cui si basa l'azione, tranne in caso di azioni per violazione dei diritti di proprietà intellettuale, che possono essere presentate entro il periodo massimo applicabile secondo i termini di legge.

12. Totalità del Contratto; Clausola salvatoria; Assenza di deroga

Il presente Contratto costituisce l'intero contratto tra Lei e il Titolare e sostituisce ogni altro accordo, proposta, comunicato o comunicato commerciale precedente, sia verbale che scritto, relativo al Software o relativo al presente Contratto. Lei riconosce di aver letto il presente Contratto, lo comprende e accetta di essere vincolato ai suoi termini e condizioni. Se un foro competente giudica una qualsiasi disposizione del presente Contratto non valida, nulla o per qualsiasi motivo non applicabile, *in toto* o in parte, tale disposizione sarà riformulata più precisamente per renderla legittima e applicabile; ciò tuttavia non inficerà il Contratto e le rimanenti disposizioni del Contratto resteranno pienamente valide e in vigore nella massima misura consentita dalla legge diritto o dall'equity, conservando quanto più possibile il loro intento originale. Non varrà alcuna deroga a disposizioni o a condizioni del presente Contratto, a meno che la deroga non sia presentata per iscritto e firmata da Lei e da rappresentante autorizzato del Titolare, purché nessuna deroga a una violazione di una disposizione del presente Contratto valga come una deroga a qualsiasi violazione precedente, concorrente o successiva. La mancata insistenza da parte del Titolare nel richiedere la stretta applicazione di qualsiasi disposizione del presente Contratto o nel far valere un diritto non potrà essere interpretata quale deroga a tale disposizione o rinuncia a tale diritto.

13. Informazioni di contatto del Titolare

Per qualsiasi domanda relativa al presente Contratto, o se si desidera consultare per qualsiasi motivo il Titolare, si prega di contattare il nostro Servizio Clienti presso:

Kaspersky Lab ZAO, 10 edificio 1 1st Volokolamsky Proezd
Mosca, 123060
Federazione Russa
Tel: +7-495-797-8700
Fax: +7-495-645-7939
E-mail: info@kaspersky.com
Sito Web: www.kaspersky.com

© 2004-2011 Kaspersky Lab ZAO. Tutti i diritti riservati. Il Software e la documentazione d'accompagnamento sono soggetti a diritto d'autore e sono protetti dalle leggi sul copyright e dai trattati internazionali sul copyright nonché da altre leggi e trattati in materia di proprietà intellettuale.

SOMMARIO

INFORMAZIONI SULLA GUIDA	12
Contenuto del documento.....	12
Convenzioni utilizzate nella documentazione	15
ULTERIORI FONTI DI INFORMAZIONI.....	16
Fonti di informazione per ulteriori ricerche.....	16
Come contattare l'Ufficio Vendite	17
Forum Web di discussione sulle applicazioni Kaspersky Lab.....	17
Come contattare il team di sviluppo della documentazione	17
KASPERSKY MOBILE SECURITY 9.....	18
Novità di Kaspersky Mobile Security 9	19
Kit di distribuzione	19
Requisiti hardware e software	19
INSTALLAZIONE DI KASPERSKY MOBILE SECURITY 9.....	20
DISINSTALLAZIONE DELL'APPLICAZIONE.....	20
AGGIORNAMENTO DELL'APPLICAZIONE	22
OPERAZIONI PRELIMINARI	24
Attivazione dell'applicazione	24
Attivazione della versione commerciale	25
Attivazione dell'abbonamento per Kaspersky Mobile Security 9	26
Acquisto online di un codice di attivazione.....	27
Attivazione della versione trial.....	27
Impostazione della password segreta	28
Abilitazione dell'opzione per il ripristino della password segreta	28
Ripristino della password segreta.....	29
Avvio dell'applicazione	30
Aggiornamento dei database dell'applicazione.....	30
Scansione anti-virus del dispositivo.....	30
Visualizzazione di informazioni sull'applicazione.....	31
GESTIONE DELLA LICENZA	32
Informazioni sul Contratto di licenza.....	32
Informazioni sulle licenze di Kaspersky Mobile Security 9.....	32
Visualizzazione delle informazioni sulla licenza.....	33
Rinnovo della licenza.....	34
Rinnovo della licenza tramite il codice di attivazione	34
Rinnovo della licenza online.....	35
Rinnovo della licenza attraverso l'attivazione dell'abbonamento.....	36
Annullamento dell'abbonamento.....	37
Rinnovo dell'abbonamento.....	38
INTERFACCIA DELL'APPLICAZIONE.....	39
Finestra Stato della protezione	39
Menu dell'applicazione	41

PROTEZIONE DEL FILE SYSTEM.....	43
Informazioni sul componente Protezione.....	43
Abilitazione e disabilitazione del componente Protezione.....	43
Selezione dell'azione da eseguire sugli oggetti rilevati.....	45
SCANSIONE DEL DISPOSITIVO.....	47
Informazioni sulle scansioni manuali.....	47
Avvio di una scansione manuale.....	48
Avvio di una scansione pianificata.....	49
Selezione del tipo di oggetti da sottoporre a scansione.....	50
Configurazione della scansione degli archivi.....	51
Selezione dell'azione da eseguire sugli oggetti rilevati.....	52
QUARANTENA DEGLI OGGETTI MALWARE.....	54
Informazioni sulla Quarantena.....	54
Visualizzazione di oggetti in quarantena.....	54
Ripristino di oggetti dalla quarantena.....	55
Eliminazione di oggetti dalla quarantena.....	55
FILTRO DELLE CHIAMATE E DEGLI SMS IN ENTRATA.....	57
Informazioni su Filtro chiamate/SMS.....	57
Informazioni su Filtro chiamate/SMS.....	58
Modifica della modalità di Filtro chiamate/SMS.....	58
Creazione di una Lista bloccati.....	59
Aggiunta di voci alla Lista bloccati.....	59
Modifica di voci nella Lista bloccati.....	60
Eliminazione di voci dalla Lista bloccati.....	61
Creazione di una Lista consentiti.....	62
Aggiunta di voci alla Lista consentiti.....	62
Modifica di voci nella Lista consentiti.....	63
Eliminazione di voci dalla Lista consentiti.....	64
Risposta ai messaggi SMS e alle chiamate da contatti non in rubrica.....	65
Risposta ai messaggi SMS da mittenti non numerici.....	66
Selezione di una risposta alle chiamate in entrata.....	67
Selezione di una risposta alle chiamate in entrata.....	67
LIMITAZIONE DELLE CHIAMATE E DEI MESSAGGI SMS IN USCITA. PARENTAL CONTROL.....	68
Informazioni su Parental Control.....	69
Modalità del Parental Control.....	69
Abilitazione/disabilitazione del Parental Control.....	70
Creazione di una Lista bloccati.....	70
Aggiunta di voci alla Lista bloccati.....	71
Modifica di voci nella Lista bloccati.....	72
Eliminazione di voci dalla Lista bloccati.....	73
Creazione di una Lista consentiti.....	73
Aggiunta di voci alla Lista consentiti.....	74
Modifica di voci nella Lista consentiti.....	75
Eliminazione di voci dalla Lista consentiti.....	75
PROTEZIONE DEI DATI IN CASO DI SMARRIMENTO O FURTO DEL DISPOSITIVO.....	77
Informazioni su Antifurto.....	77
Blocco del dispositivo.....	78

Eliminazione dei dati personali	80
Creazione di un elenco di cartelle da eliminare	82
Monitoraggio della sostituzione di una scheda SIM sul dispositivo.....	83
Determinazione delle coordinate geografiche del dispositivo	84
Avvio remoto delle funzioni di Antifurto.....	87
PROTEZIONE PRIVACY	89
Protezione privacy	89
Modalità di Protezione privacy.....	89
Abilitazione/disabilitazione di Protezione privacy.....	90
Abilitazione automatica di Protezione privacy.....	91
Abilitazione remota di Protezione privacy	92
Creazione di un elenco di numeri privati.....	94
Aggiunta di un numero all'elenco dei numeri privati.....	95
Modifica di un numero nell'elenco dei numeri privati.....	95
Eliminazione di un numero dall'elenco dei numeri privati.....	96
Selezione dei dati da nascondere: Protezione privacy	97
FILTRO DELL'ATTIVITÀ DI RETE. FIREWALL.....	98
Informazioni sul Firewall	98
Abilitazione/disabilitazione del Firewall.....	99
Selezione del livello di sicurezza del Firewall	99
Notifiche di blocco	100
CRIPTAGGIO DEI DATI PERSONALI	102
Informazioni sul componente Criptaggio	102
Criptaggio dei dati.....	102
Decriptaggio dei dati.....	104
Blocco dell'accesso ai dati criptati	105
AGGIORNAMENTO DEI DATABASE DELL'APPLICAZIONE	107
Informazioni sull'aggiornamento dei database dell'applicazione	107
Visualizzazione delle informazioni sul database.....	108
Aggiornamento manuale.....	108
Aggiornamento pianificato	109
Aggiornamento in roaming.....	110
REPORT DELL'APPLICAZIONE	112
Informazioni sui report	112
Visualizzazione dei record del report.....	112
Eliminazione di record del report	113
CONFIGURAZIONE DI IMPOSTAZIONI AGGIUNTIVE.....	113
Modifica della password segreta	114
Visualizzazione dei suggerimenti.....	114
Configurazione delle notifiche acustiche	115
COME CONTATTARE IL SERVIZIO DI ASSISTENZA TECNICA	116
GLOSSARIO	117
KASPERSKY LAB.....	120
INFORMAZIONI SUL CODICE DI TERZE PARTI	121
Codice del programma distribuito	121

ADB	121
ADBWINAPI.DLL	121
ADBWINUSBAPI.DLL.....	121
Altre informazioni.....	123
INDICE.....	125

INFORMAZIONI SULLA GUIDA

Il presente documento fornisce informazioni sull'installazione, la configurazione e l'utilizzo di Kaspersky Mobile Security 9. Il documento è destinato agli utenti generici.

Obiettivi del documento:

- aiutare l'utente a impostare l'applicazione in un dispositivo mobile, attivarla e ottimizzarla per le proprie esigenze;
- consentire di trovare rapidamente informazioni sui problemi correlati all'applicazione;
- descrivere le fonti alternative di informazioni sull'applicazione e le opzioni per ottenere assistenza tecnica.

IN QUESTA SEZIONE

Contenuto del documento	12
Convenzioni utilizzate nella documentazione	15

CONTENUTO DEL DOCUMENTO

Il documento include le seguenti sezioni:

Ulteriori fonti di informazioni

In questa sezione sono descritte ulteriori fonti di informazioni sull'applicazione e risorse Internet che consentono agli utenti di discutere dell'applicazione, porre domande e ottenere risposte.

Kaspersky Mobile Security 9

In questa sezione sono descritte le funzionalità dell'applicazione e viene fornita una breve panoramica dei componenti e delle funzioni principali. Vengono inoltre fornite informazioni sulle finalità del kit di distribuzione. Vengono inoltre descritti i requisiti hardware software che un dispositivo mobile deve soddisfare per consentire l'installazione di Kaspersky Mobile Security 9.

Installazione di Kaspersky Mobile Security 9

In questa sezione vengono fornite istruzioni per l'installazione dell'applicazione in un dispositivo mobile.

Disinstallazione dell'applicazione

In questa sezione vengono fornite istruzioni per la disinstallazione dell'applicazione da un dispositivo mobile.

Aggiornamento dell'applicazione

In questa sezione vengono fornite istruzioni per l'aggiornamento di una versione precedente dell'applicazione.

Operazioni preliminari

In questa sezione vengono fornite informazioni su come iniziare a utilizzare Kaspersky Mobile Security 9: attivazione, impostazione di una password segreta per l'applicazione, abilitazione dell'opzione per il ripristino della password segreta, ripristino della password segreta, avvio dell'applicazione, aggiornamento dei database anti-virus e scansione dei dispositivi alla ricerca di virus.

Gestione della licenza

In questa sezione sono descritti i termini più comuni utilizzati relativamente alla gestione delle licenze dell'applicazione. La sezione spiega inoltre come reperire informazioni sulla licenza di Kaspersky Mobile Security 9 e su come estenderne il periodo di validità.

Interfaccia dell'applicazione

Questa sezione fornisce informazioni sui principali elementi dell'interfaccia di Kaspersky Mobile Security 9.

Protezione del file system

Questa sezione fornisce informazioni sul componente Protezione che consente di evitare le infezioni del file system del dispositivo. La sezione descrive inoltre come attivare o arrestare il componente Protezione e regolare le relative impostazioni.

Scansione del dispositivo

Questa sezione fornisce informazioni sulla scansione manuale del dispositivo allo scopo di rilevare e rimuovere eventuali minacce. Viene inoltre descritto come avviare una scansione del dispositivo, impostare una scansione pianificata del file system, selezionare i file per la scansione e impostare l'azione da eseguire quando viene rilevato un oggetto dannoso.

Quarantena degli oggetti malware

Questa sezione fornisce informazioni sulla *quarantena*, una cartella speciale in cui vengono collocati gli oggetti potenzialmente dannosi. Viene inoltre descritto come visualizzare, ripristinare o eliminare gli oggetti dannosi presenti nella cartella.

Filtro delle chiamate e degli SMS in entrata

Questa sezione fornisce informazioni su Filtro chiamate/SMS, che impedisce le chiamate e gli SMS indesiderati in base agli elenchi Lista bloccati e Lista consentiti creati dell'utente. Viene inoltre descritto come selezionare la modalità utilizzata da Filtro chiamate/SMS per esaminare le chiamate e gli SMS in entrata, come configurare ulteriori impostazioni di filtro per gli SMS e le chiamate in entrata e come creare gli elenchi Lista bloccati e Lista consentiti.

Limitazione delle chiamate e dei messaggi SMS in uscita. Parental Control

Questa sezione fornisce informazioni sul componente Parental Control, che consente di limitare le chiamate e i messaggi SMS in uscita verso numeri definiti. La sezione spiega inoltre come creare una lista di numeri consentiti e bloccati e come specificare le impostazioni di Parental Control.

Protezione dei dati in caso di smarrimento o furto del dispositivo

Questa sezione fornisce informazioni su Antifurto, che, in caso di furto o smarrimento del dispositivo, consente di bloccare l'accesso non autorizzato ai dati salvati nel dispositivo mobile e ne semplifica l'individuazione.

Viene inoltre descritto come abilitare o disabilitare la funzione Antifurto, impostarne i parametri di esecuzione e avviare Antifurto in remoto da un altro dispositivo mobile.

Protezione privacy

Questa sezione fornisce informazioni sul componente Protezione privacy, che consente di nascondere le informazioni riservate dell'utente.

Filtro dell'attività di rete. Firewall

Questa sezione fornisce informazioni sul componente Firewall, che consente di controllare le connessioni di rete nel dispositivo. Viene inoltre descritto come abilitare e disabilitare Firewall e selezionare la modalità desiderata.

Criptaggio dei dati personali

Questa sezione fornisce informazioni sul componente Criptaggio, che consente di criptare le cartelle nel dispositivo. Viene inoltre descritto come criptare e decriptare le cartelle selezionate.

Aggiornamento dei database dell'applicazione

Questa sezione fornisce informazioni sull'aggiornamento dei database dell'applicazione, che assicura la protezione aggiornata del dispositivo. Viene inoltre descritto come visualizzare informazioni sui database anti-virus installati, eseguire manualmente l'aggiornamento e configurare l'aggiornamento automatico dei database anti-virus.

Report dell'applicazione

Questa sezione fornisce informazioni sui report in cui viene registrato il funzionamento di ogni componente e l'esecuzione di ogni attività (ad esempio, gli aggiornamenti del database dell'applicazione e le scansioni anti-virus).

Configurazione di impostazioni aggiuntive

Questa sezione fornisce informazioni sulle opzioni aggiuntive di Kaspersky Mobile Security 9: come gestire le notifiche acustiche dell'applicazione e la retroilluminazione dello schermo, e come abilitare/disabilitare la visualizzazione dei suggerimenti, dell'icona Protezione e la finestra Stato di protezione.

Come contattare il Servizio di assistenza tecnica

Questa sezione contiene raccomandazioni per contattare Kaspersky Lab dall'area Assistenza personalizzata nel sito Web del servizio di Assistenza tecnica o telefonicamente.

Glossario

In questa sezione sono disponibili un elenco dei termini utilizzati nella documentazione e le relative definizioni.

Kaspersky Lab

In questa sezione vengono fornite informazioni su Kaspersky Lab ZAO.

Informazioni sul codice di terze parti

In questa sezione vengono fornite informazioni sul codice di terze parti utilizzato nell'applicazione.

Indice

Questa sezione consente di trovare rapidamente le informazioni desiderate all'interno della documentazione.

CONVENZIONI UTILIZZATE NELLA DOCUMENTAZIONE

Le convenzioni utilizzate nella documentazione sono riportate nella tabella seguente.

Table 1. Convenzioni utilizzate nella documentazione

TESTO DI ESEMPIO	DESCRIZIONE DELLA CONVENZIONE
Si noti che...	Il testo degli avvisi è in rosso e racchiuso da un riquadro. Gli avvisi contengono informazioni importanti, ad esempio sulle operazioni di importanza critica per la sicurezza.
È consigliabile utilizzare...	Le note sono racchiuse da un riquadro. Le note contengono informazioni aggiuntive e di riferimento.
Esempio: ...	Gli esempi sono riportati su sfondo giallo e sotto l'intestazione "Esempio".
Aggiornamento significa...	I nuovi termini sono in corsivo.
ALT+F4	I nomi dei tasti sono contrassegnati dalla formattazione in grassetto e in lettere maiuscole. I nomi dei tasti uniti da un segno più (+) indicano una combinazione di tasti.
Abilita	I nomi degli elementi di interfaccia come campi di immissione, comandi di menu e pulsanti sono in grassetto.
➡ Per configurare la pianificazione per un'attività:	Le frasi introduttive delle istruzioni sono in corsivo.
help	Il testo della riga di comando e dei messaggi visualizzati sullo schermo è contrassegnato da un tipo di carattere speciale.
<Indirizzo IP del computer>	Le variabili sono racchiuse tra parentesi angolari. Le variabili rappresentano i valori corrispondenti, senza le parentesi angolari.

ULTERIORI FONTI DI INFORMAZIONI

In caso di domande sull'installazione o sull'utilizzo di Kaspersky Mobile Security 9, è possibile trovare le risposte utilizzando numerose fonti di informazioni. È possibile scegliere quella più adatta in base all'importanza ed all'urgenza della domanda.

IN QUESTA SEZIONE

Fonti di informazione per ulteriori ricerche	16
Come contattare l'Ufficio Vendite	17
Forum Web di discussione sulle applicazioni Kaspersky Lab	17
Come contattare il team di sviluppo della documentazione.....	17

FONTI DI INFORMAZIONE PER ULTERIORI RICERCHE

Sono disponibili le seguenti fonti di informazione sull'applicazione:

- sito Web dedicato all'applicazione Kaspersky Lab;
- pagine della Knowledge Base dell'applicazione sul sito Web del Servizio di assistenza tecnica;
- guida in linea e suggerimenti installati;
- documentazione dell'applicazione installata.

Pagine dedicate all'applicazione sul sito Web di Kaspersky Lab

http://www.kasperskystore.it/cata_home.html

Questa pagina fornisce informazioni generali sulle funzionalità e le opzioni di Kaspersky Mobile Security 9. È inoltre possibile acquistare Kaspersky Mobile Security 9 dal negozio di Kaspersky Lab.

Pagine dedicate all'applicazione sul sito Web del Servizio di assistenza tecnica (Knowledge Base).

<http://www.kaspersky.com/it/service>

Queste pagine contengono articoli scritti dagli esperti del Servizio di assistenza tecnica.

Questi articoli contengono informazioni utili, consigli e risposte alle domande più frequenti relative all'acquisto, l'installazione e l'utilizzo di Kaspersky Mobile Security 9. Gli articoli sono organizzati per argomento, ad esempio "Aggiornamenti dei database" e "Risoluzione dei problemi". Questi articoli forniscono informazioni non solo su Kaspersky Mobile Security 9, ma anche su altri prodotti Kaspersky Lab. Essi possono contenere inoltre notizie dal Servizio di assistenza tecnica.

Guida in linea installata

In caso di domande su specifiche finestre o schede di Kaspersky Mobile Security 9, è possibile visualizzare la guida rapida.

Per visualizzare la guida rapida, aprire la schermata desiderata e selezionare **Guida**.

Documentazione installata

La Guida dell'Utente contiene informazioni dettagliate sulle funzioni dell'applicazione e sull'utilizzo di Kaspersky Mobile Security 9, insieme a suggerimenti e raccomandazioni sulla configurazione dell'applicazione.

I documenti sono inclusi in formato PDF nel pacchetto di distribuzione di Kaspersky Mobile Security 9.

È possibile anche scaricare questi documenti in formato elettronico dal sito Web di Kaspersky Lab.

COME CONTATTARE L'UFFICIO VENDITE

Per eventuali domande sulla selezione o sull'acquisto di Kaspersky Mobile Security o per estendere la licenza, è possibile contattare telefonicamente i nostri esperti dell'Ufficio Vendite presso la Sede Centrale di Mosca ai seguenti numeri telefonici:

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

Il servizio è offerto in inglese o russo.

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

FORUM WEB DI DISCUSSIONE SULLE APPLICAZIONI KASPERSKY LAB

Per domande di natura non urgente, è possibile rivolgersi agli esperti di Kaspersky Lab e mettersi in contatto con altri utenti delle applicazioni anti-virus Kaspersky Lab nel nostro forum all'indirizzo <http://forum.kaspersky.com>.

Nel forum è possibile visualizzare le discussioni in corso, lasciare i propri commenti, creare nuovi argomenti di discussione o utilizzare il motore di ricerca per domande specifiche.

COME CONTATTARE IL TEAM DI SVILUPPO DELLA DOCUMENTAZIONE

Per porre domande sulla documentazione, segnalare un errore o inviare un commento, è possibile contattare il team di sviluppo della documentazione. Per contattare il team di sviluppo della documentazione, è possibile inviare un e-mail all'indirizzo docfeedback@kaspersky.com. Nella riga dell'oggetto specificare: "Kaspersky Help Feedback: Kaspersky Mobile Security 9".

KASPERSKY MOBILE SECURITY 9

Kaspersky Mobile Security 9 assicura la protezione dei dispositivi mobili con sistema operativo Microsoft Windows Mobile. L'applicazione consente di proteggere le informazioni nel dispositivo dall'infezione da parte delle minacce note, impedire i messaggi SMS e le chiamate indesiderate, controllare le connessioni di rete del dispositivo, criptare le informazioni, nascondere i contatti riservati e proteggere le informazioni in caso di furto o smarrimento del dispositivo. Ogni tipo di minaccia viene elaborato da componenti distinti del programma. Questo consente di configurare in modo flessibile le impostazioni dell'applicazione.

Kaspersky Mobile Security 9 comprende i seguenti componenti di protezione:

- **Anti-Virus.** Protegge il file system del dispositivo mobile da virus e altre applicazioni dannose. Anti-Virus consente di rilevare e neutralizzare gli oggetti dannosi nel dispositivo e di aggiornare i database anti-virus dell'applicazione.
- **Filtro chiamate/SMS.** Scansiona tutti i messaggi SMS e le chiamate in entrata per rilevare se si tratta di spam. Questo componente consente di bloccare in modo flessibile gli SMS e le chiamate indesiderati.
- **Antifurto.** Protegge le informazioni nel dispositivo dagli accessi non autorizzati in caso di furto o smarrimento e ne semplifica l'individuazione. Antifurto consente di bloccare il dispositivo in remoto, eliminare le informazioni memorizzate nel dispositivo e identificare la posizione geografica del dispositivo (se questo include un ricevitore GPS) utilizzando comandi SMS inviati da un altro dispositivo. Antifurto consente inoltre di bloccare il dispositivo se la scheda SIM viene sostituita o se il dispositivo viene attivato senza una scheda SIM.
- **Parental Control.** Tutti i messaggi SMS e le chiamate in uscita vengono controllati. Il componente consente una configurazione flessibile del filtro degli SMS e delle chiamate in uscita.
- **Protezione privacy.** Nasconde le informazioni relative ai numeri riservati nell'elenco dei contatti. Per questi numeri Protezione privacy nasconde le voci nei contatti, i messaggi SMS o le voci nel registro delle chiamate, i nuovi messaggi SMS ricevuti e le chiamate in entrata.
- **Firewall.** Controlla le connessioni di rete sul dispositivo mobile. Firewall imposta le connessioni consentite o bloccate.
- **Criptaggio.** Protegge le informazioni in modalità criptata. Il componente consente di criptare qualsiasi numero di cartelle non di sistema presenti nella memoria del dispositivo o su una scheda di memoria. L'accesso alle cartelle criptate è possibile solo immettendo la password segreta dell'applicazione.

L'applicazione contiene inoltre una serie di funzioni di servizio che consentono di mantenere sempre aggiornata l'applicazione, ne aumentano le opzioni di utilizzo e supportano l'utente durante l'utilizzo dell'applicazione:

- **Stato di protezione.** Sullo schermo viene visualizzato lo stato dei componenti del programma. In base alle informazioni presentate, è possibile valutare lo stato di protezione corrente delle informazioni nel dispositivo.
- **Aggiornamento dei database anti-virus dell'applicazione.** Questa funzione mantiene aggiornati i database anti-virus di Kaspersky Mobile Security 9.
- **Report eventi.** Ognuno dei componenti dell'applicazione dispone di uno specifico report eventi che include informazioni sul funzionamento del componente (ad esempio, operazioni completate, dati sugli oggetti bloccati, report di scansione e aggiornamenti).
- **Licenza.** Quando si acquista Kaspersky Mobile Security 9, tra l'utente e Kaspersky Lab intercorre un contratto di licenza, in base al quale l'utente può utilizzare l'applicazione e accedere agli aggiornamenti dei database anti-virus e al servizio di Assistenza tecnica per un determinato periodo di tempo. Il periodo di validità della licenza e le altre informazioni necessarie per l'utilizzo di tutte le funzioni dell'applicazione sono indicati nella licenza.

Utilizzando l'opzione **Licenza**, è possibile ottenere un report dettagliato sulla licenza corrente nonché rinnovarla.

Kaspersky Mobile Security 9 non supporta le operazioni di backup e ripristino.

IN QUESTA SEZIONE

Novità di Kaspersky Mobile Security 9	19
Kit di distribuzione	19
Requisiti hardware e software	19

NOVITÀ DI KASPERSKY MOBILE SECURITY 9

Di seguito è riportata una descrizione dettagliata delle novità introdotte da Kaspersky Mobile Security 9.

Kaspersky Mobile Security 9 include le seguenti nuove opzioni:

- L'accesso all'applicazione è protetto da una password segreta.
- Il componente Protezione privacy consente di nascondere le seguenti informazioni per i contatti riservati nell'elenco dei contatti: voci nei contatti, messaggi SMS, report delle chiamate e nuovi messaggi SMS e chiamate in entrata. Le informazioni riservate sono accessibili per la visualizzazione se l'occultamento viene disabilitato.
- Il componente Criptaggio consente di criptare le cartelle salvate nella memoria del dispositivo o in una scheda di memoria. Il componente protegge i dati riservati in modalità criptata e consente di accedere alle informazioni criptate solo immettendo la password segreta dell'applicazione.
- È stata aggiunta una nuova funzione di servizio denominata Mostra suggerimenti: Kaspersky Mobile Security 9 visualizza una breve descrizione di ogni componente prima della relativa configurazione.
- È possibile acquistare un codice di attivazione o estendere il periodo di validità della licenza tramite l'opzione di abbonamento direttamente dal dispositivo mobile .

KIT DI DISTRIBUZIONE

È possibile acquistare Kaspersky Mobile Security 9 online. In questo caso, il kit di distribuzione dell'applicazione e la relativa documentazione vengono forniti in formato elettronico. Kaspersky Mobile Security 9 può essere acquistato anche presso tutti i migliori negozi di telefonia e apparecchi tecnologici. Per informazioni dettagliate sull'acquisto dell'applicazione e sulla ricezione del kit di distribuzione, contattare il nostro Ufficio Vendite all'indirizzo sales@kaspersky.com.

REQUISITI HARDWARE E SOFTWARE

Kaspersky Mobile Security 9 è stato sviluppato per essere installato su dispositivi mobili basati su uno dei seguenti sistemi operativi:

- Microsoft Windows Mobile 5.0;
- Microsoft Windows Mobile 6.0, 6.1, 6.5.

INSTALLAZIONE DI KASPERSKY MOBILE SECURITY 9

L'installazione dell'applicazione su un dispositivo mobile viene eseguita mediante alcuni passaggi.

Prima di avviare l'installazione, si consiglia di chiudere tutte le altre applicazioni in esecuzione.

➤ *Per installare Kaspersky Mobile Security 9:*

1. Collegare il dispositivo mobile al computer utilizzando l'applicazione Microsoft ActiveSync.
2. Eseguire una delle seguenti operazioni:
 - Se si è acquistato il programma su CD, eseguire l'installazione automatica di Kaspersky Mobile Security 9 dal CD acquistato.
 - Se si è acquistato il pacchetto di distribuzione su Internet, copiarlo sul dispositivo mobile utilizzando uno dei seguenti metodi:
 - dal sito Web di Kaspersky Lab;
 - utilizzando l'applicazione Microsoft ActiveSync;
 - utilizzando una scheda di memoria.

Eseguire l'installazione aprendo l'archivio cab contenente il pacchetto di distribuzione sul dispositivo mobile.
3. Leggere il testo del Contratto di licenza che intercorre tra l'utente e Kaspersky Lab. Per accettare tutti i termini del contratto, premere **OK**. Kaspersky Mobile Security 9 verrà installato sul dispositivo. Se non si accettano i termini del Contratto di licenza, premere **Annulla**.
4. Selezionare la lingua dell'interfaccia di Kaspersky Mobile Security 9 e premere **OK**.
5. Riavviare il dispositivo per completare l'installazione. premendo **Riavvia**.

L'applicazione viene installata con i parametri consigliati dagli esperti di Kaspersky Lab.

DISINSTALLAZIONE DELL'APPLICAZIONE

➤ *Per disinstallare Kaspersky Mobile Security 9:*

1. Decriptare i dati sul dispositivo se questi sono stati criptati con Kaspersky Mobile Security 9 (vedere la sezione "Decriptaggio dei dati" a pagina [104](#)).
2. Disabilitare Protezione privacy (vedere la sezione "Abilitazione/disabilitazione di Protezione privacy" a pagina [90](#)).
3. Chiudere Kaspersky Mobile Security 9. A tale scopo, premere **Menu** → **Esci**.
4. Disinstallare Kaspersky Mobile Security 9. eseguendo le seguenti operazioni:
 - a. Premere **Avvio** → **Impostazioni**.

- b. Selezionare **Rimuovi programmi** nella scheda **Sistema** (vedere la figura seguente).

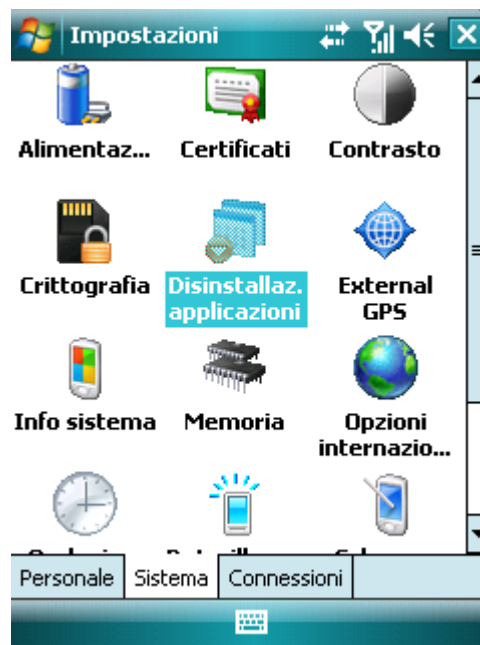


Figura 1: Scheda **Sistema**

- c. Selezionare **Kaspersky Mobile Security** dall'elenco dei programmi installati e premere il pulsante **Rimuovi** (vedere la figura seguente).



Figura 2: Selezione dell'applicazione da disinstallare

- d. Confermare l'eliminazione dell'applicazione facendo click su **Sì** nella finestra visualizzata.
- e. Immettere la password segreta e premere **OK**.
- f. Specificare se conservare o meno le impostazioni del programma e gli oggetti in quarantena (vedere la figura seguente):

- Per conservare le impostazioni dell'applicazione e gli oggetti in quarantena, premere **Conserva** (vedere la figura seguente).
- Per disinstallare completamente l'applicazione, premere **Elimina**.



Figura 3: Rimozione delle impostazioni dell'applicazione

5. Riavviare il dispositivo per completare la disinstallazione dell'applicazione.

AGGIORNAMENTO DELL'APPLICAZIONE

È possibile aggiornare Kaspersky Mobile Security 9 installando la versione più recente dell'applicazione (ad esempio, aggiornando la versione 9.0 alla versione 9.2).

Se si utilizza Kaspersky Mobile Security 8.0, è possibile passare a Kaspersky Mobile Security 9.0.

➔ *Per aggiornare la versione del programma:*

1. Disabilitare il criptaggio - decriptare tutti i dati (vedere la sezione "Decriptaggio dei dati" a pagina [104](#)).
2. Disabilitare il componente Protezione privacy (vedere la sezione "Abilitazione/disabilitazione del componente Protezione privacy" a pagina [90](#)).
3. Chiudere la versione corrente di Kaspersky Mobile Security A tale scopo, premere **Menu** → **Esci**.
4. Copiare il pacchetto di distribuzione dell'applicazione sul dispositivo utilizzando uno dei seguenti metodi:
 - dal sito Web di Kaspersky Lab;
 - utilizzando l'applicazione Microsoft ActiveSync;
 - utilizzando una scheda di espansione di memoria.
5. Avviare il pacchetto di distribuzione di Kaspersky Mobile Security 9 sul dispositivo.
6. Leggere attentamente il contratto di licenza. Per accettare i termini del contratto, premere **OK**. Verrà innanzitutto richiesto di disinstallare la versione precedente dell'applicazione.

7. Confermare la disinstallazione della versione precedente dell'applicazione premendo il pulsante **OK**.
8. Immettere la password segreta.
9. Specificare se conservare o meno le impostazioni dell'applicazione e gli oggetti in Quarantena:
 - Per conservare le impostazioni dell'applicazione e gli oggetti in quarantena, premere **Conserva** .
 - Per disinstallare completamente l'applicazione, premere **Disinstallare**.
10. Riavviare il dispositivo per completare il processo di rimozione premendo **Riavvia**.
11. Dopo aver riavviato il dispositivo, eseguire l'installazione di Kaspersky Mobile Security 9 (vedere la sezione "Installazione di Kaspersky Mobile Security 9" a pagina [20](#)).

Se la licenza corrente è ancora valida, l'applicazione verrà attivata automaticamente. Se la licenza è scaduta, eseguire l'attivazione dell'applicazione (vedere la sezione "Attivazione dell'applicazione" a pagina [24](#)).

➡ *Per passare da Kaspersky Mobile Security 8.0 alla versione 9:*

1. Decriptare tutti i dati criptati utilizzando Kaspersky Mobile Security 8.0.
2. Chiudere Kaspersky Mobile Security 9. A tale scopo, premere **Menu** → **Esci**.
3. Disinstallare Kaspersky Mobile Security 9, eseguendo le seguenti operazioni:
 - a. Premere **Avvio** → **Impostazioni**.
 - b. Selezionare **Rimuovi programmi** nella scheda **Sistema**
 - c. Selezionare **Kaspersky Mobile Security** dall'elenco dei programmi installati e premere il pulsante **Disinstalla**.
 - d. Confermare l'eliminazione dell'applicazione facendo click su **Sì** nella finestra visualizzata.
 - e. Immettere la password segreta impostata nella versione precedente dell'applicazione e premere **OK**.
 - f. Eliminare completamente le impostazioni di Kaspersky Mobile Security 8.0, poiché sono incompatibili con quelle della versione 9, premendo **Elimina**.
4. Riavviare il dispositivo per completare la disinstallazione di Kaspersky Mobile Security 8.0.
5. Avviare l'installazione di Kaspersky Mobile Security 9 (vedere la sezione "Installazione di Kaspersky Mobile Security 9" a pagina [20](#)).
6. Avviare l'attivazione dell'applicazione (vedere la sezione "Attivazione dell'applicazione" a pagina [24](#)).

Se il periodo di validità della licenza di Kaspersky Mobile Security 8.0 non è scaduto, attivare la versione 9 del programma utilizzando il codice di attivazione della versione 8.0.

OPERAZIONI PRELIMINARI

In questa sezione vengono fornite informazioni su come iniziare a utilizzare Kaspersky Mobile Security 9: attivazione, impostazione di una password segreta per l'applicazione, abilitazione dell'opzione per il ripristino della password segreta, ripristino della password segreta, avvio dell'applicazione, aggiornamento dei database anti-virus e scansione dei dispositivi alla ricerca di virus.

IN QUESTA SEZIONE

Attivazione dell'applicazione	24
Impostazione della password segreta	28
Abilitazione dell'opzione per il ripristino della password segreta	28
Ripristino della password segreta	29
Avvio dell'applicazione	30
Aggiornamento dei database dell'applicazione	30
Scansione anti-virus del dispositivo	30
Visualizzazione di informazioni sull'applicazione	31

ATTIVAZIONE DELL'APPLICAZIONE

Per poter utilizzare Kaspersky Mobile Security 9, è necessario prima attivarlo.

Per attivare Kaspersky Mobile Security 9 sul proprio dispositivo è necessario disporre di una connessione Internet configurata.

Prima di attivare l'applicazione, assicurarsi che le impostazioni della data o dell'ora di sistema del dispositivo siano corrette.

È possibile attivare l'applicazione nei seguenti modi:

- **Attivare la licenza trial.** Quando si attiva la versione trial, l'applicazione riceve una licenza trial gratuita. Il periodo di validità della licenza trial è visualizzato sullo schermo dopo il completamento dell'attivazione. Alla scadenza del periodo di validità della licenza trial, le funzioni dell'applicazione saranno limitate. Saranno disponibili solo le seguenti funzioni:
 - attivazione dell'applicazione;
 - gestione della licenza dell'applicazione;
 - guida in linea di Kaspersky Mobile Security 9;
 - disabilitazione del componente Criptaggio;
 - disabilitazione del componente Protezione privacy.

Non è possibile riattivare una licenza trial.

- **Attivare la licenza commerciale.** Per attivare la versione commerciale, è necessario utilizzare il codice di attivazione ricevuto al momento dell'acquisto dell'applicazione. Quando si attiva la versione commerciale, l'applicazione riceve una licenza commerciale, che consente di accedere a tutte le funzionalità dell'applicazione. Il periodo di validità della licenza è visualizzato sullo schermo del dispositivo. Al termine del periodo di validità della licenza commerciale, le funzionalità dell'applicazione verranno limitate e non sarà possibile eseguirne l'aggiornamento.

È possibile ottenere un codice di attivazione nei seguenti modi:

- online, visitando dall'applicazione Kaspersky Mobile Security 9 lo speciale sito Web di Kaspersky Lab per i dispositivi mobili;
- dal negozio online di Kaspersky Lab (<http://www.kaspersky.com/globalstore>);
- dai distributori Kaspersky Lab.
- **Attivare l'abbonamento.** Quando si attiva l'abbonamento, l'applicazione riceve una licenza commerciale con abbonamento. Il periodo di validità della licenza commerciale con abbonamento è limitato a 30 giorni. Quando viene attivato l'abbonamento, l'applicazione rinnova la licenza ogni 30 giorni. Al momento del rinnovo della licenza, sul conto personale dell'utente viene addebitato un importo fisso per l'utilizzo dell'applicazione, specificato al momento dell'attivazione dell'abbonamento. L'addebito viene effettuato tramite l'invio di un messaggio SMS a pagamento. Una volta effettuato l'addebito, l'applicazione riceve dal server di attivazione una nuova licenza con un abbonamento che consente di accedere a tutte le funzionalità dell'applicazione. È possibile annullare l'abbonamento per Kaspersky Mobile Security 9. In questo caso, alla scadenza della licenza corrente, le funzionalità dell'applicazione vengono limitate e i database non vengono più aggiornati.

IN QUESTA SEZIONE

Attivazione della versione commerciale	25
Attivazione dell'abbonamento per Kaspersky Mobile Security 9	26
Acquisto online di un codice di attivazione	27
Attivazione della versione trial	27

ATTIVAZIONE DELLA VERSIONE COMMERCIALE

◆ Per attivare la versione commerciale dell'applicazione con il codice di attivazione:

1. Selezionare **Start** → **Applicazioni**.
2. Selezionare **KMS 9** e avviare l'applicazione utilizzando la penna a stilo o il pulsante centrale di spostamento.

Verrà aperta la finestra **Attivazione**.

3. Selezionare **Immetti codice**.

Verrà aperta la finestra di attivazione di Kaspersky Mobile Security 9 (vedere la figura seguente).

4. Successivamente, immettere il codice di attivazione ricevuto nei quattro campi, quindi selezionare **Avanti**.

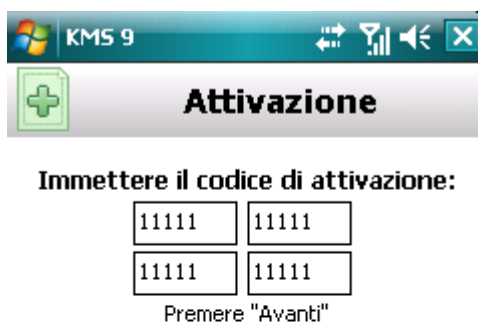


Figura 4: Attivazione della versione commerciale

5. Confermare la connessione a Internet premendo **Si**.

L'applicazione invierà una richiesta al server di attivazione di Kaspersky Lab e riceverà la licenza. Una volta ricevuta la licenza, le relative informazioni verranno visualizzate sullo schermo.

Se per qualche motivo il codice di attivazione immesso non risulta valido, sullo schermo verrà visualizzato un messaggio informativo. In questo caso, si consiglia di verificare che il codice di attivazione immesso sia corretto e di contattare il rivenditore del software presso cui è stato acquistato Kaspersky Mobile Security 9.

Se si verificano errori durante la connessione al server e non viene ricevuta la licenza, l'attivazione viene annullata. In questo caso, si consiglia di verificare i parametri di connessione a Internet. Se non è stato possibile correggere gli errori, contattare l'Assistenza tecnica.

6. Passare all'impostazione della password segreta dell'applicazione (vedere la sezione "Immissione della password segreta" a pagina [28](#)).

ATTIVAZIONE DELL'ABBONAMENTO PER KASPERSKY MOBILE SECURITY 9

Per attivare l'abbonamento, è necessario stabilire una connessione Internet sul dispositivo.

➔ Per attivare l'abbonamento per Kaspersky Mobile Security 9:

1. Selezionare **Start** → **Applicazioni**.
2. Selezionare **KMS 9** e avviare l'applicazione utilizzando la penna a stilo o il pulsante centrale di spostamento.

Verrà aperta la finestra **Attivazione**.

3. Selezionare **Acquista in 1 click**.
4. Confermare la connessione a Internet premendo **Si**.

L'applicazione verificherà se il servizio di abbonamento è supportato dall'operatore di telefonia mobile in uso. Se il servizio di abbonamento è supportato, verrà aperta la schermata **Attivazione**, in cui sono visualizzate le informazioni sulle condizioni dell'abbonamento.

Se non è possibile accedere al servizio di abbonamento, l'applicazione segnalerà il problema e verrà nuovamente visualizzata la schermata per la selezione di un altro metodo per l'attivazione dell'applicazione.

5. Leggere le condizioni dell'abbonamento e quindi confermare l'attivazione dell'abbonamento per Kaspersky Mobile Security 9 premendo **Avanti**.

L'applicazione invierà un SMS a pagamento e quindi riceverà una licenza dal server di attivazione di Kaspersky Lab. Quando l'abbonamento viene attivato, Kaspersky Mobile Security 9 segnala l'evento all'utente.

Se i fondi sul conto dell'utente sono insufficienti per l'invio di un messaggio SMS a pagamento, l'attivazione dell'abbonamento verrà annullata.

Se si verificano errori durante la connessione al server e non viene ricevuta la licenza, l'attivazione viene annullata. In questo caso, si consiglia di verificare i parametri di connessione a Internet. Se non è stato possibile correggere gli errori, contattare l'Assistenza tecnica.

Se non si accettano le condizioni dell'abbonamento, premere **Annulla**. In questo caso, l'attivazione dell'abbonamento verrà annullata e verrà nuovamente visualizzata la schermata in cui è possibile selezionare un altro metodo per l'attivazione dell'applicazione.

6. Passare all'immissione della password segreta (vedere la sezione "Immissione della password segreta" a pagina [28](#)).

ACQUISTO ONLINE DI UN CODICE DI ATTIVAZIONE

► Per acquistare online un codice di attivazione per l'applicazione, eseguire le seguenti operazioni:

1. Selezionare **Start** → **Applicazioni**.
2. Selezionare **KMS 9** e avviare l'applicazione utilizzando la penna a stilo o il pulsante centrale di spostamento.
Verrà aperta la finestra **Attivazione**.
3. Selezionare **Acquista online**.
Verrà aperta la finestra **Acquista online**.
4. Premere **Apri**.
Verrà aperto uno speciale sito Web di Kaspersky Lab per i dispositivi mobili, in cui è possibile acquistare la licenza.
5. Seguire le istruzioni dettagliate.
6. Al termine dell'acquisto di un codice di attivazione, procedere all'attivazione della versione commerciale dell'applicazione (vedere la sezione "Attivazione della versione commerciale" a pagina [25](#)).

ATTIVAZIONE DELLA VERSIONE TRIAL

► Per attivare la versione trial di Kaspersky Mobile Security 9:

1. Selezionare **Start** → **Applicazioni**.
2. Selezionare **KMS 9** e avviare l'applicazione utilizzando la penna a stilo o il pulsante centrale di spostamento.
Verrà aperta la finestra **Attivazione**.

3. Selezionare **Versione trial**.
4. Confermare la connessione a Internet premendo **Si**.

L'applicazione invierà una richiesta al server di attivazione di Kaspersky Lab e riceverà la licenza.

Se si verificano errori durante la connessione al server e non viene ricevuta la licenza, l'attivazione viene annullata. In questo caso, si consiglia di verificare i parametri di connessione a Internet. Se non è stato possibile correggere gli errori, contattare l'Assistenza tecnica.

5. Iniziare a immettere la password segreta dell'applicazione (vedere la sezione "Impostazione della password segreta" a pagina [28](#)).

IMPOSTAZIONE DELLA PASSWORD SEGRETA

Dopo l'avvio dell'applicazione, verrà richiesto di immettere la password segreta dell'applicazione. La *password segreta dell'applicazione* impedisce l'accesso non autorizzato alle impostazioni dell'applicazione.

È possibile cambiare in un secondo momento la password segreta installata.

Kaspersky Mobile Security 9 richiede la password segreta nelle seguenti circostanze:

- per l'accesso all'applicazione;
- per l'accesso alle cartelle crittate;
- durante l'invio di un comando SMS da un altro dispositivo mobile per attivare le seguenti funzioni in remoto: SMS-Block, SMS-Clean, SIM Watch, SMS-Find e Protezione privacy;
- in caso di disinstallazione dell'applicazione.

La password segreta è costituita da caratteri numerici, e deve contenere almeno quattro caratteri.

Se si dimentica la password segreta dell'applicazione, è possibile ripristinarla (vedere la sezione "Ripristino della password segreta" a pagina [29](#)). A tale scopo, è necessario abilitare in anticipo l'opzione per il ripristino della password segreta (vedere la sezione "Abilitazione dell'opzione per il ripristino della password segreta" a pagina [28](#)).

➡ *Per impostare la password segreta:*

1. Dopo l'attivazione dell'applicazione, immettere nel campo di immissione **Immettere la nuova password** le cifre della nuova password.
2. Immettere nuovamente la password nel campo **Conferma password**.

La password immessa viene verificata automaticamente.

3. Se la password viene considerata non valida in base ai risultati della verifica, verrà visualizzato un messaggio di avviso e l'applicazione richiederà una conferma. Per utilizzare la password, premere **OK**. Per creare una nuova password, premere **No**.
4. Premere **OK**.

ABILITAZIONE DELL'OPZIONE PER IL RIPRISTINO DELLA PASSWORD SEGRETA

Dopo l'attivazione iniziale dell'applicazione, è possibile abilitare l'opzione per il ripristino della password segreta. In questo modo, sarà possibile ripristinare la password segreta qualora venisse dimenticata.

Se è stata annullata l'abilitazione dell'opzione durante l'attivazione iniziale dell'applicazione, è possibile abilitarla dopo la reinstallazione di Kaspersky Mobile Security 9 nel dispositivo.

È possibile ripristinare la password segreta dell'applicazione (vedere la sezione "Ripristino della password segreta" a pagina 29) solo se l'opzione per il ripristino della password segreta è abilitata. Se si dimentica la password e l'opzione per il ripristino della password segreta è disabilitata, non sarà possibile gestire le funzioni di Kaspersky Mobile Security 9, accedere ai file criptati o disinstallare l'applicazione.

➔ Per abilitare l'opzione per il ripristino della password segreta:

1. Dopo avere impostato la password segreta per l'applicazione, confermare l'abilitazione dell'opzione per il ripristino della password segreta facendo click su **Si**.
2. Immettere il proprio indirizzo e-mail nel campo **Indirizzo e-mail** e premere **Avanti**.

L'indirizzo e-mail specificato verrà utilizzato durante il ripristino della password segreta.

L'applicazione stabilirà una connessione Internet al server per il ripristino della password segreta, invierà le informazioni immesse e abiliterà l'opzione per il ripristino della password segreta.

RIPRISTINO DELLA PASSWORD SEGRETA

È possibile ripristinare la password segreta solo abilitando l'opzione per il ripristino della password segreta in anticipo (vedere "Abilitazione dell'opzione per il ripristino della password segreta" a pagina 28).

➔ Per ripristinare la password segreta dell'applicazione:

1. Selezionare **Start** → **Applicazioni**.
2. Selezionare **KMS 9** e avviare l'applicazione utilizzando la penna a stilo o il pulsante centrale di spostamento.

Verrà visualizzata la schermata per l'immissione della password segreta.

3. Premere **Annulla**.
4. Passare al ripristino della password segreta premendo **Si**.

Nella schermata **Ripristino password segreta** verranno visualizzate le seguenti informazioni

- Sito Web di Kaspersky Lab per il ripristino della password segreta;
- codice di identificazione del dispositivo.

5. Visitare il sito Web <http://mobile.kaspersky.com/recover-code> per il ripristino della password segreta.
6. Specificare le seguenti informazioni nei campi appropriati:

- indirizzo e-mail specificato precedentemente per il ripristino della password segreta;
- codice di identificazione del dispositivo.

La password di ripristino verrà inviata all'indirizzo e-mail indicato.

7. Nella schermata **Ripristino password segreta** premere **Continua** e immettere la password di ripristino ricevuta.
8. Impostare una nuova password segreta dell'applicazione. A tale scopo, immettere la nuova password segreta dell'applicazione nei campi **Immettere la nuova password** e **Conferma password segreta**.

9. Premere **OK**.

AVVIO DELL'APPLICAZIONE

► Per avviare Kaspersky Mobile Security 9:

1. Selezionare **Start** → **Applicazioni**.
2. Selezionare **KMS 9** e avviare l'applicazione utilizzando la penna a stilo o il pulsante centrale di spostamento.
3. Immettere la password segreta dell'applicazione e premere **OK**.

L'applicazione visualizza una finestra che mostra lo stato corrente di Kaspersky Mobile Security 9 (vedere la sezione "Finestra Stato di protezione" a pagina [39](#)). Per passare alle funzioni dell'applicazione, premere **Menu**.

AGGIORNAMENTO DEI DATABASE DELL'APPLICAZIONE

Kaspersky Mobile Security 9 esegue la scansione delle minacce in base ai database dell'applicazione, che contengono le descrizioni di tutti i programmi dannosi noti attualmente e i metodi per neutralizzarli, nonché le descrizioni di altri oggetti indesiderati. Al momento dell'installazione, i database anti-virus inclusi nel pacchetto di installazione di Kaspersky Mobile Security 9 potrebbero risultare non aggiornati.

Si consiglia di aggiornare i database anti-virus dell'applicazione immediatamente dopo l'installazione dell'applicazione.

Per aggiornare i database anti-virus dell'applicazione è necessario disporre di una connessione Internet configurata sul proprio dispositivo mobile.

► Per avviare il processo di aggiornamento dei database anti-virus:

1. Selezionare **Menu** → **Anti-Virus**.
Verrà aperta la finestra **Anti-Virus**.
2. Selezionare l'opzione **Aggiornamento**.
Verrà aperta la finestra **Aggiornamento**.
3. Selezionare l'opzione **Aggiornamento**.

L'applicazione avvia il processo di aggiornamento dei database dal server Kaspersky Lab. Le informazioni sul processo di aggiornamento vengono visualizzate sullo schermo.

SCANSIONE ANTI-VIRUS DEL DISPOSITIVO

Al termine dell'installazione dell'applicazione, si consiglia di eseguire immediatamente una scansione del dispositivo mobile per individuare eventuali oggetti malware.

La prima scansione viene eseguita con le impostazioni predefinite dagli esperti Kaspersky Lab.

► Per eseguire una scansione completa del dispositivo:

1. Selezionare **Menu** → **Anti-Virus**.
Verrà aperta la finestra **Anti-Virus**.
2. Selezionare l'opzione **Scansione**.

Verrà aperta la finestra **Anti-Virus**.

3. Selezionare **Scansione completa**.

VISUALIZZAZIONE DI INFORMAZIONI SULL'APPLICAZIONE

È possibile visualizzare informazioni generali su Kaspersky Mobile Security 9 e la relativa versione.

➡ *Per visualizzare le informazioni sulla licenza:*

1. Selezionare **Menu** → **Avanzate**.

Verrà aperta la finestra **Avanzate**.

2. Selezionare la scheda **Info**.

GESTIONE DELLA LICENZA

Nell'ambito della gestione delle licenze delle applicazioni Kaspersky Lab, è importante conoscere i seguenti termini:

- Contratto di licenza;
- Licenza.

Tali termini sono inseparabilmente interconnessi e costituiscono un unico modello di gestione della licenza. La seguente sezione descrive con maggiore dettaglio ognuno di questi termini.

La sezione spiega inoltre come reperire informazioni sulla licenza di Kaspersky Mobile Security 9 e su come estenderne il periodo di validità.

IN QUESTA SEZIONE

Informazioni sul Contratto di licenza	32
Informazioni sulle licenze di Kaspersky Mobile Security 9	32
Visualizzazione delle informazioni sulla licenza	33
Rinnovo della licenza	34

INFORMAZIONI SUL CONTRATTO DI LICENZA

Il *Contratto di licenza* è un accordo che intercorre tra Kaspersky Lab e la persona fisica o il soggetto giuridico che detiene legalmente una copia di Kaspersky Mobile Security 9. Tale contratto è incluso in ogni applicazione Kaspersky Lab e contiene informazioni dettagliate sui diritti e sulle limitazioni di utilizzo di Kaspersky Mobile Security.

Secondo quanto previsto dal Contratto di licenza, al momento dell'acquisto e dell'installazione di un'applicazione Kaspersky Lab, si ottiene il diritto illimitato di possederne la copia.

Kaspersky Lab fornisce inoltre servizi aggiuntivi:

- assistenza tecnica;
- aggiornamento dei database anti-virus di Kaspersky Mobile Security 9;
- aggiornamento dei moduli di programma di Kaspersky Mobile Security 9.

Per poter usufruire di questi servizi, è necessario acquistare e attivare una licenza (vedere la sezione "Informazioni sulle licenze di Kaspersky Mobile Security" a pagina [32](#)).

INFORMAZIONI SULLE LICENZE DI KASPERSKY MOBILE SECURITY 9

Una *licenza* consiste nel diritto di utilizzo di Kaspersky Mobile Security e di usufruire dei servizi aggiuntivi (vedere la sezione "Informazioni sul Contratto di licenza" a pagina [32](#)) ad esso associati così come forniti da Kaspersky Lab o dai suoi partner.

Ogni licenza ha un periodo di validità distinto.

Il *periodo di validità della licenza* è un periodo durante il quale vengono forniti servizi aggiuntivi:

- assistenza tecnica;
- aggiornamento dei database anti-virus di Kaspersky Mobile Security 9;
- aggiornamento dei moduli di programma di Kaspersky Mobile Security 9.

L'ambito dei servizi forniti dipende dal tipo di licenza.

Sono disponibili i seguenti tipi di licenza:

- *Trial* – una licenza gratuita con un periodo di validità limitato, ad esempio 30 giorni, offerta per consentire di acquisire familiarità con Kaspersky Mobile Security 9.

È possibile utilizzare la licenza trial una sola volta.

Se si dispone di una licenza di prova, è possibile contattare il servizio di Assistenza tecnica solo per domande riguardanti l'attivazione del prodotto o l'acquisto di una licenza commerciale. Alla scadenza della licenza trial di Kaspersky Mobile Security 9, tutte le funzionalità vengono disabilitate. Per continuare a utilizzare l'applicazione, è necessario attivarla (vedere la sezione "Attivazione della versione commerciale" a pagina [25](#)).

- *Commerciale* – una licenza a pagamento con un periodo di validità limitato, ad esempio un anno, fornita al momento dell'acquisto di Kaspersky Internet Security 9.

Se viene attivata una licenza commerciale, sono disponibili tutte le funzionalità e i servizi aggiuntivi dell'applicazione.

Al termine del periodo di validità della licenza commerciale, alcune funzioni di Kaspersky Mobile Security 9 diventeranno inaccessibili e i database dell'applicazione non verranno più aggiornati. Una settimana prima della data di scadenza, viene visualizzato un avviso per consentire di rinnovare la licenza in anticipo.

- *Commerciale con abbonamento* – una licenza a pagamento con un'opzione di rinnovo in modalità automatica o manuale. Le licenze con abbonamento sono distribuite dai provider di servizi.

L'abbonamento è valido per un periodo limitato (30 giorni). Alla scadenza, l'abbonamento può essere rinnovato manualmente o in modo automatico. Il metodo per il rinnovo dell'abbonamento dipende dalla legislazione applicabile e dall'operatore di telefonia mobile. L'abbonamento viene rinnovato automaticamente, a condizione che venga effettuato il pagamento all'operatore di telefonia mobile.

In questo caso, l'importo specificato nelle condizioni dell'abbonamento viene addebitato sul conto dell'utente. L'importo viene addebitato sul conto dell'utente dopo l'invio di un messaggio SMS a pagamento al numero dell'operatore.

Se l'abbonamento non viene rinnovato, viene interrotto l'aggiornamento dei database di Kaspersky Mobile Security 9 e le funzionalità dell'applicazione diventano limitate.

Quando si utilizza l'abbonamento, è possibile attivare la licenza commerciale con un codice di attivazione. In questo caso, l'abbonamento verrà annullato automaticamente.

Quando si utilizza la licenza commerciale, è possibile attivare l'abbonamento. Se al momento dell'attivazione dell'abbonamento si dispone già di una licenza a durata limitata, questa viene sostituita dalla licenza con abbonamento.

VISUALIZZAZIONE DELLE INFORMAZIONI SULLA LICENZA

È possibile visualizzare le seguenti informazioni sulla licenza: numero di licenza, tipo, numero di giorni mancanti alla scadenza, data di attivazione e numero di serie del dispositivo.

➔ Per visualizzare le informazioni sulla licenza:

1. Selezionare **Menu** → **Avanzate**.
Verrà aperta la finestra **Avanzate**.
2. Selezionare l'opzione **Licenza**.
Verrà aperta la finestra **Licenza**.
3. Selezionare **Info licenza**.

RINNOVO DELLA LICENZA

Kaspersky Mobile Security 9 consente di rinnovare la licenza dell'applicazione.

La licenza può essere estesa in uno dei seguenti modi:

- Immettere un codice di attivazione - attivare l'applicazione con il codice di attivazione. È possibile acquistare il codice di attivazione su <http://www.kasperskystore.it/> oppure presso il proprio rivenditore Kaspersky Lab locale.
- Acquistare un codice di attivazione online – visitare il sito Web dal dispositivo mobile e acquistare un codice di attivazione online.
- Attivare l'abbonamento per Kaspersky Mobile Security 9 – attivare l'abbonamento in modo da rinnovare la licenza ogni 30 giorni.

Per attivare l'applicazione sul proprio dispositivo mobile è necessario disporre di una connessione Internet configurata.

IN QUESTA SEZIONE

Rinnovo della licenza tramite il codice di attivazione.....	34
Rinnovo della licenza online.....	35
Rinnovo della licenza attraverso l'attivazione dell'abbonamento.....	36
Annullamento dell'abbonamento.....	37
Rinnovo dell'abbonamento.....	38

RINNOVO DELLA LICENZA TRAMITE IL CODICE DI ATTIVAZIONE

➔ Per rinnovare la licenza tramite il codice di attivazione:

1. Selezionare **Menu** → **Avanzate**.
Verrà aperta la finestra **Avanzate**.
2. Selezionare l'opzione **Licenza**.
Verrà aperta la finestra **Licenza**.
3. Selezionare l'opzione **Rinnovo**.

Verrà aperta la finestra **Rinnovo**.

- Successivamente, immettere il codice di attivazione ricevuto nei quattro campi, quindi selezionare **Avanti** (vedere la figura seguente).

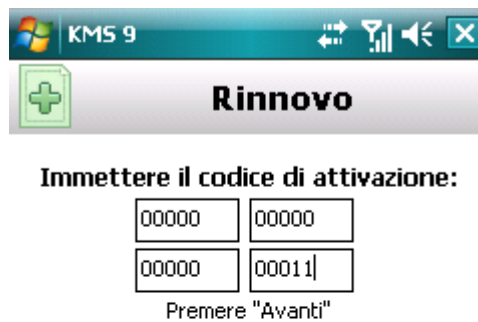


Figura 5: Rinnovo della licenza tramite il codice di attivazione

- Confermare la connessione a Internet premendo **Si**.

L'applicazione invierà una richiesta al server di attivazione di Kaspersky Lab e riceverà la licenza. Una volta ricevuta la licenza, le relative informazioni verranno visualizzate sullo schermo.

Se per qualche motivo il codice di attivazione immesso non risulta valido, sullo schermo verrà visualizzato un messaggio informativo. In questo caso, si consiglia di verificare che il codice di attivazione immesso sia corretto e di contattare il rivenditore del software presso cui è stato acquistato Kaspersky Mobile Security 9.

Se si verificano errori durante la connessione al server e non viene ricevuta la licenza, l'attivazione viene annullata. In questo caso, si consiglia di verificare i parametri di connessione a Internet. Se non è stato possibile correggere gli errori, contattare l'Assistenza tecnica.

- Al completamento dell'operazione, premere **OK**.

RINNOVO DELLA LICENZA ONLINE

➤ *Per rinnovare la licenza online:*

- Selezionare **Menu** → **Avanzate**.

Verrà aperta la finestra **Avanzate**.

- Selezionare l'opzione **Licenza**.

Verrà aperta la finestra **Licenza**.

- Selezionare l'opzione **Rinnova online**. Se il periodo di validità è scaduto, la voce del menu cambia in **Acquista online**.

Verrà aperta la finestra **Rinnova online**.

4. Premere **Apri** (vedere la figura seguente).

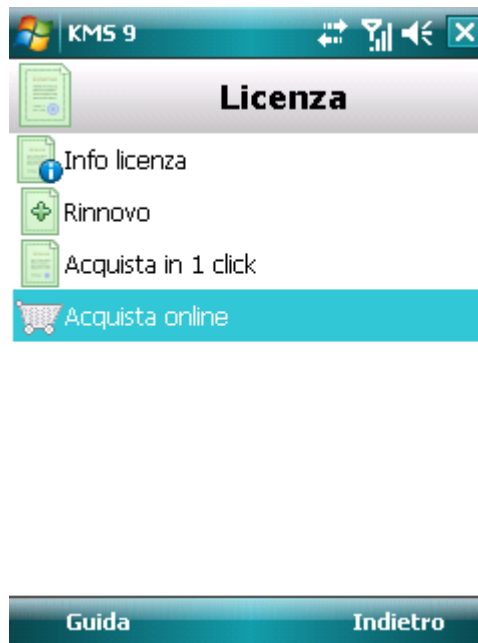


Figura 6: Rinnovo della licenza online

Verrà aperto un sito Web che consente di ordinare il rinnovo della licenza.

Se la licenza è scaduta, verrà aperto uno speciale sito Web di Kaspersky Lab per i dispositivi mobili, in cui è possibile acquistare un codice di attivazione online.

5. Seguire le istruzioni dettagliate.
6. Una volta elaborato l'ordine di rinnovo della licenza, immettere il codice di attivazione ricevuto (vedere la sezione "Rinnovo della licenza tramite il codice di attivazione" a pagina [34](#)).

RINNOVO DELLA LICENZA ATTRAVERSO L'ATTIVAZIONE DELL'ABBONAMENTO

Nel menu Avanzate è possibile estendere il periodo di validità della licenza attivando l'abbonamento (vedere la sezione "Informazioni sulle licenze di Kaspersky Mobile Security 9" a pagina [32](#)) per Kaspersky Mobile Security 9. Quando l'abbonamento è attivato, la licenza di Kaspersky Mobile Security 9 viene rinnovata ogni 30 giorni. Ogni volta che la licenza viene rinnovata, l'importo specificato nelle condizioni dell'abbonamento viene addebitato sul conto dell'utente.

Per attivare l'abbonamento per Kaspersky Mobile Security 9 sul proprio dispositivo, è necessario avere stabilito una connessione Internet.

➔ Per attivare l'abbonamento per Kaspersky Mobile Security 9:

1. Selezionare **Menu** → **Avanzate**.

Verrà aperta la finestra **Avanzate**.

2. Selezionare l'opzione **Licenza**.

Verrà aperta la finestra **Licenza**.

Selezionare la scheda **Acquista in 1 click** (vedere la figura seguente).

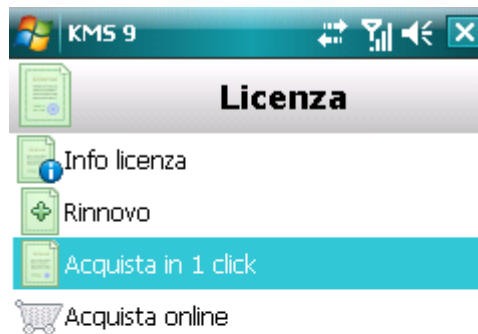


Figura 7: Attivazione dell'abbonamento

3. Confermare la connessione a Internet premendo **Si**.

L'applicazione verificherà se il servizio di abbonamento è supportato dall'operatore di telefonia mobile in uso.

Se il servizio di abbonamento è supportato, verrà aperta la schermata **Attivazione**, in cui sono visualizzate le informazioni sulle condizioni dell'abbonamento.

Se non è possibile accedere al servizio di abbonamento, l'applicazione segnalerà il problema e verrà nuovamente visualizzata la schermata per la selezione di un altro metodo per il rinnovo della licenza. L'attivazione dell'abbonamento verrà annullata.

4. Leggere le condizioni dell'abbonamento e quindi confermare l'attivazione dell'abbonamento per Kaspersky Mobile Security 9 premendo **Avanti**.

L'applicazione invierà un SMS a pagamento e quindi riceverà una licenza dal server di attivazione di Kaspersky Lab. Quando l'abbonamento viene attivato, Kaspersky Mobile Security 9 segnala l'evento all'utente.

Se i fondi sul conto dell'utente sono insufficienti per l'invio di un messaggio SMS a pagamento, l'attivazione dell'abbonamento verrà annullata.

Se si verificano errori durante la connessione al server e non viene ricevuta la licenza, l'attivazione viene annullata. In questo caso, si consiglia di verificare i parametri di connessione a Internet. Se non è stato possibile correggere gli errori, contattare l'Assistenza tecnica.

Se non si accettano le condizioni dell'abbonamento, premere **Annulla**. In questo caso, l'applicazione annullerà l'attivazione dell'abbonamento e verrà nuovamente visualizzata la schermata per la selezione di un altro metodo per il rinnovo della licenza.

5. Al completamento dell'operazione, premere **OK**.

ANNULLAMENTO DELL'ABBONAMENTO

È possibile annullare l'abbonamento per Kaspersky Mobile Security 9. In questo caso, la licenza di Kaspersky Mobile Security 9 non verrà rinnovata ogni 30 giorni. Alla scadenza della licenza corrente, le funzionalità dell'applicazione vengono limitate e i database non vengono più aggiornati.

Se è stato annullato l'abbonamento, è possibile riattivarlo (vedere la sezione "Rinnovo dell'abbonamento" a pagina [38](#)).

► Per annullare l'abbonamento per Kaspersky Mobile Security 9:

1. Selezionare **Menu** → **Avanzate**.

Verrà aperta la finestra **Avanzate**.

2. Selezionare l'opzione **Licenza**.

Verrà aperta la finestra **Licenza**.

3. Selezionare **Annulla abbonamento** (vedere la figura seguente).

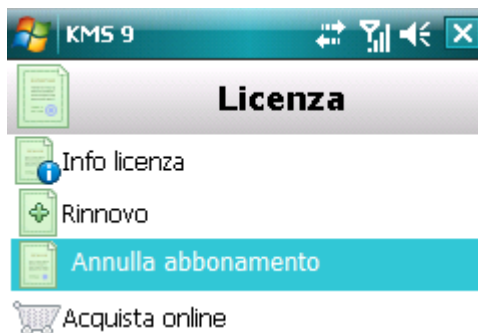


Figura 8: Annullamento dell'abbonamento

4. Confermare l'annullamento dell'abbonamento premendo **Si**.

Kaspersky Mobile Security 9 segnalerà l'annullamento dell'abbonamento.

RINNOVO DELL'ABBONAMENTO

Se è stato annullato l'abbonamento (vedere la sezione "Annullamento dell'abbonamento" a pagina [37](#)), è possibile riattivarlo. In questo caso, la licenza di Kaspersky Mobile Security 9 verrà rinnovata ogni 30 giorni.

Quando si riattiva l'abbonamento, l'importo viene addebitato sul conto dell'utente solo se la licenza corrente scade entro tre giorni.

► Per riattivare l'abbonamento:

1. Selezionare **Menu** → **Avanzate**.

Verrà aperta la finestra **Avanzate**.

2. Selezionare l'opzione **Licenza**.

Verrà aperta la finestra **Licenza**.

3. Selezionare la scheda **Acquista in 1 click**.

Se la licenza corrente è scaduta, Kaspersky Mobile Security 9 offrirà la possibilità di attivare l'abbonamento nuovamente (vedere la sezione "Rinnovo della licenza" a pagina [34](#)).

Se la licenza corrente non è ancora scaduta, l'abbonamento per Kaspersky Mobile Security 9 viene riattivato ed è rinnovato ogni 30 giorni dopo la scadenza della licenza corrente.

INTERFACCIA DELL'APPLICAZIONE

Questa sezione fornisce informazioni sui principali elementi dell'interfaccia di Kaspersky Mobile Security 9.

IN QUESTA SEZIONE

Finestra Stato della protezione.....	39
Menu dell'applicazione.....	41

FINESTRA STATO DELLA PROTEZIONE

Lo stato dei componenti principali dell'applicazione viene visualizzato nella finestra di stato corrente.

Per ciascun componente vi sono tre stati possibili, ognuno dei quali viene visualizzato con un colore specifico simile a quello dei semafori stradali. Il colore verde indica che la protezione del dispositivo è al livello necessario. I colori giallo e rosso indicano vari tipi di minacce. Le minacce non includono solo database anti-virus dell'applicazione non aggiornati ma anche, ad esempio, componenti di protezione disabilitati o impostazioni minime di esecuzione dell'applicazione.

La finestra di stato è accessibile immediatamente dopo aver avviato l'applicazione e contiene le seguenti informazioni:

- **Protezione** è lo stato della protezione in tempo reale (vedere la sezione "Protezione del file system" a pagina [43](#)).

L'icona di stato verde indica che la protezione è impostata al livello corretto e che i database anti-virus dell'applicazione sono aggiornati.

L'icona di colore giallo indica che i database non sono stati aggiornati da vari giorni.

L'icona di colore rosso indica problemi che possono causare perdita di informazioni o infezione del dispositivo. Ad esempio, la protezione è disattivata. I database dell'applicazione potrebbero non essere stati aggiornati per più di 15 giorni.

- **Firewall** è il livello di protezione del dispositivo da attività di rete indesiderate (vedere la sezione "Filtro dell'attività di rete. Firewall" a pagina [98](#)).

L'icona di stato verde indica che il componente è attivo. Il livello di protezione del Firewall è selezionato.

L'icona di colore rosso indica che l'attività di rete non è filtrata.

- **Antifurto** è lo stato di protezione dei dati in caso di smarrimento o furto del dispositivo (vedere la sezione "Protezione dei dati in caso di smarrimento o furto del dispositivo" a pagina [77](#)).

L'icona di stato verde indica che la funzione Antifurto è attiva; viene mostrata la lista delle funzioni attive del componente.

L'icona di colore rosso indica che tutte le funzioni di Antifurto sono disabilitate.

- **Protezione privacy** è lo stato di protezione dei dati riservati (vedere la sezione "Mascheramento dei dati personali" a pagina [89](#)).

L'icona di stato verde indica che il componente è attivo. I dati riservati sono nascosti.

L'icona di colore giallo avvisa il componente è disabilitato. I dati personali sono visualizzati e accessibili per la visualizzazione.

- **Licenza** è il periodo di validità della licenza (vedere la sezione "Gestione della licenza" a pagina [32](#)).

L'icona di stato verde indica che il periodo di validità della licenza scadrà tra più di 14 giorni.

L'icona di stato gialla indica che il periodo di validità della licenza scadrà tra meno di 14 giorni.

L'icona di colore rosso indica che la licenza è scaduta.



Figura 9: Finestra di stato del componente dell'applicazione

È possibile anche accedere alla finestra di stato selezionando **Menu** → **Stato di protezione**.

MENU DELL'APPLICAZIONE

I componenti dell'applicazione sono organizzati in gruppi logici e sono accessibili nel menu dell'applicazione. Ogni voce del menu consente di accedere ai parametri del componente selezionato e alla attività di protezione (vedere la figura seguente).



Figura 10: Menu dell'applicazione

Il menu di Kaspersky Mobile Security 9 contiene i seguenti elementi:

- **Anti-Virus:** protezione del file system da virus, scansione manuale e aggiornamento dei database anti-virus dell'applicazione.
- **Antifurto:** blocco del dispositivo e cancellazione dei dati in caso di smarrimento o furto.
- **Protezione privacy:** mascheramento dei dati riservati sul dispositivo.
- **Criptaggio:** protezione delle informazioni sul dispositivo tramite criptaggio.
- **Filtro chiamate/SMS:** filtro delle chiamate e degli SMS indesiderati.
- **Parental Control:** controllo delle chiamate e dei messaggi SMS in uscita.
- **Firewall:** protezione del dispositivo quando è connesso a una rete.
- **Avanzate:** impostazioni generali dell'applicazione, informazioni sull'applicazione, sui database in uso e sulla licenza.
- **Stato di protezione:** informazioni sullo stato della protezione del dispositivo.
- **Esci:** uscita dall'applicazione.

➡ *Per aprire il menu dell'applicazione:*

Selezionare **Menu**.

Per spostarsi tra le voci del menu dell'applicazione, utilizzare i pulsanti di spostamento o la penna stilo del dispositivo.

➤ *Per tornare all'applicazione:*

Selezionare **Menu** → **Stato di protezione**.

➤ *Per uscire dall'applicazione:*

Selezionare **Menu** → **Esci**.

PROTEZIONE DEL FILE SYSTEM

Questa sezione fornisce informazioni sul componente Protezione che consente di evitare le infezioni del file system del dispositivo. La sezione descrive inoltre come attivare o arrestare il componente Protezione e regolare le relative impostazioni.

IN QUESTA SEZIONE

Informazioni sul componente Protezione	43
Abilitazione e disabilitazione del componente Protezione	43
Selezione dell'azione da eseguire sugli oggetti rilevati	45

INFORMAZIONI SUL COMPONENTE PROTEZIONE

Il componente Protezione è avviato all'avvio del sistema operativo e viene eseguito costantemente nella memoria del dispositivo. Protezione esamina tutti file aperti, salvati o eseguiti. I file vengono sottoposti a scansione mediante il seguente algoritmo:

1. Protezione esamina tutti i file quando l'utente vi accede.
2. Il file viene sottoposto a scansione per verificare la presenza di eventuali oggetti dannosi. Gli oggetti dannosi vengono rilevati eseguendo un confronto con i database anti-virus dell'applicazione. I database anti-virus contengono descrizioni di tutti gli oggetti dannosi attualmente noti e i metodi per la loro neutralizzazione.
3. In base ai risultati dell'analisi, sono possibili i seguenti tipi di protezione:
 - Se all'interno del file è stato rilevato del codice dannoso, il componente Protezione blocca l'accesso al file ed esegue l'azione specificata nelle impostazioni.

Se nel file non viene rilevato alcun codice dannoso, il file verrà immediatamente ripristinato. Le informazioni sui risultati della scansione vengono salvate nel report dell'applicazione (vedere la sezione "Report dell'applicazione" a pagina [112](#)).

ABILITAZIONE E DISABILITAZIONE DEL COMPONENTE PROTEZIONE

Quando si attiva il componente Protezione, tutte le operazioni eseguite sul sistema sono costantemente sotto controllo.

Le risorse del dispositivo vengono utilizzate per assicurare la protezione da virus e altre minacce. Per ridurre il carico di lavoro sul dispositivo durante l'esecuzione di più attività, è possibile arrestare temporaneamente il componente Protezione.

Gli esperti di Kaspersky Lab consigliano di non disabilitare il componente Protezione, in quanto ciò può causare l'infezione del computer e perdita di dati.

La disabilitazione del componente Protezione non influisce sull'esecuzione delle attività di scansione virus e sull'aggiornamento dei database anti-virus dell'applicazione.

Lo stato corrente del componente Protezione è visualizzato nella finestra **Anti-Virus** accanto alla voce **Protezione**.

È possibile abilitare / disabilitare il componente Protezione nei seguenti modi:

- dal menu delle impostazioni del componente;
- dal menu **Anti-Virus**.

Per modificare i valori delle impostazioni, utilizzare i pulsanti di spostamento o la penna stilo del dispositivo.

► *Per abilitare il componente Protezione:*

1. Selezionare **Menu** → **Anti-Virus**.

Verrà aperta la finestra **Anti-Virus**.

2. Selezionare l'opzione **Protezione**.

Verrà aperta la finestra **Impostazioni**.

3. Selezionare la casella **Abilita protezione** (vedere la figura seguente).

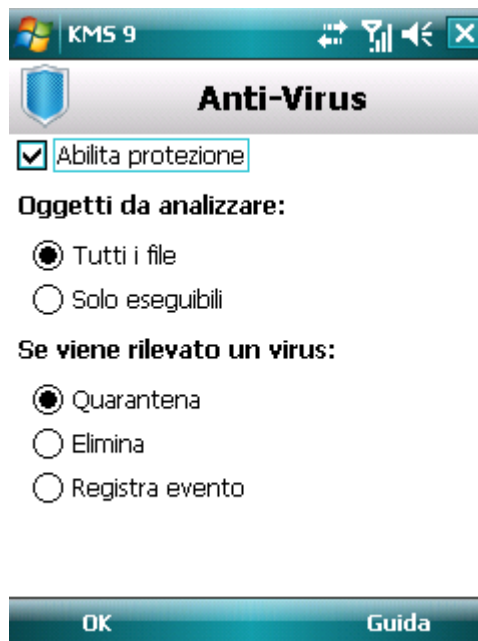


Figura 11: Abilitazione del componente Protezione

4. Premere **OK** per salvare le modifiche.

► *Per disabilitare il componente Protezione:*

1. Selezionare **Menu** → **Anti-Virus**.

Verrà aperta la finestra **Anti-Virus**.

2. Selezionare l'opzione **Protezione**.

Verrà aperta la finestra **Impostazioni**.

3. Deselezionare la casella **Abilita protezione**.

4. Premere **OK** per salvare le modifiche.

➤ *Per abilitare/disabilitare rapidamente il componente Protezione privacy;*

1. Selezionare **Menu** → Anti-Virus.
2. Verrà aperta la finestra **Anti-Virus**.
3. Premere il pulsante **Abilita / Disabilita**. Il nome del pulsante cambia in base allo stato corrente del componente Protezione.

SELEZIONE DELL'AZIONE DA ESEGUIRE SUGLI OGGETTI RILEVATI

Per impostazione predefinita, Kaspersky Mobile Security 9 sposta gli oggetti dannosi rilevati in quarantena. È possibile modificare l'azione eseguita da Kaspersky Mobile Security 9 quando rileva un oggetto dannoso.

Per modificare i valori delle impostazioni, utilizzare i pulsanti di spostamento o la penna stilo del dispositivo.

Per cambiare i valori delle impostazioni del componente Protezione, assicurarsi che sia attivo.

➤ *Per configurare la risposta dell'applicazione quando viene rilevato un oggetto malware:*

1. Selezionare **Menu** → **Anti-Virus**.
Verrà aperta la finestra **Anti-Virus**.
2. Selezionare l'opzione **Protezione**.
Verrà aperta la finestra **Impostazioni**.
3. Specificare l'azione che l'applicazione deve eseguire se viene rilevato un oggetto dannoso. Per eseguire questa operazione, selezionare un valore per l'impostazione **Se viene rilevato un virus** (vedere la figura seguente):
 - **Quarantena**: mette in quarantena gli oggetti malware.
 - **Elimina**: elimina gli oggetti malware senza avvisare l'utente.
 - **Registra evento**: non elabora gli oggetti malware ma registra le informazioni sul loro rilevamento nel report dell'applicazione; blocca l'oggetto quando ne viene tentato l'utilizzo (ad esempio, la copia o l'apertura).

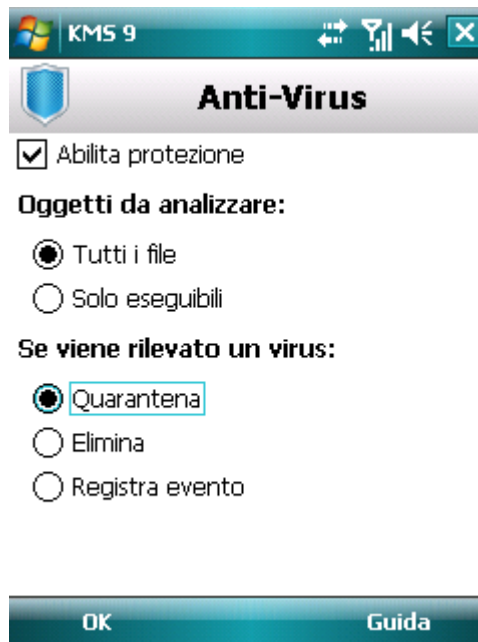


Figura 12: Selezione dell'azione da eseguire sugli oggetti dannosi

4. Premere **OK** per salvare le modifiche.

SCANSIONE DEL DISPOSITIVO

Questa sezione fornisce informazioni sulla scansione manuale del dispositivo allo scopo di rilevare e rimuovere le eventuali minacce nel dispositivo. Viene inoltre descritto come avviare una scansione del dispositivo, impostare una scansione pianificata del file system, selezionare i file per la scansione e impostare l'azione da eseguire quando viene rilevato un oggetto dannoso.

IN QUESTA SEZIONE

Informazioni sulle scansioni manuali	47
Avvio di una scansione manuale	48
Avvio di una scansione pianificata	49
Selezione del tipo di oggetti da sottoporre a scansione	50
Configurazione della scansione degli archivi.....	51
Selezione dell'azione da eseguire sugli oggetti rilevati	52

INFORMAZIONI SULLE SCANSIONI MANUALI

La scansione del dispositivo facilita il rilevamento e la neutralizzazione di eventuali oggetti dannosi. Kaspersky Mobile Security 9 consente di eseguire una scansione completa o parziale del dispositivo, ovvero solo la scansione del contenuto della memoria integrata del dispositivo o di una cartella specifica (incluse le cartelle presenti nella scheda di memoria).

La procedura di scansione del dispositivo è la seguente:

1. Kaspersky Mobile Security 9 esegue la scansione dei tipi di file selezionati (vedere la sezione "Selezione dei tipi di oggetti da sottoporre a scansione" a pagina [50](#)).
2. Ogni file viene sottoposto a scansione per verificare la presenza di eventuali oggetti dannosi (malware). Gli oggetti dannosi vengono rilevati eseguendo un confronto con i database anti-virus dell'applicazione. I database anti-virus contengono descrizioni di tutti gli oggetti dannosi attualmente noti e i metodi per la loro neutralizzazione.

Dopo l'analisi, Kaspersky Mobile Security 9 può eseguire le seguenti azioni correttive:

- Se all'interno del file è stato rilevato del codice dannoso, Kaspersky Mobile Security 9 blocca l'accesso al file ed esegue l'azione specificata nelle impostazioni (vedere la sezione "Selezione delle azioni da eseguire sugli oggetti" a pagina [52](#)).
- Se non viene rilevato alcun codice dannoso, il file diventa immediatamente accessibile per l'uso.

Un'attività di scansione può essere avviata manualmente o automaticamente in base a una pianificazione definita precedentemente (vedere la sezione "Avvio di una scansione pianificata" a pagina [49](#)).

Le informazioni sui risultati della scansione manuale vengono salvate nel report dell'applicazione (vedere la sezione "Report dell'applicazione" a pagina [112](#)).

AVVIO DI UNA SCANSIONE MANUALE

È possibile avviare una scansione manualmente in qualsiasi momento. Il momento migliore è tuttavia quando il processore del dispositivo non è occupato ad eseguire altre operazioni.

➔ Per avviare manualmente una scansione anti-virus:

1. Selezionare **Menu** → **Anti-Virus**.

Verrà aperta la finestra **Anti-Virus**.

2. Selezionare l'opzione **Scansione**.

Verrà aperta la finestra **Anti-Virus**.

3. Selezionare l'area di scansione del dispositivo (vedere la figura seguente):

- **Scansione completa:** esegue la scansione dell'intero file system del dispositivo. Per impostazione predefinita, vengono sottoposti a scansione i seguenti oggetti: memoria del dispositivo e scheda di memoria.
- **Scansione memoria:** esegue la scansione dei processi avviati nella memoria di sistema e dei file corrispondenti.
- **Scansione cartella:** esegue la scansione di un determinato oggetto nel file system del dispositivo o sulla scheda di memoria. Se si seleziona **Scansione cartella**, verrà aperta una finestra che visualizza il file system del dispositivo. Per spostarsi nel file system, utilizzare la penna a stilo o i pulsanti di spostamento. Per avviare la scansione della cartella, selezionare la cartella desiderata e selezionare **Scansione**.



Figura 13: Selezione dell'area di scansione

All'avvio della scansione, si aprirà la finestra del processo di scansione che visualizza lo stato della scansione, incluso il numero di oggetti sottoposti a scansione, il percorso dell'oggetto sottoposto a scansione e un indicatore che fornisce la percentuale di completamento della scansione.

Se Kaspersky Mobile Security 9 rileva un oggetto infetto, esegue un'azione in base ai parametri di scansione impostati (vedere la sezione "Selezione di un'azione da eseguire sugli oggetti" a pagina [52](#)).

Per impostazione predefinita, se Kaspersky Mobile Security 9 rileva una minaccia, la mette in quarantena.

Al termine della scansione, sullo schermo vengono visualizzate statistiche complessive con le seguenti informazioni:

- numero di oggetti sottoposti a scansione;
 - numero di virus rilevati, messi in quarantena o eliminati;
 - numero di oggetti ignorati (ad esempio, file bloccati dal sistema operativo o file non eseguibili, durante la scansione dei soli file di programma eseguibili);
 - tempo impiegato dalla scansione.
4. Al completamento dell'operazione, premere **OK**.

AVVIO DI UNA SCANSIONE PIANIFICATA

Kaspersky Mobile Security 9 consente di creare una pianificazione di ore in cui le scansioni verranno avviate automaticamente. Le scansioni vengono eseguite in background. Quando viene rilevato un oggetto infetto, su di esso verrà eseguita l'azione selezionata nelle impostazioni di scansione (vedere la sezione "Selezione di un'azione da eseguire sugli oggetti" a pagina [52](#)).

Per impostazione predefinita, le impostazioni pianificate sono disabilitate.

► *Per configurare una scansione pianificata:*

1. Selezionare **Menu** → **Anti-Virus**.

Verrà aperta la finestra **Anti-Virus**.

2. Selezionare l'opzione **Scansione**.

Verrà aperta la finestra **Anti-Virus**.

3. Selezionare l'opzione **Pianifica scansione**.

Verrà aperta la finestra **Pianifica**.

4. Selezionare la casella **Scansione pianificata** (vedere la figura seguente).

5. Selezionare uno dei valori per l'impostazione **Frequenza**:

- **Giornaliero**: esegue la scansione ogni giorno. Specificare l'**Ora** nel campo di immissione per impostare l'ora del giorno in cui verrà avviata la scansione.

- **Settimanale:** esegue la scansione una volta alla settimana. Specificare l'**Ora** e il **Giorno della settimana**.

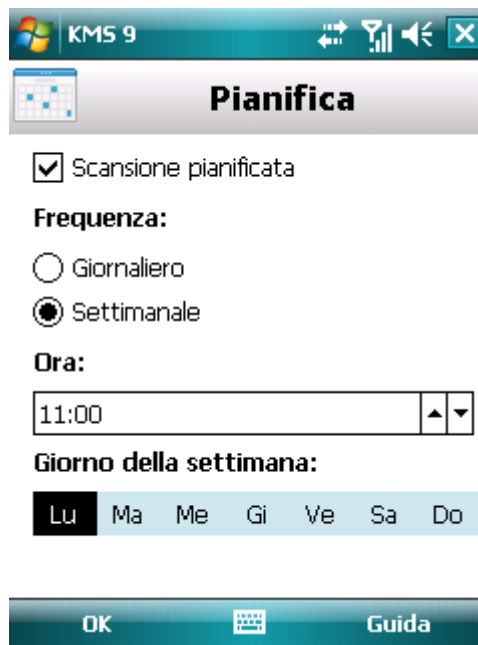


Figura 14: Configurazione di una scansione automatica pianificata

6. Premere **OK** per salvare le modifiche.

SELEZIONE DEL TIPO DI OGGETTI DA SOTTOPORRE A SCANSIONE

È possibile specificare il tipo di oggetti da sottoporre a scansione per rilevare codice dannoso.

Per modificare i valori delle impostazioni, utilizzare i pulsanti di spostamento o la penna stilo del dispositivo.

► Per selezionare gli oggetti da sottoporre a scansione:

1. Selezionare **Menu** → **Anti-Virus**.

Verrà aperta la finestra **Anti-Virus**.

2. Selezionare l'opzione **Scansione**.

Verrà aperta la finestra **Anti-Virus**.

3. Selezionare l'opzione **Oggetti e azioni**.

Verrà aperta la finestra **Oggetti e azioni**.

4. Selezionare gli oggetti da sottoporre a scansione nella sezione **Oggetti da analizzare** (vedere la figura seguente).

- **Tutti i file** - esegue la scansione di tutti i tipi di file.
- **Solo eseguibili** – esegue solo la scansione dei file di applicazione dei seguenti formati: EXE, DLL, MDL, APP, RDL, PRT, PXT, LDD, PDD, CLASS.

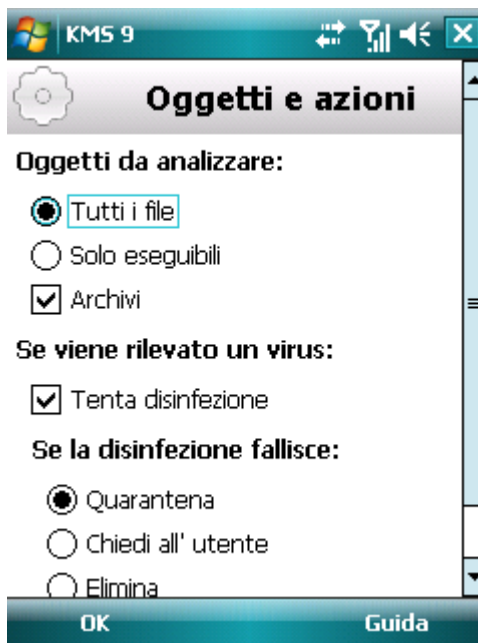


Figura 15: Selezione degli oggetti per la protezione

5. Premere **OK** per salvare le modifiche.

CONFIGURAZIONE DELLA SCANSIONE DEGLI ARCHIVI

I virus si nascondono spesso negli archivi. Il programma esamina i seguenti formati di archivi: ZIP, JAR, JAD e CAB. Gli archivi vengono decompressi durante la scansione e questo può ridurre significativamente la velocità della scansione manuale.

È possibile abilitare o disabilitare la scansione degli archivi alla ricerca di codice dannoso durante la scansione manuale.

Per modificare i valori delle impostazioni, utilizzare i pulsanti di spostamento o la penna stilo del dispositivo.

► *Per abilitare la scansione degli archivi:*

1. Selezionare **Menu** → **Anti-Virus**.
Verrà aperta la finestra **Anti-Virus**.
2. Selezionare l'opzione **Scansione**.
Verrà aperta la finestra **Anti-Virus**.
3. Selezionare l'opzione **Oggetti e azioni**.
Verrà aperta la finestra **Oggetti e azioni**.
4. Selezionare la casella **Archivi** nella sezione **Oggetti da analizzare**.
5. Premere **OK** per salvare le modifiche.

SELEZIONE DELL'AZIONE DA ESEGUIRE SUGLI OGGETTI RILEVATI

Per impostazione predefinita, Kaspersky Mobile Security 9 sposta gli oggetti infetti rilevati in quarantena. È possibile cambiare l'azione eseguita dall'applicazione quando rileva un oggetto dannoso.

Per modificare i valori delle impostazioni, utilizzare i pulsanti di spostamento o la penna stilo del dispositivo.

► *Per configurare la risposta dell'applicazione quando viene rilevato un oggetto malware:*

1. Selezionare **Menu** → **Anti-Virus**.

Verrà aperta la finestra **Anti-Virus**.

2. Selezionare l'opzione **Scansione**.

Verrà aperta la finestra **Anti-Virus**.

3. Selezionare l'opzione **Oggetti e azioni**.

Verrà aperta la finestra **Oggetti e azioni**.

4. Se si desidera che l'applicazione tenti di disinfettare gli oggetti infetti, selezionare la casella **Tenta disinfezione** accanto all'impostazione **Se viene rilevato un virus**.

5. Specificare l'azione da eseguire nei confronti di un oggetto dannoso rilevato. Per eseguire questa operazione, selezionare un valore per l'impostazione **Esegui azione**:

Se in precedenza è stata selezionata la casella **Tenta disinfezione**, il nome di questa impostazione cambia in **Se fallisce disinfezione**. Questa impostazione determina l'azione del programma, anche se la correzione dell'oggetto non va a buon fine.

- **Quarantena**: mette in quarantena gli oggetti.
- **Chiedi a utente**: richiede all'utente quale azione eseguire quando viene rilevato un oggetto dannoso.
- **Elimina**: elimina gli oggetti malware senza avvisare l'utente.

- **Registra evento:** non elabora gli oggetti malware ma registra le informazioni sul loro rilevamento nel report dell'applicazione; blocca l'oggetto quando ne viene tentato l'utilizzo (ad esempio, la copia o l'apertura).

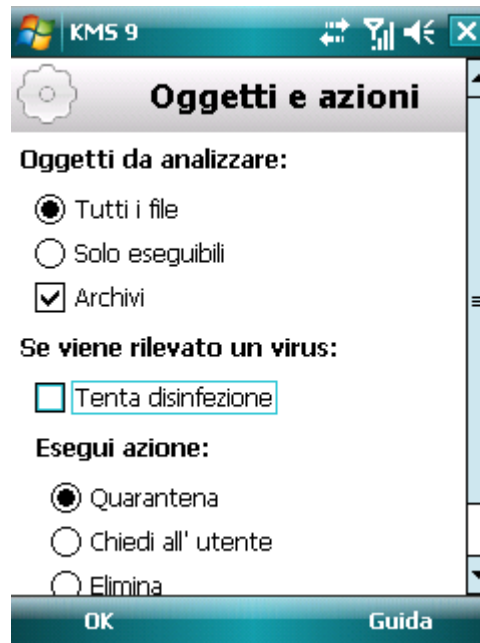


Figura 16: Selezione dell'azione da eseguire sugli oggetti dannosi

6. Premere **OK** per salvare le modifiche.

QUARANTENA DEGLI OGGETTI MALWARE

Questa sezione fornisce informazioni sulla *quarantena*, una cartella speciale in cui vengono collocati gli oggetti potenzialmente dannosi. Viene inoltre descritto come visualizzare, ripristinare o eliminare gli oggetti dannosi presenti nella cartella.

IN QUESTA SEZIONE

Informazioni sulla Quarantena	54
Visualizzazione di oggetti in quarantena	54
Ripristino di oggetti dalla quarantena	55
Eliminazione di oggetti dalla quarantena.....	55

INFORMAZIONI SULLA QUARANTENA

Durante la scansione del dispositivo o se è abilitata la protezione, qualsiasi oggetto dannoso rilevato viene spostato in una speciale cartella isolata, denominata *Quarantena*. Gli oggetti messi in quarantena vengono memorizzati in un formato compresso che ne impedisce l'attivazione e neutralizza la potenziale minaccia al dispositivo.

È possibile visualizzare, eliminare e ripristinare i file messi in quarantena.

VISUALIZZAZIONE DI OGGETTI IN QUARANTENA

È possibile visualizzare l'elenco degli oggetti messi in quarantena dall'applicazione. Per ogni oggetto vengono specificati nell'elenco il nome completo e la data di rilevamento.

È inoltre possibile visualizzare ulteriori informazioni sull'oggetto infetto selezionato: il percorso dell'oggetto nel dispositivo prima dello spostamento in Quarantena da parte dell'applicazione e il nome della minaccia.

► *Per visualizzare l'elenco degli oggetti in quarantena:*

1. Selezionare **Menu** → **Anti-Virus**.

Verrà aperta la finestra **Anti-Virus**.

2. Selezionare l'opzione **Quarantena**.

Verrà aperta la schermata **Quarantena**, in cui è visualizzato l'elenco degli oggetti messi in quarantena (vedere la figura seguente).

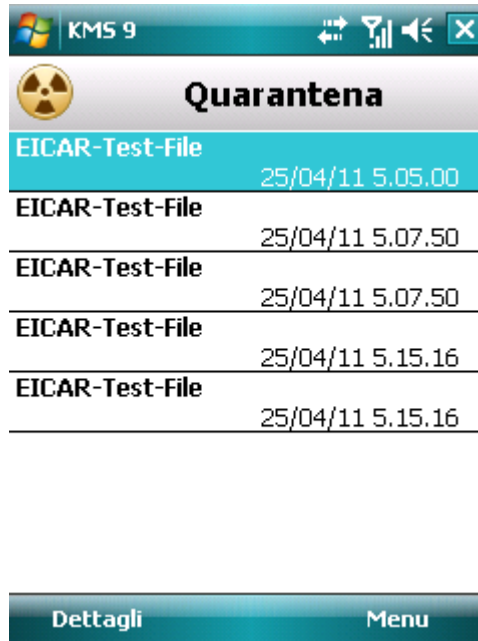


Figura 17: Elenco di oggetti in Quarantena

➔ Per visualizzare le informazioni su un oggetto infetto:

Premere **Dettagli**.

Nella schermata **Dettagli** verranno visualizzate le seguenti informazioni sull'oggetto: percorso del file nel dispositivo prima del rilevamento da parte dell'applicazione e nome del virus.

Verrà aperta la schermata **Info oggetto**.

RIPRISTINO DI OGGETTI DALLA QUARANTENA

Se si è sicuri che l'oggetto rilevato non rappresenta una minaccia per il dispositivo, è possibile ripristinarlo dalla quarantena. L'oggetto ripristinato viene rimesso nella cartella originale.

➔ Per ripristinare un oggetto dalla quarantena:

1. Selezionare **Menu** → **Anti-Virus**.

Verrà aperta la finestra **Anti-Virus**.

2. Selezionare l'opzione **Quarantena**.

Verrà aperta la finestra **Quarantena**.

3. Selezionare l'oggetto che si desidera ripristinare e premere **Menu** → **Ripristina**.

L'oggetto selezionato verrà ripristinato dalla quarantena nella cartella originale.

ELIMINAZIONE DI OGGETTI DALLA QUARANTENA

È possibile eliminare un singolo oggetto o tutti gli oggetti in quarantena.

➤ *Per eliminare un oggetto dalla quarantena:*

1. Selezionare **Menu** → **Anti-Virus**.

Verrà aperta la finestra **Anti-Virus**.

2. Selezionare l'opzione **Quarantena**.

Verrà aperta la finestra **Quarantena**.

3. Selezionare l'oggetto che si desidera eliminare e premere **Menu** → **Elimina**.

L'oggetto selezionato verrà eliminato dalla quarantena.

➤ *Per eliminare tutti gli oggetti in quarantena:*

1. Selezionare **Menu** → **Anti-Virus**.

Verrà aperta la finestra **Anti-Virus**.

2. Selezionare l'opzione **Quarantena**.

Verrà aperta la finestra **Quarantena**.

3. Selezionare **Menu** → **Elimina tutto**.

Tutti gli oggetti in quarantena verranno eliminati.

FILTRO DELLE CHIAMATE E DEGLI SMS IN ENTRATA

Questa sezione fornisce informazioni su Filtro chiamate/SMS, che impedisce le chiamate e gli SMS indesiderati in base agli elenchi Lista bloccati e Lista consentiti creati dell'utente. Viene inoltre descritto come selezionare la modalità utilizzata da Filtro chiamate/SMS per esaminare le chiamate e gli SMS in entrata, come configurare ulteriori impostazioni di filtro per gli SMS e le chiamate in entrata e come creare gli elenchi Lista bloccati e Lista consentiti.

IN QUESTA SEZIONE

Informazioni su Filtro chiamate/SMS.....	57
Informazioni sulle modalità di Filtro chiamate/SMS.....	58
Modifica della modalità di Filtro chiamate/SMS.....	58
Creazione di una Lista bloccati	59
Creazione di una Lista consentiti	62
Risposta ai messaggi SMS e alle chiamate da contatti non in rubrica	65
Risposta ai messaggi SMS da mittenti non numerici	66
Selezione di una risposta agli SMS in entrata.....	67
Selezione di una risposta alle chiamate in entrata	67

INFORMAZIONI SU FILTRO CHIAMATE/SMS

Filtro chiamate/SMS impedisce la ricezione delle chiamate e degli SMS indesiderati in base agli elenchi Lista bloccati e Lista consentiti compilati dall'utente.

Le liste sono composte da voci. Le voci negli elenchi contengono le seguenti informazioni:

- Numero di telefono da cui Filtro chiamate/SMS blocca le comunicazioni se il numero è incluso nella Lista bloccati o consente le comunicazioni se il numero è incluso nella Lista consentiti.
- Tipo di eventi bloccati o consentiti da Filtro chiamate/SMS se il numero è incluso nella Lista bloccati o nella Lista consentiti. Sono disponibili i seguenti tipi di comunicazioni: Chiamate e SMS, Solo chiamate e Solo SMS.
- Frase chiave utilizzata da Filtro chiamate/SMS per identificare gli SMS desiderati e indesiderati. Per la Lista bloccati, Filtro chiamate/SMS blocca gli SMS che contengono questa frase, mentre consente quelli che non la contengono. Per la Lista consentiti, Filtro chiamate/SMS consente gli SMS che contengono questa frase, mentre blocca quelli che non la contengono.

Filtro chiamate/SMS filtra le chiamate e gli SMS in entrata in base alla modalità selezionata (vedere la sezione "Informazioni sulle modalità di Filtro chiamate/SMS" a pagina [58](#)). A seconda della modalità, Filtro chiamate/SMS esegue la scansione di ogni SMS o chiamata in entrata e determina se l'SMS o la chiamata è desiderata o indesiderata (spam). Non appena Filtro chiamate/SMS assegna lo stato di desiderato o indesiderato a un SMS o a una chiamata, la scansione termina.

Le informazioni sulle chiamate e sugli SMS bloccati vengono registrate nel report dell'applicazione (vedere la sezione "Report dell'applicazione" a pagina [112](#)).

INFORMAZIONI SU FILTRO CHIAMATE/SMS

La modalità definisce le regole in base alle quali Filtro chiamate/SMS filtra le chiamate e gli SMS in entrata.

Sono disponibili le seguenti modalità di Filtro chiamate/SMS:

- **Disabilitato** - sono consentiti tutte le chiamate e gli SMS in entrata.
- **Consenti Lista consentiti** - sono consentiti solo le chiamate e gli SMS dai numeri nella Lista consentiti.
- **Blocca Lista bloccati** - sono consentiti tutte le chiamate e gli SMS, tranne quelli dai numeri nella Lista bloccati.
- **Entrambe le liste** - le chiamate e gli SMS in entrata dai numeri nella Lista consentiti sono consentiti, mentre quelli dai numeri nella Lista bloccati sono bloccati. Dopo una conversazione o la lettura di un SMS ricevuto da un numero che non è presente in alcuno dei due elenchi, Filtro chiamate/SMS richiederà di immettere il numero in uno degli elenchi.

È possibile modificare la modalità di Filtro chiamate/SMS (vedere la sezione "Modifica della modalità di Filtro chiamate/SMS" a pagina [58](#)). La modalità corrente di Filtro chiamate/SMS è visualizzata nella schermata **Filtro chiamate/SMS**, accanto all'opzione **Modalità**.

MODIFICA DELLA MODALITÀ DI FILTRO CHIAMATE/SMS

➔ Per modificare la modalità di Filtro chiamate/SMS:

1. Selezionare **Menu** → **Filtro chiamate/SMS**.

Verrà aperto **Filtro chiamate/SMS**.

2. Selezionare l'opzione **Modalità**.

Verrà aperta la finestra **Modalità**.

3. Selezionare un valore per l'impostazione **Modalità Filtro chiamate/SMS** (vedere la figura precedente).



Figura 18: Modifica della modalità di Filtro chiamate/SMS

4. Premere **OK** per salvare le modifiche.

CREAZIONE DI UNA LISTA BLOCCATI

La Lista bloccati contiene le voci relative ai numeri per i quali Filtro chiamate/SMS blocca le chiamate e gli SMS. Ogni voce contiene le seguenti informazioni:

- Numero di telefono da cui Filtro chiamate/SMS blocca le chiamate e/o gli SMS.
- Tipi di eventi bloccati da Filtro chiamate/SMS per il numero. Sono disponibili i seguenti tipi di eventi: Chiamate e SMS, Solo chiamate e Solo SMS.
- Frase chiave utilizzata da Filtro chiamate/SMS per classificare un SMS come indesiderato (spam). Filtro chiamate/SMS blocca solo gli SMS che contengono la frase chiave, mentre consente tutti gli altri SMS.

Filtro chiamate/SMS blocca le chiamate e gli SMS che soddisfano tutti i criteri di una voce nella Lista bloccati. Le chiamate e gli SMS che non soddisfano anche solo uno dei criteri di una voce nella Lista bloccati vengono consentiti.

Non è possibile aggiungere un numero di telefono con criteri di filtro identici sia alla Lista bloccati che alla Lista consentiti.

Le informazioni sulle chiamate e sugli SMS bloccati vengono registrate nel report dell'applicazione (vedere la sezione "Report dell'applicazione" a pagina [112](#)).

IN QUESTA SEZIONE

Aggiunta di voci alla Lista bloccati.....	59
Modifica di voci nella Lista bloccati	60
Eliminazione di voci dalla Lista bloccati.....	61

AGGIUNTA DI VOCI ALLA LISTA BLOCCATI

Non è possibile aggiungere contemporaneamente lo stesso numero con criteri di filtro identici nella Lista bloccati e nella Lista consentiti di Filtro chiamate/SMS. Se un numero con i criteri di filtro specificati è già stato salvato in uno dei due elenchi, Kaspersky Mobile Security 9 segnalerà l'evento e verrà visualizzato un messaggio sullo schermo.

➔ Per aggiungere una voce alla Lista bloccati di Filtro chiamate/SMS:

1. Selezionare **Menu** → **Filtro chiamate/SMS**.

Verrà aperto **Filtro chiamate/SMS**.

2. Selezionare l'opzione **Lista bloccati**.

Verrà aperta la finestra **Lista bloccati**.

3. Selezionare **Menu** → **Aggiungi**.

Verrà aperta la finestra **Nuova voce**.

4. Selezionare i valori per le seguenti impostazioni (vedere la figura seguente).

- **Blocca in entrata** - tipo di evento bloccato da Filtro chiamate/SMS per i numeri nella Lista bloccati:

- **Chiamate e SMS:** blocca le chiamate e gli SMS in entrata.
- **Solo chiamate:** blocca solo le chiamate in entrata.
- **Solo SMS:** blocca solo i messaggi SMS in entrata.
- **Numero di telefono** - numero di telefono per cui Filtro chiamate/SMS blocca le informazioni in arrivo. Il numero di telefono deve comprendere solo caratteri alfanumerici; può iniziare con una cifra, una lettera o essere preceduto dal simbolo "+". Per i numeri è inoltre possibile utilizzare i caratteri jolly "*" o "?" (dove "*" rappresenta un numero qualsiasi di simboli e "?" qualsiasi singolo simbolo). Ad esempio, *1234? nella Lista bloccati. Filtro chiamate/SMS blocca le chiamate o gli SMS da un numero che contiene qualsiasi carattere dopo 1234.
- **Contenente il testo** - frase chiave che indica che il messaggio SMS ricevuto è indesiderato (spam). Filtro chiamate/SMS blocca solo gli SMS che contengono la frase chiave, mentre consente tutti gli altri SMS.

Se si desidera bloccare tutti gli SMS in entrata da uno specifico numero nella Lista bloccati, lasciare vuoto il campo **Contenente il testo** per questa voce.

Nuova voce

Blocca in entrata:

Chiamate e SMS

Solo chiamate

Solo SMS

Numero di telefono:

1234567

Contenente il testo:

pubblicità

OK Menu

Figura 19: Impostazioni della voce

Premere **OK** per salvare le modifiche.

MODIFICA DI VOCI NELLA LISTA BLOCCATI

È possibile cambiare il valore di tutte le impostazioni relative ai numeri presenti nella Lista bloccati.

◆ Per modificare una voce nella Lista bloccati di Filtro chiamate/SMS:

1. Selezionare **Menu** → **Filtro chiamate/SMS**.

Verrà aperto **Filtro chiamate/SMS**.

2. Selezionare l'opzione **Lista bloccati**.

Verrà aperta la finestra **Lista bloccati**.

3. Selezionare dall'elenco la voce che si desidera modificare, quindi selezionare **Menu** → **Modifica**.

Verrà aperta la finestra **Modifica voce**.

4. Modificare le impostazioni necessarie:

- **Blocca in entrata** - tipo di evento bloccato da Filtro chiamate/SMS per i numeri nella Lista bloccati:
 - **Chiamate e SMS**: blocca le chiamate e gli SMS in entrata.
 - **Solo chiamate**: blocca solo le chiamate in entrata.
 - **Solo SMS**: blocca solo i messaggi SMS in entrata.
- **Numero di telefono** - numero di telefono per cui Filtro chiamate/SMS blocca le informazioni in arrivo. Il numero di telefono deve comprendere solo caratteri alfanumerici; può iniziare con una cifra, una lettera o essere preceduto dal simbolo "+". Per i numeri è inoltre possibile utilizzare i caratteri jolly "*" o "?" (dove "*" rappresenta un numero qualsiasi di simboli e "?" qualsiasi singolo simbolo). Ad esempio, *1234? nella Lista bloccati. Filtro chiamate/SMS blocca le chiamate o gli SMS da un numero che contiene qualsiasi carattere dopo 1234.
- **Contenente il testo** - frase chiave che indica che il messaggio SMS ricevuto è indesiderato (spam). Filtro chiamate/SMS blocca solo gli SMS che contengono la frase chiave, mentre consente tutti gli altri SMS.

Se si desidera bloccare tutti gli SMS in entrata da uno specifico numero nella Lista bloccati, lasciare vuoto il campo **Contenente il testo** per questa voce.

5. Premere **OK** per salvare le modifiche.

ELIMINAZIONE DI VOCI DALLA LISTA BLOCCATI

È possibile eliminare un numero dalla Lista bloccati. È inoltre possibile svuotare la Lista bloccati di Filtro chiamate/SMS rimuovendo da essa tutte le voci.

➡ *Per eliminare una voce dalla Lista bloccati di Filtro chiamate/SMS:*

1. Selezionare **Menu** → **Filtro chiamate/SMS**.

Verrà aperto **Filtro chiamate/SMS**.

2. Selezionare l'opzione **Lista bloccati**.

Verrà aperta la finestra **Lista bloccati**.

3. Selezionare la voce da eliminare dall'elenco, quindi selezionare **Menu** → **Elimina**.

4. Confermare la cancellazione della voce premendo **Si**.

➡ *Per cancellare la Lista bloccati di Filtro chiamate/SMS:*

1. Selezionare **Menu** → **Filtro chiamate/SMS**.

Verrà aperto **Filtro chiamate/SMS**.

2. Selezionare l'opzione **Lista bloccati**.

Verrà aperta la finestra **Lista bloccati**.

3. Selezionare **Menu** → **Elimina tutto**.

La lista verrà svuotata.

CREAZIONE DI UNA LISTA CONSENTITI

La Lista consentiti contiene le voci relative ai numeri per i quali Filtro chiamate/SMS consente le chiamate e gli SMS all'utente. Ogni voce contiene le seguenti informazioni:

- Numero di telefono da cui Filtro chiamate/SMS consente le chiamate e/o gli SMS.
- Tipi di eventi consentiti da Filtro chiamate/SMS per il numero. Sono disponibili i seguenti tipi di eventi: Chiamate e SMS, Solo chiamate e Solo SMS.
- Frase chiave utilizzata da Filtro chiamate/SMS per classificare un SMS come desiderato (non spam). Filtro chiamate/SMS consente solo gli SMS che contengono la frase chiave, mentre blocca tutti gli altri SMS.

Filtro chiamate/SMS consente le chiamate e gli SMS che soddisfano tutti i criteri di una voce nella Lista consentiti. Le chiamate e gli SMS che non soddisfano anche solo uno dei criteri di una voce nella Lista consentiti vengono bloccati.

IN QUESTA SEZIONE

Aggiunta di voci alla Lista consentiti.....	62
Modifica di voci nella Lista consentiti	63
Eliminazione di voci dalla Lista consentiti.....	64

AGGIUNTA DI VOCI ALLA LISTA CONSENTITI

Non è possibile aggiungere contemporaneamente lo stesso numero con criteri di filtro identici nella Lista bloccati e nella Lista consentiti di Filtro chiamate/SMS. Se un numero con i criteri di filtro specificati è già stato salvato in uno dei due elenchi, Kaspersky Mobile Security 9 segnalerà l'evento e verrà visualizzato un messaggio sullo schermo.

➔ Per aggiungere una voce alla Lista consentiti di Filtro chiamate/SMS:

1. Selezionare **Menu** → **Filtro chiamate/SMS**.

Verrà aperto **Filtro chiamate/SMS**.

2. Selezionare l'opzione **Lista consentiti**.

Verrà aperta la finestra **Lista consentiti**.

3. Selezionare **Menu** → **Aggiungi**.

Verrà aperta la finestra **Nuova voce**.

4. Selezionare i valori per le seguenti impostazioni (vedere la figura seguente).

- **Consenti in entrata** - tipo di evento consentito da Filtro chiamate/SMS per i numeri nella Lista consentiti:
 - **Chiamate e SMS**: consente le chiamate e gli SMS in entrata.
 - **Solo chiamate**: consente solo le chiamate in entrata.
 - **Solo SMS**: consente solo i messaggi SMS in entrata.

- **Numero di telefono** - numero di telefono per cui Filtro chiamate/SMS blocca le informazioni in arrivo. Il numero di telefono deve comprendere solo caratteri alfanumerici; può iniziare con una cifra, una lettera o essere preceduto dal simbolo "+". Per i numeri è inoltre possibile utilizzare i caratteri jolly "*" o "?" (dove "*" rappresenta un numero qualsiasi di simboli e "?" qualsiasi singolo simbolo). Ad esempio, *1234? nella Lista consentiti. Filtro chiamate/SMS consente le chiamate o gli SMS da un numero che contiene qualsiasi carattere dopo 1234.
- **Contenente il testo** - frase chiave che indica che il messaggio SMS ricevuto è desiderato. Per i numeri nella Lista consentiti, Filtro chiamate/SMS consente solo gli SMS che contengono la frase chiave, mentre blocca tutti gli altri SMS.

Se si desidera consentire tutti gli SMS in entrata da uno specifico numero nella Lista consentiti, lasciare vuoto il campo **Contenente il testo** per questa voce.

Figura 20: Impostazioni della voce

5. Premere **OK** per salvare le modifiche.

MODIFICA DI VOCI NELLA LISTA CONSENTITI

È possibile cambiare i valori di tutte le impostazioni relative ai numeri presenti nella Lista consentiti.

► Per modificare una voce nella Lista consentiti di Filtro chiamate/SMS:

1. Selezionare **Menu** → **Filtro chiamate/SMS**.
Verrà aperto **Filtro chiamate/SMS**.
2. Selezionare l'opzione **Lista consentiti**.
Verrà aperta la finestra **Lista consentiti**.
3. Selezionare dall'elenco la voce che si desidera modificare, quindi selezionare **Menu** → **Modifica**.
Verrà aperta la finestra **Modifica voce**.
4. Modificare le impostazioni necessarie:

- **Consenti in entrata** - tipo di evento consentito da Filtro chiamate/SMS per i numeri nella Lista consentiti:
 - **Chiamate e SMS:** consente le chiamate e gli SMS in entrata.
 - **Solo chiamate:** consente solo le chiamate in entrata.
 - **Solo SMS:** consente solo i messaggi SMS in entrata.
- **Numero di telefono** - numero di telefono per cui Filtro chiamate/SMS blocca le informazioni in arrivo. Il numero di telefono deve comprendere solo caratteri alfanumerici; può iniziare con una cifra, una lettera o essere preceduto dal simbolo "+". Per i numeri è inoltre possibile utilizzare i caratteri jolly "*" o "?" (dove "*" rappresenta un numero qualsiasi di simboli e "?" qualsiasi singolo simbolo). Ad esempio, *1234? nella Lista consentiti. Filtro chiamate/SMS consente le chiamate o gli SMS da un numero che contiene qualsiasi carattere dopo 1234.
- **Contenente il testo** - frase chiave che indica che il messaggio SMS ricevuto è desiderato. Per i numeri nella Lista consentiti, Filtro chiamate/SMS consente solo gli SMS che contengono la frase chiave, mentre blocca tutti gli altri SMS.

Se si desidera consentire tutti gli SMS in entrata da uno specifico numero nella Lista consentiti, lasciare vuoto il campo **Contenente il testo** per questa voce.

5. Premere **OK** per salvare le modifiche.

ELIMINAZIONE DI VOCI DALLA LISTA CONSENTITI

È possibile eliminare una voce dalla Lista consentiti o cancellarla completamente

➔ *Per eliminare una voce dalla Lista consentiti di Filtro chiamate/SMS:*

1. Selezionare **Menu** → **Filtro chiamate/SMS**.

Verrà aperto **Filtro chiamate/SMS**.

2. Selezionare l'opzione **Lista consentiti**.

Verrà aperta la finestra **Lista consentiti**.

3. Selezionare la voce da eliminare dall'elenco, quindi selezionare **Menu** → **Elimina**.

4. Confermare la cancellazione della voce premendo **Si**.

➔ *Per cancellare la Lista consentiti di Filtro chiamate/SMS:*

1. Selezionare **Menu** → **Filtro chiamate/SMS**.

Verrà aperto **Filtro chiamate/SMS**.

2. Selezionare l'opzione **Lista consentiti**.

Verrà aperta la finestra **Lista consentiti**.

3. Selezionare **Menu** → **Elimina tutto**.

La lista verrà svuotata.

RISPOSTA AI MESSAGGI SMS E ALLE CHIAMATE DA CONTATTI NON IN RUBRICA

Se per Filtro chiamate/SMS è selezionata le modalità **Entrambe le liste** o **Lista consentiti** (vedere la sezione "**Informazioni sulle modalità di Filtro chiamate/SMS**" a pagina 58), è possibile impostare la risposta di Filtro chiamate/SMS agli SMS e alle chiamate dai numeri non inclusi nei contatti. Inoltre, Filtro chiamate/SMS consente di espandere la Lista consentiti aggiungendovi i numeri dall'elenco dei contatti.

Per modificare i valori delle impostazioni, utilizzare i pulsanti di spostamento o la penna stilo del dispositivo.

➔ Per selezionare la risposta di Filtro chiamate/SMS a un numero non incluso nella rubrica:

1. Selezionare **Menu** → **Filtro chiamate/SMS**.

Verrà aperto **Filtro chiamate/SMS**.

2. Selezionare l'opzione **Modalità**.

3. Verrà aperta la finestra **Modalità**.

4. Selezionare il valore desiderato per l'impostazione **Consenti contatti** (vedere la figura seguente):

- se si desidera che Filtro chiamate/SMS consideri i numeri della rubrica come Lista consentiti aggiuntiva e blocchi la ricezione degli SMS e delle chiamate da mittenti non presenti nella rubrica, selezionare la casella **Consenti contatti**;
- per far sì che Filtro chiamate/SMS filtri i messaggi SMS e le chiamate in base alla modalità di Filtro chiamate/SMS impostata, deselezionare la casella **Consenti contatti**.



Figura 21: Risposta di Filtro chiamate/SMS ai numeri non inclusi nella rubrica del dispositivo

5. Premere **OK** per salvare le modifiche.

RISPOSTA AI MESSAGGI SMS DA MITTENTI NON NUMERICI

Se è selezionata la modalità di Filtro chiamate/SMS **Entrambe le liste** o **Lista bloccati** (vedere la sezione "**Modifica della modalità di Filtro chiamate/SMS**" a pagina 58), è possibile espandere l'elenco includendo tutti i mittenti non numerici (che includono lettere). Filtro chiamate/SMS bloccherà quindi i messaggi SMS provenienti dai mittenti non numerici.

Per modificare i valori delle impostazioni, utilizzare i pulsanti di spostamento o la penna stilo del dispositivo.

► Per impostare la risposta di Filtro chiamate/SMS alla ricezione di messaggi da mittenti non numerici:

1. Selezionare **Menu** → **Filtro chiamate/SMS**.

Verrà aperto **Filtro chiamate/SMS**.

2. Selezionare l'opzione **Modalità**.

Verrà aperta la finestra **Modalità**.

3. Selezionare un valore per l'impostazione **Blocca mittenti non numerici** (vedere la figura seguente):

- per far sì che Filtro chiamate/SMS elimini automaticamente i messaggi dai mittenti non numerici, selezionare la casella **Blocca mittenti non numerici**;
- se si desidera che Filtro chiamate/SMS filtri gli SMS e le chiamate dai mittenti non numerici solo in base alla modalità di Anti-Spam impostata, deselegionare la casella **Blocca mittenti non numerici**.

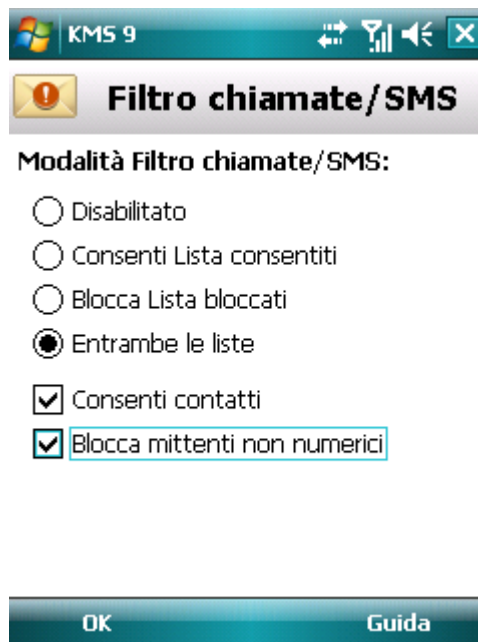


Figura 22: Configurazione dell'azione di Filtro chiamate/SMS alla ricezione di SMS da mittenti non numerici

4. Premere **OK** per salvare le modifiche.

SELEZIONE DI UNA RISPOSTA ALLE CHIAMATE IN ENTRATA

In modalità **Entrambe le liste** (vedere la sezione "**Informazioni sulle modalità di Filtro chiamate/SMS**" a pagina [58](#)), Filtro chiamate/SMS controlla gli SMS in entrata in base alla Lista bloccati e alla Lista consentiti.

Se il numero del mittente non è contenuto né nella Lista bloccati né nella Lista consentiti, Filtro chiamate/SMS informerà l'utente e richiederà di selezionare una delle azioni suggerite nei confronti del messaggio SMS in entrata (vedere la figura seguente).



Figura 23: Notifica di Filtro chiamate/SMS della ricezione di un messaggio

È possibile selezionare una delle seguenti azioni da eseguire nei confronti dell'SMS:

- Per bloccare il messaggio SMS e aggiungere il numero di telefono del mittente alla Lista bloccati, selezionare **Menu** → **Aggiungi a Lista bloccati**.
- Per recapitare il messaggio SMS e aggiungere il numero di telefono del mittente alla Lista consentiti, selezionare **Menu** → **Aggiungi a Lista consentiti**.
- Per recapitare il messaggio SMS senza aggiungere il numero di telefono del mittente a nessuna delle liste, premere **Ignora**.

Le informazioni su messaggi bloccati vengono inserite nel report dell'applicazione (vedere la sezione "Report dell'applicazione" a pagina [112](#)).

SELEZIONE DI UNA RISPOSTA ALLE CHIAMATE IN ENTRATA

In modalità **Entrambe le liste** (vedere la sezione "**Informazioni sulle modalità di Filtro chiamate/SMS**" a pagina [58](#)), Filtro chiamate/SMS controlla le chiamate in entrata in base alla Lista bloccati e alla Lista consentiti.

Se il numero del mittente non è contenuto né nella Lista bloccati né nella Lista consentiti, Filtro chiamate/SMS informerà l'utente dopo aver completato la scansione e richiederà un'azione nei confronti della chiamata in entrata (vedere la figura seguente).



Figura 24: Notifica di Filtro chiamate/SMS su una chiamata accettata

È possibile selezionare una delle seguenti azioni da eseguire per il numero da cui è stata effettuata la chiamata:

- Per aggiungere il numero di telefono del chiamante alla Lista bloccati, selezionare **Menu** → **Aggiungi a Lista bloccati**.
- Per aggiungere il numero di telefono del chiamante alla Lista consentiti, selezionare **Menu** → **Aggiungi a Lista consentiti**.
- Se non si desidera aggiungere il numero di telefono del chiamante ad alcun elenco, premere **Ignora**.

Le informazioni sulle chiamate bloccate vengono immesse nel report dell'applicazione.

LIMITAZIONE DELLE CHIAMATE E DEI MESSAGGI SMS IN USCITA. PARENTAL CONTROL

Questa sezione fornisce informazioni sul componente Parental Control, che consente di limitare le chiamate e i messaggi SMS in uscita verso numeri definiti. La sezione spiega inoltre come creare una lista di numeri consentiti e bloccati e come specificare le impostazioni di Parental Control.

IN QUESTA SEZIONE

Informazioni su Parental Control	69
Modalità del Parental Control	69
Abilitazione/disabilitazione del Parental Control	70
Creazione di una Lista bloccati	70
Creazione di una Lista consentiti	73

INFORMAZIONI SU PARENTAL CONTROL

Parental Control consente di controllare i messaggi SMS e le chiamate in uscita in base ai numeri inclusi nella Lista bloccati e nella Lista consentiti. Il funzionamento del componente è determinato dalla modalità selezionata.

Nella modalità **Lista bloccati**, Parental Control blocca i messaggi SMS e le chiamate in uscita ai numeri inclusi nella Lista bloccati, mentre consente quelli a tutti gli altri numeri. Nella modalità **Lista consentiti**, Parental Control consente solo i messaggi SMS e le chiamate in uscita ai numeri inclusi nella Lista consentiti, mentre blocca quelli a tutti gli altri numeri. Nella modalità **Disabilitato**, Parental Control non filtra i messaggi SMS e le chiamate in uscita.

Parental Control blocca solo i messaggi SMS in uscita inviati utilizzando le funzionalità standard del dispositivo. I messaggi SMS in uscita inviati utilizzando applicazioni di terze parti sono consentiti.

Le informazioni sul funzionamento del componente vengono inserite nel report dell'applicazione (vedere la sezione "Report dell'applicazione" a pagina [112](#)).

MODALITÀ DEL PARENTAL CONTROL

La modalità del Parental Control determina la regola che definisce il controllo dei messaggi SMS e delle chiamate in uscita.

Sono disponibili le seguenti modalità del Parental Control:

- **Disabilitato:** disabilita Parental Control. I messaggi SMS e le chiamate in uscita non vengono controllati.

Questa modalità è selezionata per impostazione predefinita.

- **Lista consentiti:** consente l'invio di messaggi SMS e/o di effettuare chiamate solo ai numeri inclusi nella Lista consentiti (vedere la sezione "Creazione di una Lista consentiti" a pagina [73](#)). Tutti gli altri messaggi SMS e le altre chiamate sono bloccati.
- **Lista bloccati:** blocca l'invio di messaggi SMS e/o di chiamate solo ai numeri inclusi nella Lista bloccati (vedere la sezione "Creazione di una Lista bloccati" a pagina [70](#)). Tutti gli altri messaggi SMS e le altre chiamate sono consentiti.

È possibile modificare la modalità di Parental Control (vedere la sezione "Abilitazione/disabilitazione di Parental Control" a pagina [70](#)). La modalità di funzionamento corrente di Parental Control è visualizzata nella finestra **Parental Control** accanto alla voce **Modalità**.

ABILITAZIONE/DISABILITAZIONE DEL PARENTAL CONTROL

➔ Per modificare la modalità del Parental Control:

1. Selezionare **Menu** → **Parental Control**.
2. Verrà aperta la finestra **Parental Control**.
3. Selezionare l'opzione **Modalità**.
Verrà aperta la finestra **Modalità**.
4. Selezionare una delle modalità del Parental Control suggerita (vedere la figura seguente).



Figura 25: Modifica della modalità di Parental Control

5. Premere **OK** per salvare le modifiche.

CREAZIONE DI UNA LISTA BLOCCATI

È possibile creare una Lista bloccati, che verrà utilizzata da Parental Control per bloccare le chiamate e i messaggi SMS in uscita. La lista contiene i numeri di telefono per i quali l'invio di SMS e l'esecuzione di chiamate non è bloccato.

Le informazioni sulle chiamate e sui messaggi SMS bloccati vengono registrate nel report dell'applicazione (vedere la sezione "Report dell'applicazione" a pagina [112](#)).

IN QUESTA SEZIONE

Aggiunta di voci alla Lista bloccati.....	71
Modifica di voci nella Lista bloccati	72
Eliminazione di voci dalla Lista bloccati.....	73

AGGIUNTA DI VOCI ALLA LISTA BLOCCATI

Non è possibile aggiungere contemporaneamente lo stesso numero con criteri di filtro identici nella Lista bloccati e nella Lista consentiti di Parental Control. Se un numero con i criteri specificati è già stato salvato in uno dei due elenchi, Kaspersky Mobile Security 9 segnalerà l'evento e verrà visualizzato un messaggio sullo schermo.

➔ *Per aggiungere una voce alla Lista bloccati di Parental Control:*

1. Selezionare **Menu** → **Parental Control**.
2. Verrà aperta la finestra **Parental Control**.
3. Selezionare l'opzione **Lista bloccati**.
Verrà aperta la finestra **Lista bloccati**.
4. Selezionare **Menu** → **Aggiungi**.
Verrà aperta la finestra **Nuova voce**.
5. Selezionare i valori per le seguenti impostazioni (vedere la figura seguente):
 - **Blocca in uscita:** tipo di informazione in uscita, dal numero dell'abbonato, che verrà bloccato da Parental Control:
 - **Chiamate e SMS:** blocca le chiamate e i messaggi SMS in uscita.
 - **Solo chiamate:** blocca solo le chiamate in uscita.
 - **Solo SMS:** blocca solo i messaggi SMS in uscita.

- **Numero di telefono:** numero di telefono che verrà bloccato per i messaggi SMS e/o le chiamate in uscita. Il numero di telefono deve comprendere solo caratteri alfanumerici; può iniziare con una cifra, una lettera o essere preceduto dal simbolo "+". Per i numeri è inoltre possibile utilizzare i caratteri jolly "*" o "?" (dove "*" rappresenta un numero qualsiasi di simboli e "?" qualsiasi singolo simbolo).

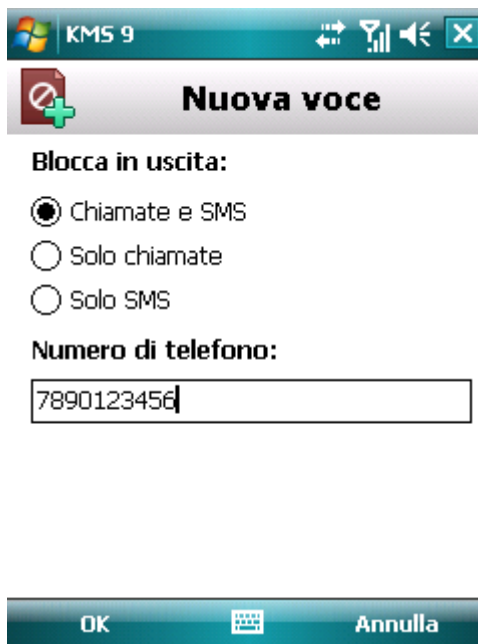


Figura 26: Impostazioni della voce

6. Premere **OK** per salvare le modifiche.

MODIFICA DI VOCI NELLA LISTA BLOCCATI

È possibile cambiare il valore di tutte le impostazioni relative ai numeri presenti nella Lista bloccati.

► Per modificare una voce della Lista bloccati di Parental Control:

1. Selezionare **Menu** → **Parental Control**.
2. Verrà aperta la finestra **Parental Control**.
3. Selezionare l'opzione **Lista bloccati**.
Verrà aperta la finestra **Lista bloccati**.
4. Selezionare dall'elenco la voce che si desidera modificare, quindi selezionare **Menu** → **Modifica**.
Verrà aperta la finestra **Modifica voce**.
5. Modificare le impostazioni necessarie:

- **Blocca in uscita:** tipo di informazione in uscita, dal numero dell'abbonato, che verrà bloccato da Parental Control:
 - **Chiamate e SMS:** blocca le chiamate e i messaggi SMS in uscita.
 - **Solo chiamate:** blocca solo le chiamate in uscita.
 - **Solo SMS:** blocca solo i messaggi SMS in uscita.

- **Numero di telefono:** numero di telefono che verrà bloccato per i messaggi SMS e/o le chiamate in uscita. Il numero di telefono deve comprendere solo caratteri alfanumerici; può iniziare con una cifra, una lettera o essere preceduto dal simbolo "+". Per i numeri è inoltre possibile utilizzare i caratteri jolly "*" o "?" (dove "*" rappresenta un numero qualsiasi di simboli e "?" qualsiasi singolo simbolo).

6. Premere **OK** per salvare le modifiche.

ELIMINAZIONE DI VOCI DALLA LISTA BLOCCATI

In caso di aggiunta accidentale di un numero alla Lista bloccati è possibile eliminare tale numero dalla lista. È inoltre possibile svuotare la Lista bloccati di Parental Control rimuovendo da essa tutte le voci.

➤ *Per eliminare una voce dalla Lista bloccati di Parental Control, eseguire le seguenti operazioni:*

1. Selezionare **Menu** → **Parental Control**.
2. Verrà aperta la finestra **Parental Control**.
3. Selezionare l'opzione **Lista bloccati**.
Verrà aperta la finestra **Lista bloccati**.
4. Selezionare la voce da eliminare dall'elenco, quindi selezionare **Menu** → **Elimina**.
5. Confermare l'eliminazione premendo **Sì**.

➤ *Per cancellare la Lista bloccati di Filtro chiamate/SMS:*

1. Selezionare **Menu** → **Parental Control**.
2. Verrà aperta la finestra **Parental Control**.
3. Selezionare l'opzione **Lista bloccati**.
Verrà aperta la finestra **Lista bloccati**.
4. Selezionare **Menu** → **Elimina tutto**.

La lista verrà svuotata.

CREAZIONE DI UNA LISTA CONSENTITI

È possibile creare una Lista consentiti, che verrà utilizzata da Filtro chiamate/SMS per consentire le chiamate e gli SMS in entrata.

IN QUESTA SEZIONE

Aggiunta di voci alla Lista consentiti.....	74
Modifica di voci nella Lista consentiti	75
Eliminazione di voci dalla Lista consentiti.....	75

AGGIUNTA DI VOCI ALLA LISTA CONSENTITI

Non è possibile aggiungere contemporaneamente lo stesso numero con criteri di filtro identici nella Lista bloccati e nella Lista consentiti di Parental Control. Se un numero con i criteri specificati è già stato salvato in uno dei due elenchi, Kaspersky Mobile Security 9 segnalerà l'evento e verrà visualizzato un messaggio sullo schermo.

➔ Per aggiungere una voce alla Lista consentiti di Parental Control:

1. Selezionare **Menu** → **Parental Control**.
2. Verrà aperta la finestra **Parental Control**.
3. Selezionare l'opzione **Lista consentiti**.
4. Verrà aperta la finestra **Lista consentiti**.
5. Selezionare **Menu** → **Aggiungi**.

Verrà aperta la finestra **Nuova voce**.

6. Selezionare i valori per le seguenti impostazioni (vedere la figura seguente):
 - **Consenti in uscita:** tipo di informazione in uscita che Parental Control consente di inviare al numero dell'abbonato:
 - **Chiamate e SMS:** consente le chiamate e i messaggi SMS in uscita.
 - **Solo chiamate:** consente solo le chiamate in uscita.
 - **Solo SMS:** consente solo i messaggi SMS in uscita.
 - **Numero di telefono:** numero di telefono a cui Parental Control consente l'invio di messaggi SMS e/o di chiamate in uscita. Il numero di telefono deve comprendere solo caratteri alfanumerici; può iniziare con una cifra, una lettera o essere preceduto dal simbolo "+". Per i numeri è inoltre possibile utilizzare i caratteri jolly "*" o "?" (dove "*" rappresenta un numero qualsiasi di simboli e "?" qualsiasi singolo simbolo).

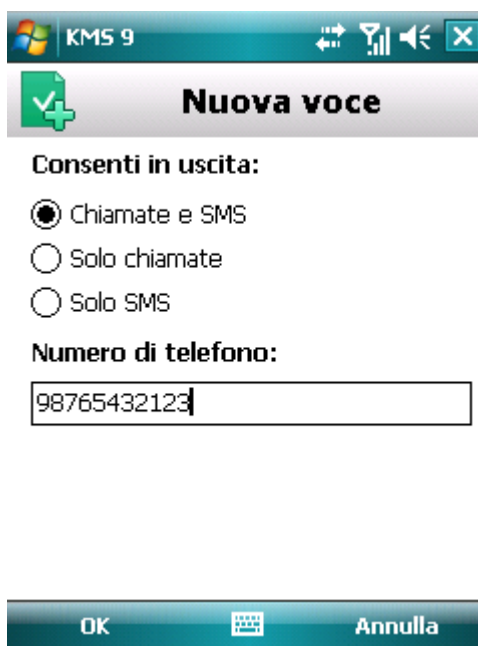


Figura 27: Impostazioni della voce

7. Premere **OK** per salvare le modifiche.

MODIFICA DI VOCI NELLA LISTA CONSENTITI

È possibile cambiare i valori di tutte le impostazioni relative ai numeri presenti nella Lista consentiti.

➤ *Per modificare una voce della Lista consentiti di Parental Control:*

1. Selezionare **Menu** → **Parental Control**.
2. Verrà aperta la finestra **Parental Control**.
3. Selezionare l'opzione **Lista consentiti**.
4. Verrà aperta la finestra **Lista consentiti**.
5. Selezionare dall'elenco la voce che si desidera modificare, quindi selezionare **Menu** → **Modifica**.

Verrà aperta la finestra **Modifica voce**.

6. Modificare le impostazioni necessarie:
 - **Consenti in uscita:** tipo di informazione in uscita che Parental Control consente di inviare al numero dell'abbonato:
 - **Chiamate e SMS:** consente le chiamate e i messaggi SMS in uscita.
 - **Solo chiamate:** consente solo le chiamate in uscita.
 - **Solo SMS:** consente solo i messaggi SMS in uscita.
 - **Numero di telefono:** numero di telefono a cui Parental Control consente l'invio di messaggi SMS e/o di chiamate in uscita. Il numero di telefono deve comprendere solo caratteri alfanumerici; può iniziare con una cifra, una lettera o essere preceduto dal simbolo "+". Per i numeri è inoltre possibile utilizzare i caratteri jolly "*" o "?" (dove "*" rappresenta un numero qualsiasi di simboli e "?" qualsiasi singolo simbolo).

7. Premere **OK** per salvare le modifiche.

ELIMINAZIONE DI VOCI DALLA LISTA CONSENTITI

È possibile rimuovere una voce o svuotare completamente la Lista consentiti.

➤ *Per eliminare una voce dalla Lista consentiti di Parental Control:*

1. Selezionare **Menu** → **Parental Control**.
2. Verrà aperta la finestra **Parental Control**.
3. Selezionare l'opzione **Lista consentiti**.
4. Verrà aperta la finestra **Lista consentiti**.
5. Selezionare la voce da eliminare dall'elenco, quindi selezionare **Menu** → **Elimina**.
6. Confermare l'eliminazione premendo **Sì**.

➤ *Per cancellare la Lista consentiti di Filtro chiamate/SMS:*

1. Selezionare **Menu** → **Parental Control**.

2. Verrà aperta la finestra **Parental Control**.
3. Selezionare l'opzione **Lista consentiti**.
4. Verrà aperta la finestra **Lista consentiti**.
5. Selezionare **Menu** → **Elimina tutto**.

La lista verrà svuotata.

PROTEZIONE DEI DATI IN CASO DI SMARRIMENTO O FURTO DEL DISPOSITIVO

Questa sezione fornisce informazioni su Antifurto, che, in caso di furto o smarrimento del dispositivo, consente di bloccare l'accesso non autorizzato ai dati salvati nel dispositivo mobile e ne semplifica l'individuazione.

Viene inoltre descritto come abilitare o disabilitare la funzione Antifurto, impostarne i parametri di esecuzione e avviare Antifurto in remoto da un altro dispositivo mobile.

IN QUESTA SEZIONE

Informazioni su Antifurto.....	77
Blocco del dispositivo.....	78
Eliminazione dei dati personali.....	80
Creazione di un elenco di cartelle da eliminare.....	82
Monitoraggio della sostituzione di una scheda SIM sul dispositivo.....	83
Determinazione delle coordinate geografiche del dispositivo.....	84
Avvio remoto delle funzioni di Antifurto.....	87

INFORMAZIONI SU ANTIFURTO

Il componente Antifurto protegge i dati memorizzati nel dispositivo da accessi non autorizzati.

Antifurto comprende le seguenti funzioni:

- **SMS-Block** consente di bloccare il dispositivo in remoto e di specificare il testo da visualizzare sullo schermo del dispositivo bloccato.
- **SMS-Clean** consente di eliminare in remoto i dati dell'utente dal dispositivo (voci nei contatti, SMS, immagini, calendario, report, impostazioni di connessione a Internet) e le informazioni dalle schede di memoria e dalle cartelle nell'elenco per l'eliminazione.
- **SIM Watch** consente di ottenere il numero di telefono corrente in caso di sostituzione della scheda SIM, nonché di bloccare il dispositivo se la scheda SIM viene sostituita o se il dispositivo viene attivato senza una scheda SIM. Le informazioni sul numero di telefono vengono inviate in un messaggio al numero di telefono e/o all'indirizzo e-mail specificato.
- La funzionalità **SMS-Find** consente di individuare un dispositivo in remoto. Le coordinate geografiche del dispositivo vengono inviate in un messaggio al numero di telefono da cui è stato inviato uno speciale comando SMS e a un indirizzo e-mail.

Dopo l'installazione di Kaspersky Mobile Security 9, tutte le funzioni di Antifurto sono disabilitate.

Kaspersky Mobile Security 9 consente di abilitare Antifurto in remoto inviando un comando SMS (vedere "Avvio remoto delle funzioni di Antifurto" a pagina [87](#)) da un altro dispositivo mobile.

Per avviare Antifurto in remoto, è necessario conoscere la password segreta dell'applicazione impostata al primo avvio di

Kaspersky Mobile Security 9.

Lo stato corrente di ogni funzione viene visualizzato nella schermata **Antifurto** accanto al nome della funzione.

Le informazioni sul funzionamento del componente vengono inserite nel report dell'applicazione (vedere "Report dell'applicazione" a pagina [112](#)).

BLOCCO DEL DISPOSITIVO

Quando viene ricevuto uno speciale comando SMS, la funzione SMS-Block consente di bloccare in remoto l'accesso al dispositivo e ai dati memorizzati su di esso. Il dispositivo può essere sbloccato solo dopo aver immesso la password segreta.

Questa funzione non blocca il dispositivo ma abilita semplicemente l'opzione di blocco remoto.

➔ Per abilitare la funzione SMS-Block:

1. Selezionare **Menu** → **Antifurto**.

Verrà aperta la finestra **Antifurto**.

2. Selezionare l'opzione **SMS-Block**.

Verrà aperta la finestra **SMS-Block**.

3. Selezionare la casella **Abilita SMS-Block**.

4. Immettere il messaggio da visualizzare sullo schermo del dispositivo in modalità di blocco nel campo **Testo quando bloccato** (vedere la figura seguente). Per impostazione predefinita, per il messaggio verrà utilizzato il testo standard in cui è possibile aggiungere il numero di telefono del proprietario.

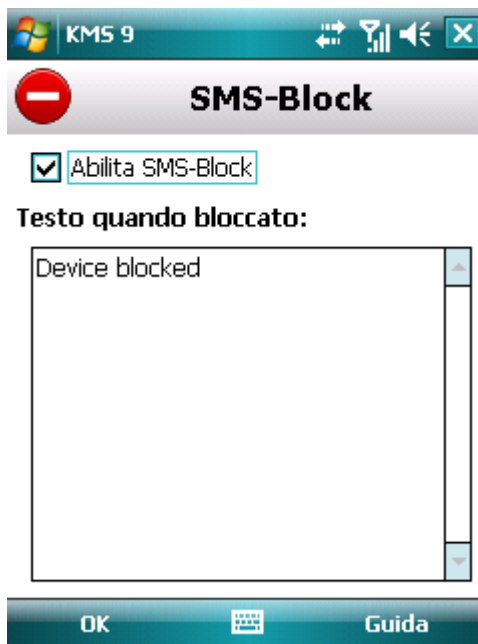


Figura 28: Impostazioni della funzione SMS-Block

5. Premere **OK** per salvare le modifiche.

Se la funzione SMS-Block è abilitata in un altro dispositivo, è possibile bloccare il dispositivo utilizzando uno dei seguenti metodi:

- Utilizzare un'applicazione Kaspersky Lab per dispositivi mobili, come ad esempio Kaspersky Mobile Security 9, su un altro dispositivo mobile per creare e inviare un comando SMS al dispositivo. Per creare uno speciale comando SMS, utilizzare la funzione **Invia comando**. Il dispositivo riceverà un SMS nascosto e verrà bloccato.
- In un altro dispositivo mobile, creare e inviare un SMS contenente un testo speciale e la password segreta precedentemente impostata per il dispositivo ricevente. Il dispositivo riceverà un SMS nascosto e verrà bloccato.

Per i messaggi SMS in uscita verranno applicati i costi previsti dall'operatore di telefonia mobile dell'altro dispositivo.

Per bloccare il dispositivo in remoto, è consigliabile utilizzare la funzione **Invia comando**. In tal modo, la password segreta dell'applicazione viene inviata in formato crittografato.

➔ Per inviare un comando SMS a un altro dispositivo utilizzando la funzione **Invia comando**:

1. Selezionare **Menu** → **Avanzate**.

Verrà aperta la finestra **Avanzate**.

2. Selezionare **Invia comando**.

Verrà aperta la finestra **Invia comando**.

3. Selezionare il valore **SMS-Block** per l'opzione **Comando SMS** (vedere la figura seguente).

4. Nel campo **Numero di telefono** immettere il numero di telefono del dispositivo a cui inviare il comando SMS.

5. Nel campo **Password del dispositivo remoto** immettere la password segreta impostata nel dispositivo a cui inviare il comando SMS.

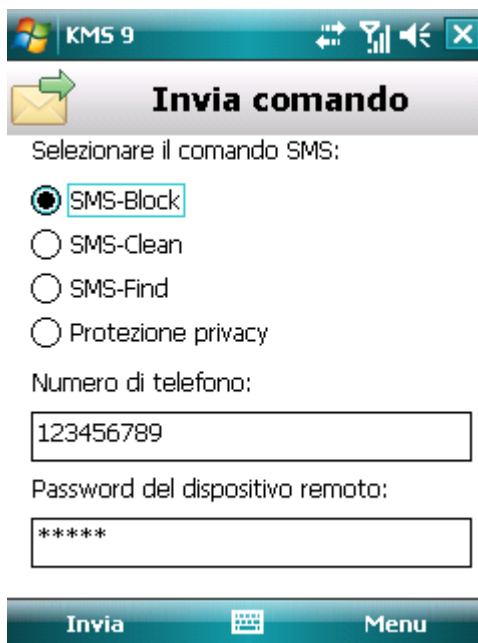


Figura 29: Avvio remoto del blocco del dispositivo

6. Premere **Invia**.

- Per creare un messaggio SMS con le funzioni standard di creazione SMS del telefono,

inviare un messaggio SMS al dispositivo che si desidera bloccare. Il messaggio SMS deve contenere il testo block:<password>, dove <password> è la password segreta impostata sul dispositivo da bloccare. Il messaggio non distingue tra maiuscole/minuscole e gli spazi prima o dopo i due punti vengono ignorati.

ELIMINAZIONE DEI DATI PERSONALI

Quando viene ricevuto uno speciale comando SMS, la funzione SMS-Clean consente di eliminare le seguenti informazioni memorizzate nel dispositivo:

- dati personali dell'utente (voci nei contatti e nella scheda SIM, messaggi SMS, immagini, calendario, impostazioni di connessione a Internet);
- informazioni sulla scheda di memoria;
- file nella cartella **Documenti** e nelle cartelle incluse nell'elenco **Cartelle da eliminare**.

Questa funzione non elimina i dati memorizzati sul dispositivo, ma include l'opzione di cancellazione.

- Per abilitare la funzione SMS-Clean:

1. Selezionare **Menu** → **Antifurto**.

Verrà aperta la finestra **Antifurto**.

2. Selezionare l'opzione **SMS-Clean**.

Verrà aperta la finestra **SMS-Clean**.

3. Selezionare l'opzione **Modalità**.

Verrà aperta la finestra **SMS-Clean**.

4. Selezionare la casella **Abilita SMS-Clean**.

5. Selezionare le informazioni che si desidera eliminare selezionando le caselle accanto alle impostazioni desiderate nella sezione **Elimina** (vedere la figura seguente):

- per eliminare i dati personali, selezionare la casella **Dati personali**;

- per eliminare i file nella cartella **Documenti** e nelle cartelle incluse nell'elenco **Cartelle da eliminare**, selezionare la casella **Cartelle**.

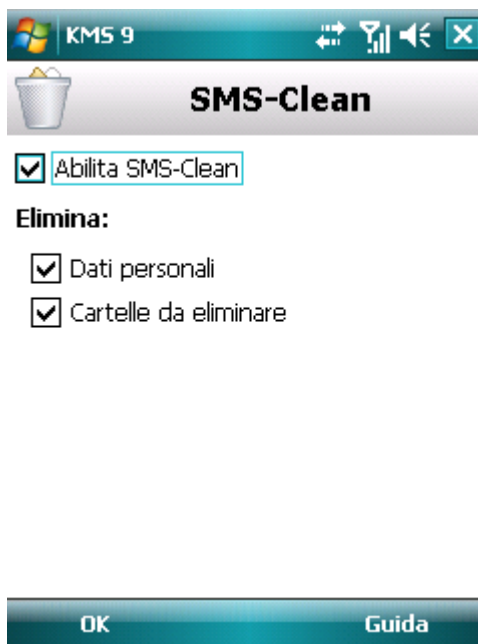


Figura 30: Selezione del tipo di dati da eliminare

6. Premere **OK** per salvare le modifiche.
7. Passare alla creazione dell'elenco **Cartelle da eliminare** (vedere la sezione "**Creazione di un elenco di cartelle da eliminare**" a pagina [82](#)).

Abilitando la funzione, è possibile eliminare dal dispositivo i dati personali utilizzando i seguenti metodi:

- Utilizzare un'applicazione Kaspersky Lab per dispositivi mobili, come ad esempio Kaspersky Mobile Security 9, su un altro dispositivo mobile per creare e inviare un comando SMS al dispositivo. Per creare uno speciale comando SMS, utilizzare la funzione Invia comando. Il dispositivo riceverà un messaggio SMS nascosto e le informazioni verranno eliminate.
- In un altro dispositivo mobile, creare e inviare un SMS contenente un testo speciale e la password segreta precedentemente impostata per il dispositivo ricevente.

Per eliminare le informazioni nel dispositivo in remoto, è consigliabile utilizzare la funzione Invia comando, che trasmette il comando e la password segreta in forma criptata.

➔ Per inviare un comando a un altro dispositivo:

1. Selezionare **Menu** → **Avanzate**.

Verrà aperta la finestra **Avanzate**.

2. Selezionare **Invia comando**.

Verrà aperta la finestra **Invia comando**.

3. Selezionare il valore **SMS-Clean** per l'impostazione **Comando SMS** (vedere la figura seguente).

4. Nel campo **Numero di telefono** immettere il numero di telefono del dispositivo a cui inviare il comando SMS.

5. Nel campo **Password del dispositivo remoto** immettere la password segreta impostata nel dispositivo a cui inviare il comando SMS.

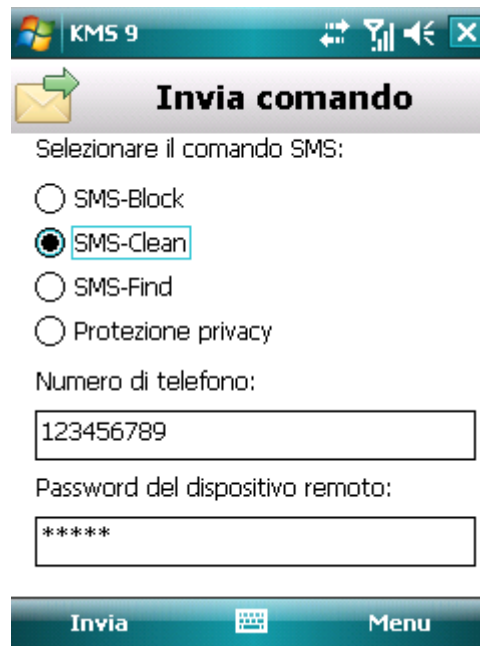


Figura 31: Avvio remoto dell'eliminazione dei dati personali

6. Premere **Invia**.

► Per creare un messaggio SMS con le funzioni standard di creazione SMS del telefono,

Inviare un SMS standard che contiene il testo wipe:<password>, dove <password> è la password segreta impostata sul dispositivo. Il messaggio non distingue tra maiuscole/minuscole e gli spazi prima o dopo i due punti vengono ignorati.

CREAZIONE DI UN ELENCO DI CARTELLE DA ELIMINARE

La funzione SMS-Clean consente di creare un elenco di cartelle da eliminare quando viene ricevuto uno speciale messaggio SMS.

Per abilitare Antifurto per l'eliminazione di tutte le cartelle incluse nell'elenco dopo la ricezione di uno speciale messaggio SMS, verificare che la casella **Cartelle** sia selezionata nell'opzione **Modalità**.

► Per aggiungere una cartella all'elenco di cartelle da eliminare:

1. Selezionare **Menu** → **Antifurto**.

Verrà aperta la finestra **Antifurto**.

2. Selezionare l'opzione **SMS-Clean**.

Verrà aperta la finestra **SMS-Clean**.

3. Selezionare l'opzione **Cartelle da eliminare**.

Verrà aperta la finestra **Cartelle da eliminare**.

4. Selezionare **Menu** → **Aggiungi cartella** (vedere la figura seguente).

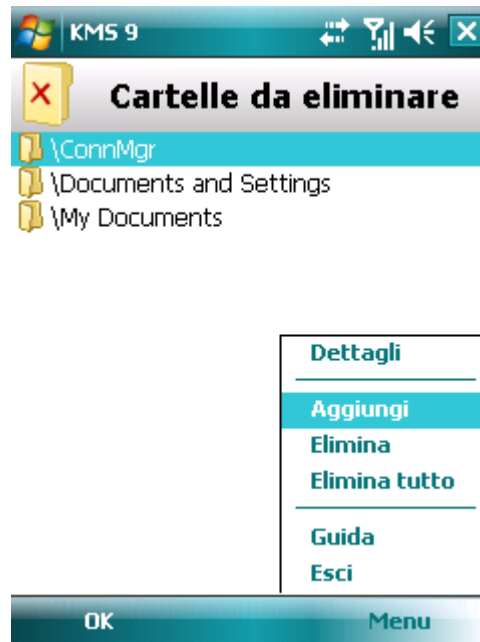


Figura 32: Selezione delle cartelle da eliminare.

5. Selezionare la cartella desiderata dalla struttura di cartelle e premere **Seleziona**.

La cartella verrà aggiunta all'elenco.

► *Per rimuovere una cartella dall'elenco:*

1. Selezionare **Menu** → **Antifurto**.

Verrà aperta la finestra **Antifurto**.

2. Selezionare l'opzione **SMS-Clean**.

Verrà aperta la finestra **SMS-Clean**.

3. Selezionare l'opzione **Cartelle da eliminare**.

Verrà aperta la finestra **Cartelle da eliminare**.

4. Selezionare una cartella dall'elenco e premere **Menu** → **Elimina**.

MONITORAGGIO DELLA SOSTITUZIONE DI UNA SCHEDE SIM SUL DISPOSITIVO

Se la scheda SIM viene sostituita, SIM Watch consente di inviare un messaggio con il nuovo numero al proprio numero di telefono e/o indirizzo e-mail o di bloccare il dispositivo.

► *Per abilitare la funzione SIM Watch e monitorare la sostituzione della scheda SIM:*

1. Selezionare **Menu** → **Antifurto**.

Verrà aperta la finestra **Antifurto**.

2. Selezionare l'opzione **SIM Watch**.

Verrà aperta la finestra **SIM Watch**.

3. Selezionare la casella **Abilita SIM Watch**.

4. Per controllare la sostituzione della scheda SIM sul dispositivo, selezionare le seguenti impostazioni (vedere la figura seguente):

- Per inviare automaticamente un messaggio sul nuovo numero di telefono, immettere il numero di telefono al quale deve essere inviato il messaggio nel campo **Numero di telefono** della sezione **Invia nuovo numero**.
- Il numero di telefono può iniziare con una cifra o con un "+" e deve contenere solo cifre.
- Per ricevere un messaggio e-mail con il nuovo numero di telefono del dispositivo, immettere un indirizzo e-mail nel campo **Indirizzo e-mail** della sezione **Invia nuovo numero**.
 - Per bloccare il dispositivo quando la scheda SIM viene sostituita o quando il dispositivo viene acceso senza una scheda, selezionare la casella **Blocca** per l'impostazione **Durante sostituzione scheda SIM**. È possibile sbloccare il dispositivo solo dopo aver immesso la password segreta.
 - Per visualizzare un messaggio sullo schermo in modalità blocco, inserirlo nel campo **Testo quando bloccato**. Per impostazione predefinita, per il messaggio verrà utilizzato il testo standard in cui è possibile aggiungere il numero di telefono del proprietario.



Figura 33: Impostazioni della funzione SIM Watch

5. Premere **OK** per salvare le modifiche.

DETERMINAZIONE DELLE COORDINATE GEOGRAFICHE DEL DISPOSITIVO

Quando viene ricevuto uno speciale comando SMS, SMS-Find consente di rilevare le coordinate geografiche dispositivo e di inviarle tramite un SMS e un messaggio e-mail al dispositivo richiedente e a un indirizzo e-mail.

Per i messaggi SMS in uscita verrà applicato il costo previsto dall'operatore di telefonia mobile.

Questa opzione funziona solo su dispositivi con ricevitore GPS integrato. Il ricevitore GPS viene abilitato automaticamente quando il dispositivo riceve uno speciale messaggio SMS. Se il dispositivo si trova all'interno dell'area raggiunta dai satelliti, la funzione SMS-Find riceve e invia le coordinate geografiche del dispositivo. Se non sono disponibili satelliti al momento dell'invio della richiesta, SMS-Find tenta periodicamente di determinare le coordinate e di inviare i dati sulla posizione del dispositivo.

➔ Per abilitare la funzione SMS-Find:

1. Selezionare **Menu** → **Antifurto**.

Verrà aperta la finestra **Antifurto**.

2. Selezionare l'opzione **SMS-Find**.

Verrà aperta la finestra **SMS-Find**.

3. Selezionare la casella **Abilita SMS-Find**.

Per impostazione predefinita, Kaspersky Mobile Security 9 invia le coordinate del dispositivo in un messaggio SMS di risposta.

4. Per ricevere le coordinate del dispositivo anche via e-mail, immettere l'indirizzo e-mail per l'impostazione **Invia coordinate** (vedere la figura seguente).



Figura 34: Impostazioni della funzione SMS-Find

5. Premere **OK** per salvare le modifiche.

È possibile richiedere le coordinate di un dispositivo su cui è abilitata la funzione SMS-Find utilizzando i seguenti metodi:

- Utilizzare un'applicazione Kaspersky Lab per dispositivi mobili, come ad esempio Kaspersky Mobile Security 9, su un altro dispositivo mobile per creare e inviare un comando SMS al dispositivo. Il dispositivo riceverà un SMS nascosto e l'applicazione invierà le coordinate del dispositivo. Per creare uno speciale comando SMS, utilizzare la funzione Invia comando.

- In un altro dispositivo mobile, creare e inviare un SMS contenente un testo speciale e la password segreta precedentemente impostata per il dispositivo ricevente. Il dispositivo riceverà un SMS nascosto e l'applicazione invierà le coordinate del dispositivo.

Per i messaggi SMS in uscita verranno applicati i costi previsti dall'operatore di telefonia mobile dell'altro dispositivo.

Per determinare la posizione del dispositivo in remoto, è consigliabile utilizzare la funzione **Invia comando**, che trasmette il comando e la password segreta in forma criptata.

► Per inviare un comando a un altro dispositivo:

1. Selezionare **Menu** → **Avanzate**.

Verrà aperta la finestra **Avanzate**.

2. Selezionare **Invia comando**.

Verrà aperta la finestra **Invia comando**.

3. Selezionare il valore **SMS-Find** per l'impostazione **Comando SMS** (vedere la figura seguente).
4. Nel campo **Numero di telefono** immettere il numero di telefono del dispositivo a cui inviare il comando SMS.
5. Nel campo **Password del dispositivo remoto** immettere la password segreta impostata nel dispositivo a cui inviare il comando SMS.

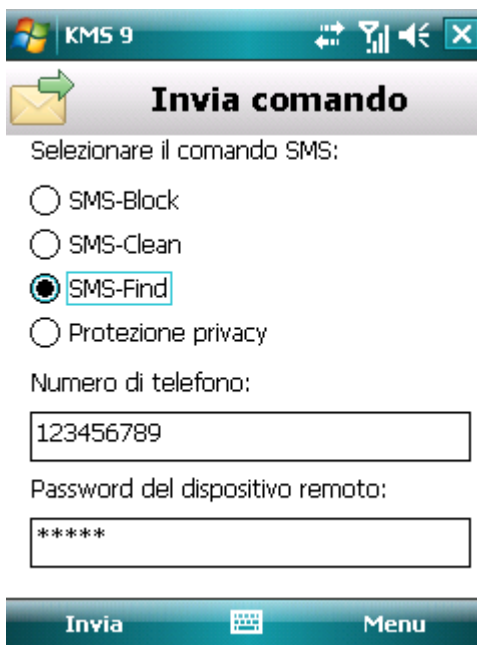


Figura 35: Determinazione della posizione del dispositivo

6. Premere **Invia**.

► Per creare un messaggio SMS con le funzioni standard di creazione SMS del telefono,

Inviare un SMS standard che contiene il testo `find:<password>`, dove `<password>` è la password segreta impostata sul dispositivo. Il messaggio non distingue tra maiuscole/minuscole e gli spazi prima o dopo i due punti vengono ignorati.

Un messaggio SMS con le coordinate del dispositivo verrà inviato al numero di telefono da cui è stato inviato il comando SMS e a un indirizzo e-mail, se questo è stato precedentemente specificato nelle opzioni di SMS-Find.

AVVIO REMOTO DELLE FUNZIONI DI ANTIFURTO

L'applicazione consente di inviare uno speciale comando SMS per eseguire da remoto le funzioni di Antifurto su un altro dispositivo in cui è installato Kaspersky Mobile Security. Un comando SMS viene inviato come messaggio SMS criptato e contiene la password segreta dell'applicazione impostata nel dispositivo ricevente. La ricezione del comando SMS non potrà essere notata in alcun modo.

Per l'invio dell'SMS viene applicato il costo previsto dall'operatore di telefonia mobile dell'utente.

► Per inviare un comando a un altro dispositivo:

1. Selezionare **Menu** → **Avanzate**.

Verrà aperta la finestra **Avanzate**.

2. Selezionare **Invia comando**.

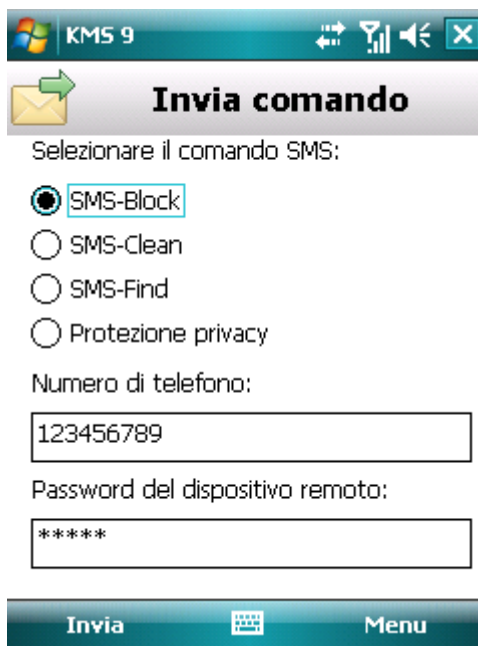
3. Verrà aperta la finestra **Invia comando**.

4. Selezionare uno dei valori disponibili per l'impostazione **Comando SMS** (vedere la figura seguente):

- **SMS-Block.**
- **SMS-Clean.**
- **SMS-Find.**
- **Protezione privacy** (vedere la sezione "**Mascheramento dei dati personali**" a pagina [89](#)).

5. Nel campo **Numero di telefono** immettere il numero di telefono del dispositivo a cui inviare il comando SMS.

6. Nel campo **Password del dispositivo remoto** immettere la password segreta impostata nel dispositivo a cui inviare il comando SMS.



KMS 9

Invia comando

Selezionare il comando SMS:

- SMS-Block
- SMS-Clean
- SMS-Find
- Protezione privacy

Numero di telefono:

123456789

Password del dispositivo remoto:

Invia Menu

Figura 36: Avvio remoto delle funzioni di Antifurto

7. Premere **Invia**.

PROTEZIONE PRIVACY

Questa sezione fornisce informazioni sul componente Protezione privacy, che consente di nascondere le informazioni riservate dell'utente.

IN QUESTA SEZIONE

Protezione privacy.....	89
Modalità di Protezione privacy	89
Abilitazione/disabilitazione di Protezione privacy	90
Abilitazione automatica di Protezione privacy	91
Abilitazione remota di Protezione privacy.....	92
Creazione di un elenco di numeri privati	94
Selezione dei dati da nascondere: Protezione privacy	97

PROTEZIONE PRIVACY

Protezione privacy nasconde i dati riservati in base all'elenco di contatti, che contiene numeri privati. Per i numeri riservati, Protezione privacy nasconde le voci dei contatti, gli SMS in entrata, inviati e le bozze, nonché le voci della cronologia delle chiamate. Protezione privacy elimina il segnale dei nuovi SMS e nasconde i messaggi stessi nella Posta in arrivo. Protezione privacy blocca le chiamate in entrata dei numeri privati e non visualizza le informazioni sulle chiamate in entrata sullo schermo. Come risultato, il chiamante riceve un segnale di occupato. Per visualizzare le chiamate e gli SMS in entrata per il periodo di tempo in cui Protezione privacy era abilitato, disabilitare Protezione privacy. Quando Protezione privacy è nuovamente abilitato, le informazioni vengono nascoste.

È possibile abilitare Protezione privacy da Kaspersky Mobile Security 9 o in remoto da un altro dispositivo mobile. In entrambi i casi, sarà possibile disabilitare Protezione privacy solo dall'applicazione.

Le informazioni sul funzionamento di Protezione privacy vengono memorizzate nel report (vedere "Report dell'applicazione" a pagina [112](#)).

MODALITÀ DI PROTEZIONE PRIVACY

È possibile gestire la modalità di funzionamento di Protezione privacy. La modalità definisce se il componente è abilitato o disabilitato.

Per impostazione predefinita, il componente Protezione privacy è disabilitato.

Sono disponibili le seguenti modalità di Protezione privacy:

- **Normale** – i dati personali sono visualizzati. Le impostazioni di Protezione privacy sono accessibili per la modifica.
- **Privato** – i dati personali sono nascosti. Le impostazioni di Protezione privacy non possono essere modificate.

È possibile impostare Protezione privacy per l'avvio automatico (vedere la sezione "Abilitazione automatica di Protezione privacy" a pagina [91](#)) o avviarlo da remoto da un altro dispositivo (vedere la sezione "Abilitazione remota di Protezione privacy" a pagina [92](#)).

La modalità di funzionamento corrente del componente è visualizzata nella scheda **Protezione privacy** accanto alla voce del menu **Modalità**.

La modifica della modalità di Protezione privacy può richiedere un certo tempo.

ABILITAZIONE/DISABILITAZIONE DI PROTEZIONE PRIVACY

La modalità di Protezione privacy può essere modificata come indicato di seguito:

- dal menu delle impostazioni del componente;
- dal menu **Protezione privacy**.

► *Per modificare la modalità di Protezione privacy:*

1. Selezionare **Menu** → **Protezione privacy**.

Verrà aperta la finestra **Protezione privacy**.

2. Selezionare l'opzione **Modalità**.

Verrà aperta la finestra **Modalità**.

3. Selezionare un valore per l'impostazione **Modalità** (vedere la figura seguente).

4. Premere **OK**.



Figura 37: Modifica della modalità di Protezione privacy

5. Confermare la modifica della modalità di Protezione privacy premendo **Sì**.

► *Per modificare rapidamente la modalità di Protezione privacy:*

1. Selezionare **Menu** → **Protezione privacy**.

Verrà aperta la finestra **Protezione privacy**.

2. Premere **Privato / Normale**. Il nome del pulsante cambia in base allo stato corrente del componente Protezione privacy.
3. Confermare la modifica della modalità di Protezione privacy premendo **Sì**.

ABILITAZIONE AUTOMATICA DI PROTEZIONE PRIVACY

È possibile configurare l'abilitazione automatica dell'occultamento delle informazioni riservate dopo un intervallo di tempo specificato. La funzione viene attivata dopo che il dispositivo passa in modalità di risparmio energia.

Disabilitare Protezione privacy prima di modificarne le impostazioni.

➤ *Per abilitare automaticamente Protezione privacy dopo un intervallo di tempo specificato:*

1. Selezionare **Menu** → **Protezione privacy**.
Verrà aperta la finestra **Protezione privacy**.
2. Selezionare l'opzione **Modalità**.
3. Verrà aperta la finestra **Modalità**.
4. Selezionare la casella **Blocca accesso** (vedere la figura seguente).
5. Selezionare un valore per l'intervallo di tempo da attendere prima di abilitare Protezione privacy. Per eseguire questa operazione, impostare uno dei valori disponibili per l'impostazione **Ora**:
 - **Nessun ritardo**.
 - **Dopo 1 minuto**.
 - **Dopo 5 minuti**.
 - **Dopo 15 minuti**.

- Dopo 1 ora.



Figura 38: Avvio automatico di Protezione privacy

6. Premere **OK**.

ABILITAZIONE REMOTA DI PROTEZIONE PRIVACY

Kaspersky Mobile Security 9 consente di abilitare Protezione privacy da remoto tramite un altro dispositivo mobile. A tale scopo, attivare prima l'opzione Nascondi tramite comando SMS sul dispositivo.

► Per consentire l'avvio remoto di Protezione privacy:

1. Selezionare **Menu** → **Protezione privacy**.

Verrà aperta la finestra **Protezione privacy**.

2. Selezionare l'opzione **Modalità**.

Verrà aperta la finestra **Modalità**.

3. Selezionare la casella **Nascondi tramite comando SMS** (vedere la figura seguente).



Figura 39: Impostazioni di abilitazione remota di Protezione privacy

4. Premere **OK**.

È possibile abilitare Protezione privacy in remoto utilizzando uno dei seguenti metodi:

- Utilizzare un'applicazione Kaspersky Lab per dispositivi mobili, come ad esempio Kaspersky Mobile Security 9, su un altro dispositivo mobile per creare e inviare un comando SMS al dispositivo. Il dispositivo riceverà un SMS nascosto e le informazioni riservate verranno nascoste. Per creare uno speciale comando SMS, utilizzare la funzione Invia comando.
- In un altro dispositivo mobile, creare e inviare un messaggio SMS contenente un testo speciale e la password segreta dell'applicazione specificata nel dispositivo. Il dispositivo riceverà un SMS e le informazioni riservate verranno nascoste.

Per gli SMS in uscita verranno applicati i costi previsti dall'operatore di telefonia mobile del dispositivo da cui viene inviato il comando SMS.

➔ Per abilitare Protezione privacy in remoto utilizzando uno speciale comando SMS:

1. Selezionare **Menu** → **Avanzate**.

Verrà aperta la finestra **Avanzate**.

2. Selezionare **Invia comando**.

Verrà aperta la finestra **Invia comando**.

3. Selezionare il valore **Protezione privacy** per l'impostazione **Comando SMS** (vedere la figura seguente).

4. Nel campo **Numero di telefono** immettere il numero di telefono del dispositivo a cui inviare il comando SMS.

5. Nel campo **Password del dispositivo remoto** immettere la password segreta impostata nel dispositivo a cui inviare il comando SMS.

KMS 9

Invia comando

Selezionare il comando SMS:

SMS-Block

SMS-Clean

SMS-Find

Protezione privacy

Numero di telefono:

123456789

Password del dispositivo remoto:

Invia Menu

Figura 40: Avvio remoto di Protezione privacy

6. Premere **Invia**.

Quando il dispositivo riceve il comando SMS, il componente Protezione privacy viene abilitato automaticamente.

- Per abilitare Protezione privacy in remoto utilizzando gli strumenti standard del telefono per la creazione di SMS:

Inviare un SMS al dispositivo che si desidera bloccare; il messaggio deve contenere il testo `hide:<password>`, dove `<password>` è la password segreta dell'applicazione impostata nel dispositivo da bloccare. Il messaggio non distingue tra maiuscole/minuscole e gli spazi prima o dopo i due punti vengono ignorati.

CREAZIONE DI UN ELENCO DI NUMERI PRIVATI

L'Elenco contatti contiene i numeri privati per cui il componente Protezione privacy nasconde le informazioni e gli eventi. È possibile estendere l'elenco aggiungendo manualmente un numero oppure importando un numero dai Contatti o dalla scheda SIM.

Prima di creare l'elenco dei contatti, disabilitare l'occultamento delle informazioni riservate.

IN QUESTA SEZIONE

Aggiunta di un numero all'elenco dei contatti privati	95
Modifica di un numero nell'elenco dei contatti privati	95
Eliminazione di un numero dall'elenco dei contatti privati	96

AGGIUNTA DI UN NUMERO ALL'ELENCO DEI NUMERI PRIVATI

È possibile aggiungere un numero manualmente (ad esempio, +12345678) oppure importare un numero dai contatti o dalla scheda SIM.

Disabilitare Protezione privacy prima di modificarne le impostazioni.

➤ Per aggiungere un numero di telefono all'elenco dei contatti:

1. Selezionare **Menu** → **Protezione privacy**.

Verrà aperta la finestra **Protezione privacy**.

2. Selezionare l'opzione **Elenco contatti**.

Verrà aperta la finestra **Elenco contatti**.

3. Eseguire una delle seguenti operazioni (vedere la figura seguente):

- Per aggiungere un numero dai contatti, selezionare **Menu** → **Aggiungi** → **Contatto Outlook**. Nella schermata **Contatto Outlook** visualizzata, specificare la voce desiderata e premere **Seleziona**.
- Per aggiungere un numero salvato sulla scheda SIM, selezionare **Menu** → **Aggiungi** → **Contatto da SIM**. Nella finestra **Contatto da SIM** visualizzata, selezionare la voce desiderata e premere **OK**.
- Per aggiungere un numero manualmente, selezionare **Menu** → **Aggiungi** → **Numero**. Nella finestra **Aggiungi voce** visualizzata, compilare il campo **Numero di telefono** e premere **OK**.

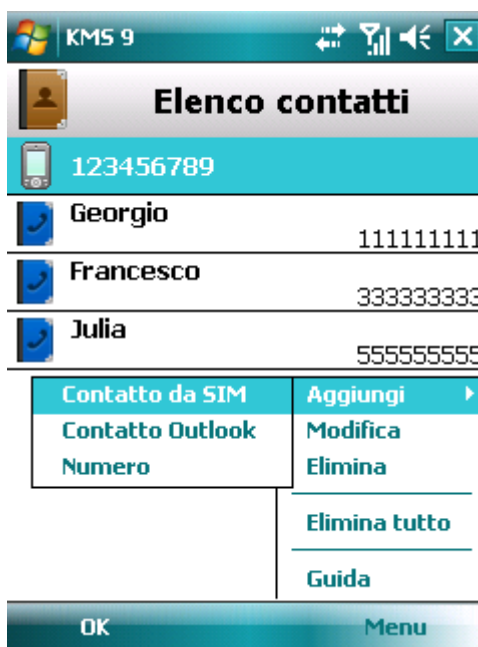


Figura 41: Aggiunta di voci all'elenco dei contatti protetti

Il numero verrà aggiunto all'elenco dei contatti.

MODIFICA DI UN NUMERO NELL'ELENCO DEI NUMERI PRIVATI

Prima di creare l'elenco dei contatti, disabilitare l'occultamento delle informazioni riservate.

I numeri di telefono aggiunti manualmente sono disponibili per la modifica solo nell'Elenco contatti. Non è possibile modificare i numeri selezionati dalla rubrica o da un elenco di numeri sulla scheda SIM.

► *Per modificare un numero di telefono nell'Elenco contatti:*

1. Selezionare **Menu** → **Protezione privacy**.
Verrà aperta la finestra **Protezione privacy**.
2. Selezionare l'opzione **Elenco contatti**.
Verrà aperta la finestra **Elenco contatti**.
3. Selezionare il numero da modificare dall'elenco dei contatti, quindi selezionare **Menu** → **Modifica**.
Verrà aperta la schermata **Modifica**.
4. Modificare i dati nel campo **Numero di telefono**.
5. Al termine della modifica, premere **OK**.

Il numero verrà modificato.

ELIMINAZIONE DI UN NUMERO DALL'ELENCO DEI NUMERI PRIVATI

È possibile eliminare un singolo numero dall'elenco dei contatti riservati o eliminare l'intero elenco di contatti.

Prima di creare l'elenco dei contatti, disabilitare l'occultamento delle informazioni riservate.

► *Per rimuovere un numero dall'Elenco contatti:*

1. Selezionare **Menu** → **Protezione privacy**.
Verrà aperta la finestra **Protezione privacy**.
2. Selezionare l'opzione **Elenco contatti**.
Verrà aperta la finestra **Elenco contatti**.
3. Selezionare il numero da eliminare, quindi selezionare **Menu** → **Elimina**.
4. Confermare l'eliminazione premendo **Sì**.

► *Per cancellare l'Elenco contatti:*

1. Selezionare **Menu** → **Protezione privacy**.
Verrà aperta la finestra **Protezione privacy**.
2. Selezionare l'opzione **Elenco contatti**.
Verrà aperta la finestra **Elenco contatti**.
3. Selezionare **Menu** → **Elimina tutto**.
4. Confermare l'eliminazione premendo **Sì**.

L'Elenco contatti risulterà vuoto.

SELEZIONE DEI DATI DA NASCONDERE: PROTEZIONE PRIVACY

Protezione privacy consente di nascondere le seguenti informazioni per i numeri nell'elenco dei contatti: contatti, corrispondenza SMS, voci del report delle chiamate, chiamate e messaggi SMS in entrata. È possibile selezionare le informazioni e gli eventi che devono essere nascosti da Protezione privacy per i numeri privati.

Disabilitare Protezione privacy prima di modificarne le impostazioni.

➔ Per selezionare le informazioni e gli eventi che devono essere nascosti per i numeri privati:

1. Selezionare **Menu** → **Protezione privacy**.

Verrà aperta la finestra **Protezione privacy**.

2. Selezionare l'opzione **Oggetti nascosti**.

Verrà aperta la finestra **Oggetti nascosti** (vedere la figura seguente).

3. Nella sezione **Nascondi voci**, selezionare le informazioni da nascondere per i numeri privati. Sono disponibili le seguenti impostazioni:

- **Contatti** - nasconde tutte le informazioni sui numeri riservati nei contatti
- **SMS** - nasconde i messaggi SMS nelle cartelle **In entrata**, **In uscita** e **Inviati** per i numeri riservati.
- **Chiamate** - accetta le chiamate dai numeri riservati, nascondendo il numero del chiamante e senza visualizzare le informazioni sui numeri riservati nell'elenco delle chiamate (in entrata, in uscita, senza risposta).

4. Nella sezione **Nascondi eventi**, selezionare gli eventi da nascondere per i numeri privati. Sono disponibili le seguenti impostazioni:

- **SMS in entrata** - non visualizza il recapito dei messaggi SMS in entrata (non verrà visualizzato alcun messaggio circa la ricezione di un nuovo messaggio SMS da un numero riservato). Tutti i messaggi SMS ricevuti dai numeri privati saranno disponibili per la visualizzazione se il componente Protezione privacy viene disabilitato.

- **Chiamate in entrata** : blocca le chiamate dai numeri privati (in questo caso il chiamante udirà il segnale di occupato). Le informazioni sulle chiamate ricevute vengono visualizzate se il componente Protezione privacy viene disabilitato.

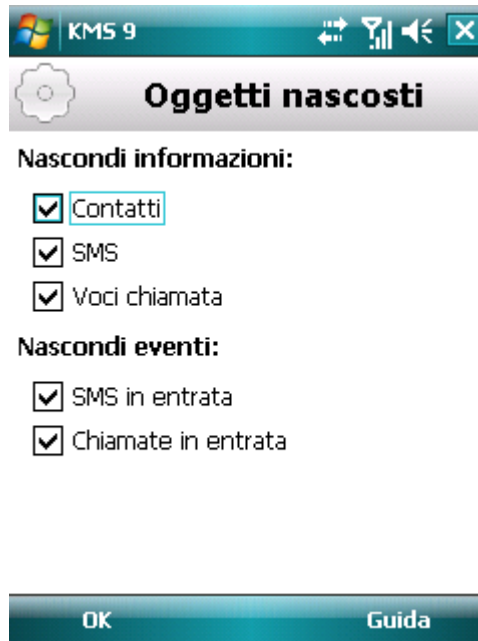


Figura 42: Selezione degli oggetti nascosti

5. Premere **OK**.

FILTRO DELL'ATTIVITÀ DI RETE. FIREWALL

Questa sezione fornisce informazioni sul componente Firewall, che consente di controllare le connessioni di rete nel dispositivo. Viene inoltre descritto come abilitare e disabilitare Firewall e selezionare la modalità desiderata.

IN QUESTA SEZIONE

Informazioni sul Firewall.....	98
Abilitazione/disabilitazione del Firewall	99
Selezione del livello di sicurezza del Firewall.....	99
Notifiche di blocco	100

INFORMAZIONI SUL FIREWALL

Firewall monitora le connessioni di rete del dispositivo in base alla modalità selezionata. Firewall consente di specificare le connessioni consentite (ad esempio, per la sincronizzazione con il sistema di amministrazione remota) e quelle bloccate (ad esempio, per la ricerca di informazioni su Internet e il download di file).

Al termine dell'installazione, il componente Firewall di Kaspersky Mobile Security 9 è disabilitato.

Firewall consente di impostare notifiche delle connessioni bloccate (vedere la sezione "Abilitazione/disabilitazione del Firewall" a pagina [99](#)).

Le informazioni sul funzionamento del Firewall vengono inserite nel report dell'applicazione (vedere la sezione "Report dell'applicazione" a pagina [112](#)).

ABILITAZIONE/DISABILITAZIONE DEL FIREWALL

È possibile selezionare la modalità utilizzata da Firewall per determinare le connessioni consentite e bloccate. Sono disponibili le seguenti modalità di Firewall:

- **Disabilitato:** tutte le attività di rete sono consentite. Questo è il livello di sicurezza predefinito selezionato.
- **Protezione minima:** vengono bloccate solo le connessioni in entrata. Le connessioni in uscita sono consentite.
- **Protezione massima:** vengono bloccate tutte le connessioni in entrata. Sono accessibili il controllo delle e-mail, la visualizzazione di siti web e il download di file. Le connessioni in uscita possono essere stabilite solo mediante le porte SSH, HTTP, HTTPS, IMAP, SMTP, POP3.
- **Blocca tutto:** blocca tutte le attività di rete tranne l'aggiornamento dei database dell'applicazione e il rinnovo della licenza.

È possibile cambiare il livello di sicurezza del Firewall (vedere la sezione "Selezione del livello di sicurezza del Firewall" a pagina [99](#)). La modalità corrente è visualizzata nella finestra **Firewall** accanto alla voce del menu **Modalità**.

SELEZIONE DEL LIVELLO DI SICUREZZA DEL FIREWALL

Per modificare i valori delle impostazioni, utilizzare i pulsanti di spostamento o la penna stilo del dispositivo.

➔ *Per impostare il livello di sicurezza del Firewall:*

1. Selezionare **Menu** → **Firewall**.

Verrà aperta la finestra **Firewall**.

2. Selezionare l'opzione **Modalità**.

Verrà aperta la finestra **Impostazioni**.

3. Selezionare uno dei livelli di sicurezza suggeriti (vedere la figura seguente).

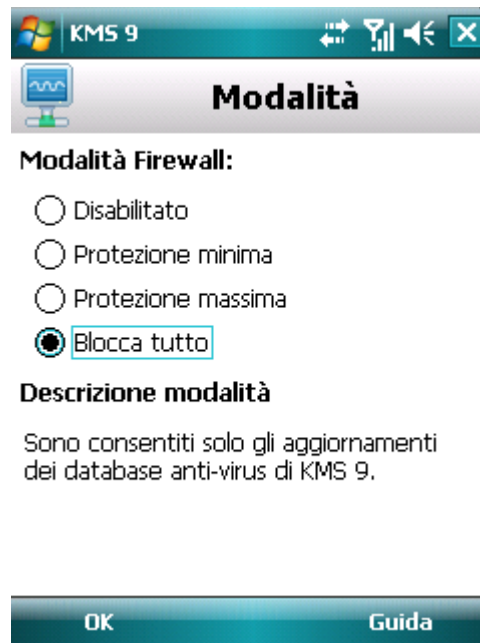


Figura 43: Selezione del livello di sicurezza di Firewall

4. Premere **OK**.

NOTIFICHE DI BLOCCO

Firewall consente la ricezione delle notifiche delle connessioni bloccate. È possibile gestire le notifiche del Firewall.

Per impostazione predefinita, la visualizzazione delle notifiche di blocco è disabilitata.

► *Per gestire le notifiche di blocco:*

1. Selezionare **Menu** → **Firewall**.
Verrà aperta la finestra **Firewall**.
2. Selezionare **Notifiche**.

Verrà aperta la schermata **Notifiche** (vedere la figura seguente).



Figura 44: Configurazione della visualizzazione delle notifiche di blocco

3. Nella sezione **Notifiche di blocco**, selezionare una delle azioni disponibili:
 - **Mostra** – consente la visualizzazione delle notifiche. Firewall notifica le connessioni bloccate.
 - **Non mostrare** – disabilita la visualizzazione delle notifiche. Firewall non notifica le connessioni bloccate.
4. Premere **OK**.

CRIPTAGGIO DEI DATI PERSONALI

Questa sezione fornisce informazioni sul componente Criptaggio, che consente di criptare le cartelle nel dispositivo. Viene inoltre descritto come criptare e decriptare le cartelle selezionate.

IN QUESTA SEZIONE

Informazioni sul componente Criptaggio	102
Criptaggio dei dati	102
Decriptaggio dei dati	104
Blocco dell'accesso ai dati criptati	105

INFORMAZIONI SUL COMPONENTE CRIPTAGGIO

Criptaggio consente di criptare i dati nell'elenco delle cartelle per il criptaggio. Il funzionamento della funzione Criptaggio è basato sulla funzione omonima integrata nel sistema operativo del dispositivo. La funzione Criptaggio consente di criptare qualsiasi tipo di cartella, ad eccezione delle cartelle di sistema. È possibile selezionare le cartelle per il criptaggio nella memoria del dispositivo o su una scheda di memoria. Per ottenere l'accesso ai dati criptati, immettere il codice PIN dell'applicazione impostato al primo avvio dell'applicazione.

Per avviare file eseguibili da una cartella criptata, è prima necessario decriptare la cartella. A tale scopo, è necessario immettere il codice PIN dell'applicazione.

Per accedere alle cartelle criptate, immettere la password segreta dell'applicazione (vedere la sezione "Immissione della password segreta" a pagina [28](#)). Dopo il passaggio del dispositivo alla modalità di risparmio energia o alla scadenza dell'intervallo di tempo impostato (vedere la sezione "Protezione dell'accesso ai dati criptati" a pagina [105](#)), l'accesso ai dati viene automaticamente bloccato.

I file nella cartella verranno criptati dopo l'esecuzione del comando **Cripta**. Successivamente, i file verranno criptati e decriptati in tempo reale quando vengono spostati in una cartella, rimossi da essa o al loro accesso.

Per avviare file eseguibili da una cartella criptata, è prima necessario decriptare la cartella.

Al termine dell'installazione di Kaspersky Mobile Security 9, il componente Criptaggio è disabilitato.

Le informazioni sul funzionamento del componente vengono inserite nel report dell'applicazione (vedere la sezione "Report dell'applicazione" a pagina [112](#)).

CRIPTAGGIO DEI DATI

Criptaggio consente di criptare qualsiasi numero di cartelle non di sistema presenti nella memoria del dispositivo o su una scheda di memoria.

L'elenco di tutti i file precedentemente criptati e decriptati è accessibile nella finestra **Criptaggio** da **Elenco cartelle**.

È possibile anche criptare immediatamente una o tutte le cartelle presenti nell'elenco delle cartelle.

➤ *Per criptare i dati:*

1. Selezionare **Menu** → **Criptaggio**.

Verrà aperta la finestra **Criptaggio**.

2. Selezionare l'opzione **Elenco cartelle**.

Verrà aperta la finestra **Elenco cartelle**.

3. Premere **Menu** → **Aggiungi cartella**.

Verrà aperta una schermata contenente la struttura dei file del sistema del dispositivo.

4. Selezionare la cartella da criptare e premere **Cripta** (vedere la figura seguente).

Per spostarsi nel file system, utilizzare la penna a stilo o i pulsanti di spostamento del dispositivo.

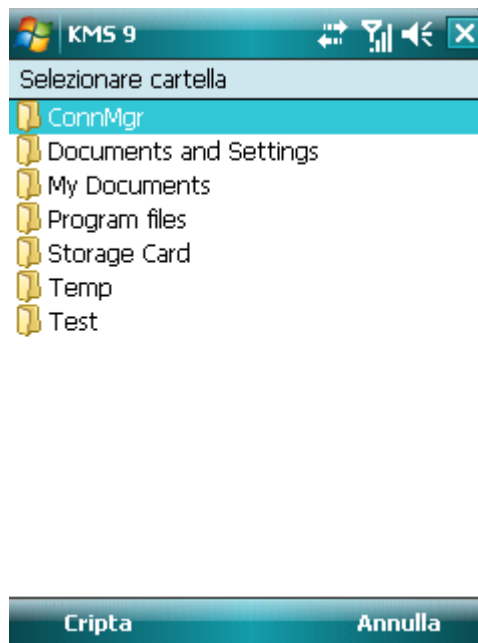


Figura 45: Criptaggio dei dati

Al termine della procedura di criptaggio, Kaspersky Mobile Security 9 informerà l'utente visualizzando una finestra di notifica.

5. Premere **OK**.

Se la cartella è criptata, il nome dell'opzione **Cripta** cambia in **Decripta** nel **Menu**.

Dopo il processo di criptaggio, i dati verranno decriptati e criptati automaticamente alla loro apertura o spostamento dalla cartella criptata oppure se si collocano nuovi dati nella cartella criptata.

➤ *Per criptare in un solo passaggio tutte le cartelle presenti nell'elenco, eseguire le seguenti operazioni:*

1. Selezionare **Menu** → **Criptaggio**.

Verrà aperta la finestra **Criptaggio**.

2. Selezionare l'opzione **Elenco cartelle**.

Verrà aperta la finestra **Elenco cartelle**.

3. Selezionare **Opzioni** → **Altre azioni** → **Cripta tutto**.

Al termine della procedura di criptaggio, Kaspersky Mobile Security 9 informerà l'utente visualizzando una finestra di notifica.

4. Premere **OK**.

DECRIPTAGGIO DEI DATI

È possibile decriptare completamente i dati criptati precedentemente (vedere la sezione "Criptaggio dei dati" a pagina [102](#)). È possibile decriptare una o tutte le cartelle precedentemente criptate nel dispositivo.

► Per decriptare una cartella precedentemente criptata:

1. Selezionare **Menu** → **Criptaggio**.

Verrà aperta la finestra **Criptaggio**.

2. Selezionare l'opzione **Elenco cartelle**.

Verrà aperta la finestra **Elenco cartelle** contenente un elenco di tutte le cartelle precedentemente decriptate e criptate.

3. Selezionare una cartella criptata dall'elenco e premere **Menu** → **Decripta** (vedere la figura seguente).

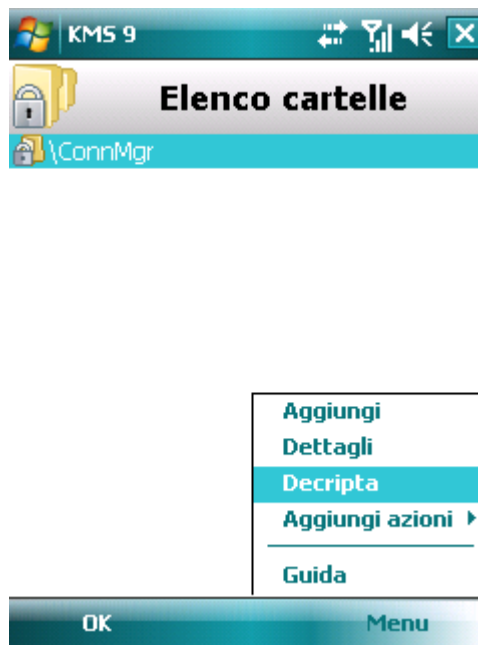


Figura 46: Abilitazione dell'opzione

Al termine della procedura di decriptaggio, Kaspersky Mobile Security 9 informerà l'utente visualizzando una finestra di notifica.

4. Premere **OK**.

Se la cartella è decriptata, il nome dell'opzione **Decripta** cambia in **Cripta** nel **Menu**. È possibile a questo punto criptare nuovamente i dati (vedere la sezione "Criptaggio dei dati" a pagina [102](#)).

► Per decriptare in un solo passaggio tutte le cartelle presenti nell'elenco, eseguire le seguenti operazioni:

1. Selezionare **Menu** → **Criptaggio**.

Verrà aperta la finestra **Criptaggio**.

2. Selezionare l'opzione **Elenco cartelle**.

Verrà aperta la finestra **Elenco cartelle**.

3. Selezionare **Opzioni** → **Altre azioni** → **Decrypta tutto**.

Al termine della procedura di decriptaggio, Kaspersky Mobile Security 9 informerà l'utente visualizzando una finestra di notifica.

4. Premere **OK**.

BLOCCO DELL'ACCESSO AI DATI CRIPTATI

È possibile impostare il tempo dopo il quale avviare il blocco dell'accesso alle cartelle criptate. Questa funzionalità viene attivata quando il dispositivo passa in modalità di risparmio energia. Per utilizzare i dati criptati, immettere il codice PIN dell'applicazione. Per continuare a utilizzare i dati criptati, è necessario immettere la password segreta (vedere la sezione "Impostazione della password segreta" a pagina [28](#)).

È anche possibile impedire momentaneamente l'accesso ai dati criptati e abilitare la richiesta della password segreta.

► *Per impedire l'accesso alla cartella con un ritardo temporale, eseguire le seguenti operazioni:*

1. Selezionare **Menu** → **Criptaggio**.

Verrà aperta la finestra **Criptaggio**.

2. Selezionare l'opzione **Blocca accesso**.

Verrà aperta la finestra **Blocca accesso**.

3. Immettere il tempo dopo il quale il dispositivo entra in standby e in cui i dati sono accessibili. Per eseguire questa operazione, selezionare per l'impostazione **Blocca accesso** uno dei valori suggeriti (vedere la figura seguente):

- **Nessun ritardo.**
- **Dopo 1 minuto.**
- **Dopo 5 minuti.**
- **Dopo 15 minuti.**

- Dopo 1 ora.

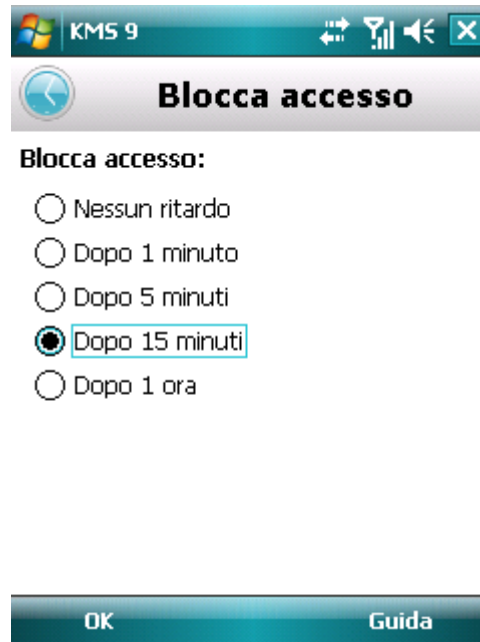


Figura 47: Blocco dell'accesso ai dati criptati

4. Premere **OK** per salvare le modifiche.

- ➔ Per bloccare immediatamente l'accesso a una cartella,

Premere l'icona di Kaspersky Mobile Security 9 nell'area di notifica della barra delle applicazioni e selezionare **Blocca dati** (vedere la figura seguente).



Figura 48: Menu di scelta rapida dell'applicazione nell'area di notifica del dispositivo

AGGIORNAMENTO DEI DATABASE DELL'APPLICAZIONE

Questa sezione fornisce informazioni sull'aggiornamento dei database dell'applicazione, che assicura la protezione aggiornata del dispositivo. Viene inoltre descritto come visualizzare informazioni sui database anti-virus installati, eseguire manualmente l'aggiornamento e configurare l'aggiornamento automatico dei database anti-virus.

IN QUESTA SEZIONE

Informazioni sull'aggiornamento dei database dell'applicazione	107
Visualizzazione delle informazioni sul database	108
Aggiornamento manuale	108
Aggiornamento pianificato	109
Aggiornamento in roaming	110

INFORMAZIONI SULL'AGGIORNAMENTO DEI DATABASE DELL'APPLICAZIONE

L'applicazione esegue la scansione del dispositivo per individuare eventuali programmi malware utilizzando il database anti-virus dell'applicazione, che contiene le descrizioni di tutti i programmi malware e di altri programmi indesiderati noti attualmente e i metodi per neutralizzarli. È quindi estremamente importante mantenere aggiornati i database anti-virus.

Si consiglia di aggiornare regolarmente i database dell'applicazione. Se sono trascorsi più di 15 giorni dall'ultimo aggiornamento, i database vengono considerati non aggiornati. La protezione risulterà pertanto meno affidabile.

Kaspersky Mobile Security 9 esegue gli aggiornamenti dei database dell'applicazione dai server degli aggiornamenti di Kaspersky Lab. Si tratta di siti Internet dedicati contenenti gli aggiornamenti per i database di tutti i prodotti Kaspersky Lab.

Per aggiornare i database anti-virus dell'applicazione è necessario disporre di una connessione Internet configurata sul proprio dispositivo mobile.

I database dell'applicazione anti-virus vengono aggiornati mediante il seguente algoritmo:

1. I database dell'applicazione installati sul dispositivo mobile vengono confrontati con quelli sul server degli aggiornamenti dedicato di Kaspersky Lab.
2. Kaspersky Mobile Security 9 esegue una delle seguenti operazioni:
 - Se sono installati i database anti-virus più recenti, sullo schermo viene visualizzato un messaggio informativo.
 - Se i database anti-virus installati sono diversi, viene scaricato e installato un nuovo pacchetto di aggiornamento.

Al termine del processo di aggiornamento, la connessione viene automaticamente chiusa. Se la connessione è stata stabilita prima dell'avvio dell'aggiornamento, rimarrà aperta per ulteriore utilizzo.

È possibile avviare l'operazione di aggiornamento manualmente in qualsiasi momento mentre il dispositivo è occupato con altre operazioni oppure pianificare aggiornamenti automatici.

Informazioni dettagliate sui database anti-virus in uso sono disponibili nella finestra **Avanzate** dall'opzione **Info database**.

Le informazioni sugli aggiornamenti dei database anti-virus vengono registrate nel report dell'applicazione (vedere la sezione "Report dell'applicazione" a pagina [112](#)).

VISUALIZZAZIONE DELLE INFORMAZIONI SUL DATABASE

È possibile visualizzare le seguenti informazioni sui database anti-virus dell'applicazione installati: ultimo aggiornamento, data di rilascio del database, dimensione del database e numero di voci che contiene.

► *Per visualizzare le informazioni sui database installati:*

1. Selezionare **Menu** → **Avanzate**.

Verrà aperta la finestra **Avanzate**.

2. Selezionare la scheda **Info database**.

Verrà visualizzata la finestra **Info database**, con informazioni sui database anti-virus del programma installati.

AGGIORNAMENTO MANUALE

È possibile avviare manualmente l'aggiornamento dei database anti-virus dell'applicazione.

► *Per avviare il processo di aggiornamento del database:*

1. Selezionare **Menu** → **Anti-Virus**.

Verrà aperta la finestra **Anti-Virus**.

2. Selezionare l'opzione **Aggiornamento**.

Verrà aperta la finestra **Aggiornamento**.

3. Selezionare l'opzione **Aggiornamento** (vedere la figura seguente).



Figura 49: Avvio manuale dell'aggiornamento

L'applicazione avvia il processo di aggiornamento dei database dal server Kaspersky Lab. Le informazioni sul processo di aggiornamento vengono visualizzate sullo schermo.

AGGIORNAMENTO PIANIFICATO

L'esecuzione regolare degli aggiornamenti è il requisito di base per l'efficace protezione del dispositivo contro le infezioni di oggetti malware. Per maggiore comodità, è possibile configurare aggiornamenti automatici dei database anti-virus.

► Per configurare una pianificazione per l'aggiornamento automatico dei database anti-virus:

1. Selezionare **Menu** → **Anti-Virus**.

Verrà aperta la finestra **Anti-Virus**.

2. Selezionare l'opzione **Aggiornamento**.

Verrà aperta la finestra **Aggiornamento**.

3. Selezionare l'opzione **Pianifica aggiornamento**.

Verrà aperta la finestra **Pianifica**.

4. Selezionare la casella **Aggiornamento pianificato** (vedere la figura seguente).

5. Creare una pianificazione per l'esecuzione degli aggiornamenti selezionando un valore per l'impostazione **Frequenza**:

- **Giornaliero** - aggiorna i database anti-virus ogni giorno. Immettere quindi un valore per l'impostazione **Ora**.

- **Settimanale** - aggiorna i database anti-virus una volta alla settimana. Selezionare quindi un valore per le impostazioni **Ora** e **Giorno della settimana**.

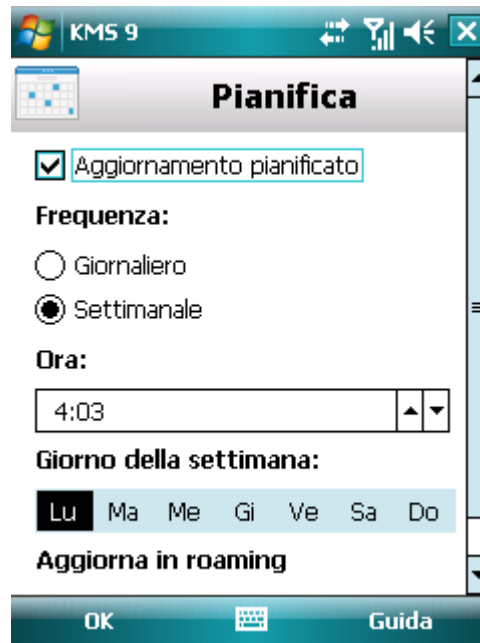


Figura 50: Impostazioni di aggiornamento automatico

6. Premere **OK** per salvare le modifiche.

AGGIORNAMENTO IN ROAMING

Quando il dispositivo si trova in una zona roaming, è possibile abilitare o disabilitare gli aggiornamenti pianificati dei database anti-virus. Se l'aggiornamento in roaming è bloccato, l'aggiornamento manuale è accessibile in modalità standard.

- *Per consentire gli aggiornamenti pianificati dei database anti-virus quando il dispositivo si trova in una zona roaming, eseguire le seguenti operazioni:*

1. Selezionare **Menu** → **Anti-Virus**.

Verrà aperta la finestra **Anti-Virus**.

2. Selezionare l'opzione **Aggiornamento**.

Verrà aperta la finestra **Aggiornamento**.

3. Selezionare l'opzione **Pianifica aggiornamento**.

Verrà aperta la finestra **Pianifica**.

- Nella sezione **Aggiorna in roaming**, selezionare la casella **Aggiorna in roaming**.

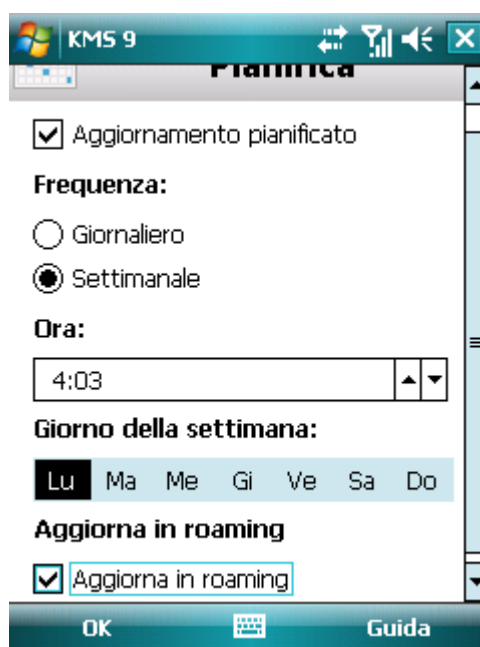


Figura 51: Configurazione degli aggiornamenti in roaming

- Premere **OK** per salvare le modifiche.

REPORT DELL'APPLICAZIONE

Questa sezione fornisce informazioni sui report in cui viene registrato il funzionamento di ogni componente e l'esecuzione di ogni attività (ad esempio, gli aggiornamenti del database dell'applicazione e le scansioni anti-virus).

IN QUESTA SEZIONE

Informazioni sui report.....	112
Visualizzazione dei record del report	112
Eliminazione dei record del report.....	113

INFORMAZIONI SUI REPORT

Nei report dell'applicazione vengono memorizzati i record relativi agli eventi che si verificano durante il funzionamento di Kaspersky Mobile Security 9. Le voci vengono ordinate in base all'ora dell'evento e a partire dagli eventi più recenti.

Per ogni modulo viene utilizzato un report eventi distinto.

VISUALIZZAZIONE DEI RECORD DEL REPORT

► *Per visualizzare tutti i record memorizzati nel report:*

1. Selezionare **Menu** → **Avanzate**.

Verrà aperta la finestra **Avanzate**.

2. Selezionare l'opzione **Report**.

Verrà aperta la finestra **Report**.

3. Selezionare il componente del quale si desidera visualizzare il report eventi.

Verrà aperto il report eventi del componente selezionato.

► *Per visualizzare informazioni dettagliate sui record del report:*

Selezionare il record desiderato e premere **Dettagli**.

Nella schermata **Dettagli** sono visualizzate informazioni sulle azioni dell'applicazione, con i relativi dettagli. Ad esempio, per l'azione "Oggetto trasferito in Quarantena", viene visualizzato anche il percorso del file infetto nel dispositivo.

► *Per tornare ai report,*

Selezionare **Menu** → **Indietro**.

ELIMINAZIONE DI RECORD DEL REPORT

È possibile svuotare tutti i report. Le informazioni sul funzionamento di tutti i componenti di Kaspersky Mobile Security 9 verranno eliminate.

➔ Per cancellare tutti i report:

1. Selezionare **Menu** → **Avanzate**.

Verrà aperta la finestra **Avanzate**.

2. Selezionare l'opzione **Report**.

Verrà aperta la finestra **Report**.

3. Aprire il report di un qualunque componente.

4. Selezionare **Menu** → **Elimina tutto** (vedere la figura seguente).

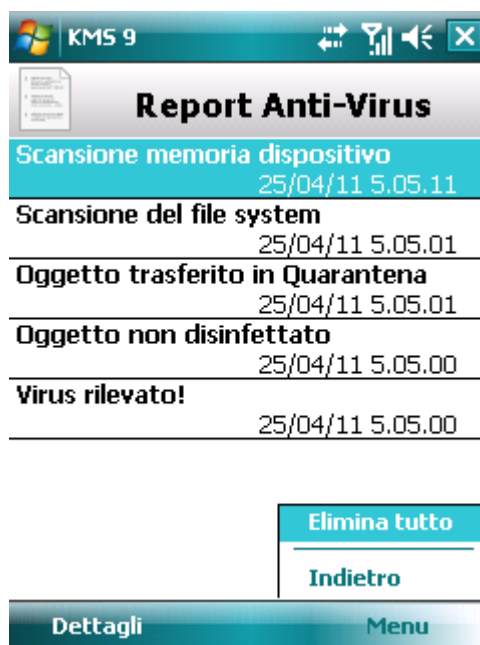


Figura 52: Eliminazione dei record

5. Confermare la cancellazione dei report premendo il pulsante **Sì**.

Verranno eliminati tutti i record in tutti i report dei componenti.

CONFIGURAZIONE DI IMPOSTAZIONI AGGIUNTIVE

Questa sezione fornisce informazioni sulle opzioni aggiuntive di Kaspersky Mobile Security 9: come gestire le notifiche acustiche dell'applicazione e come abilitare/disabilitare la visualizzazione dei suggerimenti.

IN QUESTA SEZIONE

Modifica della password segreta	114
Visualizzazione dei suggerimenti	114
Configurazione delle notifiche acustiche	115

MODIFICA DELLA PASSWORD SEGRETA

È possibile modificare la password segreta dell'applicazione impostata dopo l'attivazione.

► *Per modificare la password segreta:*

1. Selezionare **Menu** → **Avanzate**.
Verrà aperta la finestra **Avanzate**.
2. Selezionare l'opzione **Impostazioni**.
Verrà aperta la finestra **Impostazioni**.
3. Selezionare **Modifica del codice**.
4. Immettere la password corrente nel campo di immissione **Immetti password**.
5. Immettere la nuova password nei campi **Immettere nuova password** e **Conferma password**, quindi premere **OK** per salvare le modifiche.

VISUALIZZAZIONE DEI SUGGERIMENTI

Quando si configurano le impostazioni dei componenti, Kaspersky Mobile Security 9 visualizza un messaggio predefinito con una descrizione sintetica della funzione selezionata. È possibile configurare la visualizzazione dei suggerimenti di Kaspersky Mobile Security 9.

► *Per configurare la visualizzazione dei suggerimenti:*

1. Selezionare **Menu** → **Avanzate**.
Verrà aperta la finestra **Avanzate**.
2. Selezionare l'opzione **Impostazioni**.
Verrà aperta la finestra **Impostazioni**.
3. Selezionare l'opzione **Suggerimenti**.
Verrà aperta la finestra **Suggerimenti**.
4. Selezionare uno dei valori suggeriti per l'impostazione **Suggerimenti**:
 - **Mostra**: visualizza i suggerimenti prima di configurare le impostazioni della funzione selezionata.
 - **Nascondi**: non visualizza i suggerimenti.
5. Premere **OK**.

CONFIGURAZIONE DELLE NOTIFICHE ACUSTICHE

In seguito al funzionamento dell'applicazione, si verificano eventi specifici: ad esempio, è stato rilevato un oggetto infetto o un virus, il periodo di validità della licenza sta per scadere, ecc. Per specificare all'applicazione di informare l'utente di ogni evento del genere, è possibile abilitare l'emissione di notifiche acustiche al verificarsi degli eventi.

Per impostazione predefinita, Kaspersky Mobile Security 9 emette le notifiche acustiche solo in base alla modalità impostata sul dispositivo.

Per modificare i valori delle impostazioni, utilizzare i pulsanti di spostamento o la penna stilo del dispositivo.

► *Per gestire l'emissione di notifiche acustiche dell'applicazione, eseguire le seguenti operazioni:*

1. Selezionare **Menu** → **Avanzate**.

Verrà aperta la finestra **Avanzate**.

2. Selezionare l'opzione **Impostazioni**.

Verrà aperta la finestra **Impostazioni**.

3. Selezionare l'opzione **Segnale acustico**.

Verrà aperta la finestra **Segnale acustico**.

4. Selezionare uno dei valori suggeriti per l'impostazione **Notifiche acustiche** (vedere la figura seguente):

- **Abilita**: emette notifiche acustiche indipendentemente dal profilo del dispositivo selezionato.
- **Disabilita**: non emette notifiche acustiche.

5. Premere **OK** per salvare le modifiche.

COME CONTATTARE IL SERVIZIO DI ASSISTENZA TECNICA

Dopo l'acquisto di Kaspersky Internet Security, è possibile ottenere informazioni sull'applicazione tramite il Servizio di assistenza tecnica per telefono o via Internet.

Gli esperti del Servizio di assistenza tecnica risponderanno a tutte le domande relative all'installazione e all'utilizzo dell'applicazione. Gli esperti sono disponibili ad assistere l'utente nel processo di eliminazione delle conseguenze dannose delle attività del malware, nel caso in cui il dispositivo sia stato infettato.

Prima di contattare il Servizio di assistenza tecnica, leggere le regole sull'assistenza per i prodotti Kaspersky Lab (<http://support.kaspersky.com/it/support/rules>).

Invio di domande al Servizio di assistenza tecnica via e-mail

È possibile inviare le proprie domande agli specialisti del servizio di Assistenza tecnica compilando il modulo Web Helpdesk all'indirizzo <http://support.kaspersky.com/helpdesk.html?LANG=it>.

È possibile scrivere le proprie domande in russo, inglese, tedesco, francese, italiano o spagnolo.

Per poter inviare un messaggio e-mail contenente la domanda, è necessario includere l'**ID cliente** e la **password** ricevuti al momento della registrazione sul sito Web del Servizio di assistenza tecnica.

Se non si è ancora utenti registrati delle applicazioni Kaspersky Lab, è possibile compilare un modulo di registrazione (<https://my.kaspersky.com/it>). Durante la registrazione, immettere il *codice di attivazione* dell'applicazione o il *file chiave*.

Il servizio di Assistenza tecnica risponderà alle richieste nell'area Assistenza personalizzata (<https://my.kaspersky.com/it>) e all'indirizzo e-mail specificato dall'utente nella propria richiesta.

Nella richiesta, descrivere il problema riscontrato. Specificare quanto segue nei campi obbligatori:

- **Tipo di richiesta.** Selezionare l'argomento corrispondente più da vicino al problema riscontrato, ad esempio "Problema di installazione/disinstallazione prodotto" o "Problema di scansione anti-virus/rimozione virus". Se non è disponibile un argomento appropriato, selezionare "Domanda generale".
- **Nome dell'applicazione e numero della versione.**
- **Testo della richiesta.** Descrivere il problema riscontrato fornendo quanti più dettagli possibile.
- **ID cliente e password.** Immettere l'ID cliente e la password ricevuti al momento della registrazione sul sito Web del Servizio di assistenza tecnica.
- **Indirizzo e-mail.** Il Servizio di assistenza tecnica risponderà alla domanda a questo indirizzo e-mail.

Assistenza tecnica per telefono

Per problemi urgenti, è possibile contattare il Servizio di assistenza tecnica locale. Prima di contattare il servizio di Assistenza tecnica locale (http://support.kaspersky.com/support/support_local) o internazionale (<http://support.kaspersky.com/support/international>), raccogliere le informazioni necessarie (<http://support.kaspersky.com/support/details>) sul proprio dispositivo e sull'applicazione anti-virus installata. Ciò consentirà ai nostri esperti di assistere l'utente più rapidamente.

GLOSSARIO

A

AGGIORNAMENTO DEI DATABASE

Una delle funzioni eseguite dall'applicazione Kaspersky Lab per mantenere aggiornata la protezione. I database anti-virus vengono copiati nel dispositivo dai server degli aggiornamenti di Kaspersky Lab e l'applicazione viene connessa automaticamente a tali database.

ARCHIVIO

File "contenente" uno o più oggetti che possono essere a loro volta archivi.

ATTIVAZIONE DELL'APPLICAZIONE

Passaggio dell'applicazione alla modalità completamente operativa. L'utente deve disporre di una licenza per attivare l'applicazione.

B

BLOCCO DI UN OGGETTO

Bloccare dell'accesso a un oggetto da parte di applicazioni esterne. Un oggetto bloccato non può essere letto, eseguito, modificato o eliminato.

D

DATABASE ANTI-VIRUS

Database creati dagli esperti di Kaspersky Lab, contenenti descrizioni dettagliate di tutte le minacce note per la sicurezza dei computer e i relativi metodi di rilevamento e disinfezione. Questi database vengono costantemente aggiornati da Kaspersky Lab man mano che vengono identificate nuove minacce.

DISINFEZIONE DI OGGETTI

Metodo utilizzato per elaborare oggetti infetti, che determina il ripristino completo o parziale dei dati o la determinazione che non è possibile disinfettarli. La disinfezione degli oggetti viene eseguita in base al database dell'applicazione. Una parte dei dati validi di un file potrebbe andare persa durante il processo di disinfezione.

E

ELIMINAZIONE DEI MESSAGGI SMS

Metodo di elaborazione di un messaggio SMS contenente caratteristiche SPAM tali da comportarne la cancellazione. È consigliabile applicare questo metodo ai messaggi SMS che contengono inequivocabilmente spam.

ELIMINAZIONE DI UN OGGETTO

Metodo di elaborazione degli oggetti che comporta la loro eliminazione fisica dalle posizioni originali. Si consiglia di applicare questo metodo di elaborazione a qualunque oggetto dannoso che non può essere disinfettato.

L

LISTA BLOCCATI

Le voci in questo elenco contengono le seguenti informazioni:

Numero di telefono da cui Filtro chiamate/SMS blocca le chiamate e/o gli SMS.

Tipi di eventi bloccati da Filtro chiamate/SMS per il numero. Sono disponibili i seguenti tipi di eventi: Chiamate e SMS, Solo chiamate e Solo SMS.

Frase chiave utilizzata da Filtro chiamate/SMS per classificare un SMS come indesiderato (spam). Filtro chiamate/SMS blocca solo gli SMS che contengono la frase chiave, mentre consente tutti gli altri SMS.

LISTA CONSENTITI

Le voci in questo elenco contengono le seguenti informazioni:

Numero di telefono da cui Filtro chiamate/SMS consente le chiamate e/o gli SMS.

Tipi di eventi consentiti da Filtro chiamate/SMS per il numero. Sono disponibili i seguenti tipi di eventi: Chiamate e SMS, Solo chiamate e Solo SMS.

Frase chiave utilizzata da Filtro chiamate/SMS per classificare un SMS come desiderato (non spam). Filtro chiamate/SMS consente solo gli SMS che contengono la frase chiave, mentre blocca tutti gli altri SMS.

M

MASCHERA FILE

Rappresentazione del nome e dell'estensione di un file che utilizza i caratteri jolly. I due caratteri jolly principali utilizzati nelle maschere file sono "*" e "?", dove "*" rappresenta un numero qualsiasi di caratteri e "?" qualsiasi carattere singolo. Utilizzando questi caratteri jolly, è possibile rappresentare qualsiasi file. Notare che il nome e l'estensione del file sono sempre separati da un punto.

MITTENTE NON NUMERICO

Numero di telefono che include o è composto unicamente da lettere.

O

OGGETTO INFETTO

Oggetto contenente codice dannoso. L'applicazione rileva gli oggetti infetti eseguendo la scansione del codice binario interno e individua che una sezione del codice dell'oggetto è identica a quella del codice di una minaccia nota. Gli esperti di Kaspersky Lab sconsigliano l'utilizzo di questi oggetti in quanto possono infettare il dispositivo.

P

PASSWORD SEGRETA DELL'APPLICAZIONE

La password segreta impedisce l'accesso non autorizzato alle impostazioni dell'applicazione e alle informazioni bloccate nel dispositivo. L'utente la imposta al primo avvio dell'applicazione ed è composta da almeno quattro caratteri. La password segreta viene richiesta nei seguenti casi:

per l'accesso alle impostazioni dell'applicazione;

per l'accesso alle cartelle crittate;

durante l'invio di un comando SMS da un altro dispositivo mobile per attivare le seguenti funzioni in remoto: SMS-Block, SMS-Clean, SIM Watch, SMS-Find e Protezione privacy;

in caso di disinstallazione dell'applicazione.

PERIODO DELLA LICENZA.

Periodo di tempo durante il quale l'utente può utilizzare tutte le funzioni dell'applicazione Kaspersky Lab. Alla scadenza della licenza, l'applicazione passa in modalità con funzionalità limitate. In questa modalità, è possibile eseguire le seguenti operazioni:

disabilitazione di tutti i componenti;
criptaggio di una o più cartelle;
disabilitazione dell'occultamento dei dati personali;
blocco dell'occultamento automatico delle informazioni riservate;
visualizzazione della Guida in linea dell'applicazione.

Q

QUARANTENA

Cartella progettata per memorizzare tutti gli oggetti potenzialmente infetti rilevati dalle scansioni del dispositivo o tramite l'elaborazione da parte del componente Protezione.

R

RIPRISTINO DI UN OGGETTO

Spostamento di un oggetto dalla Quarantena nella cartella originale (in cui era contenuto prima di essere spostato in quarantena, disinfettato o eliminato) o in un'altra cartella definita dall'utente.

S

SCANSIONI MANUALI

Modalità di funzionamento dell'applicazione Kaspersky Lab avviata dall'utente e destinata alla scansione di qualsiasi file.

T

TRASFERIMENTO DI OGGETTI IN QUARANTENA

Metodo utilizzato per elaborare un oggetto potenzialmente infetto, che blocca l'accesso a tale oggetto e lo sposta dalla posizione originale alla cartella Quarantena. Nella Quarantena l'oggetto viene memorizzato in forma criptata, il che impedisce l'infezione del dispositivo.

KASPERSKY LAB

Fondata nel 1997, Kaspersky Lab rappresenta oggi una delle aziende leader nello sviluppo di una vasta gamma di prodotti software a elevate prestazioni destinati alla protezione delle informazioni, tra cui sistemi anti-virus, anti-spam e anti-hacking.

Kaspersky Lab è un'azienda internazionale, con sede centrale nella Federazione Russa e uffici nel Regno Unito, Francia, Germania, Giappone, Benelux, Cina, Polonia, Romania e USA (California). Recentemente è stato aperto in Francia un nuovo ufficio, l'European Anti-Virus Research Centre. La rete di partner di Kaspersky Lab comprende oltre 500 aziende in tutto il mondo.

Attualmente Kaspersky Lab conta oltre mille dipendenti specialisti altamente qualificati, tra cui 10 laureati in economia aziendale e 16 con titolo di PhD. Tutti gli esperti anti-virus Kaspersky Lab senior sono membri dell'organizzazione CARO (Computer Anti-Virus Researchers Organization).

Kaspersky Lab offre soluzioni di protezione all'avanguardia, grazie alla notevole competenza e alla significativa esperienza maturata in più di 14 anni di attività di sviluppo di soluzioni anti-virus. Un'analisi approfondita delle attività dei virus informatici consente agli specialisti dell'azienda di anticipare le tendenze nello sviluppo di malware e di offrire agli utenti una protezione efficace e tempestiva contro i nuovi tipi di attacchi. Questo vantaggio è alla base dei prodotti e dei servizi offerti da Kaspersky Lab. I prodotti dell'azienda sono sempre un passo avanti rispetto a quelli della concorrenza nell'ambito della protezione anti-virus, sia per gli utenti home che per i clienti aziendali.

Anni di lavoro intenso hanno reso l'azienda una dei principali sviluppatori di software anti-virus. Kaspersky Lab è stata la prima azienda a sviluppare numerosi standard moderni per la difesa dai virus. Il prodotto di punta, Kaspersky Anti-Virus, protegge in modo efficace tutti i tipi di sistemi dagli attacchi dei virus, incluse le workstation, i file server, i sistemi di posta, i firewall, i gateway Internet e i computer palmari. I clienti di Kaspersky Lab possono usufruire di una vasta gamma di servizi aggiuntivi che garantiscono il funzionamento costante dei prodotti e una compatibilità completa con i propri requisiti specifici. Numerosi sviluppatori in tutto il mondo utilizzano il kernel di Kaspersky Anti-Virus® nei propri prodotti, tra cui: Nokia ICG (Stati Uniti), Aladdin (Israele), Sybari (Stati Uniti), G Data (Germania), Deerfield (Stati Uniti), Alt-N (Stati Uniti), Microworld (India) e BorderWare (Canada).

I clienti di Kaspersky Lab possono contare su un'ampia gamma di servizi aggiuntivi che assicurano sia la stabilità operativa dei prodotti dell'azienda che la conformità con requisiti specifici aziendali. L'azienda progetta, installa e supporta sistemi anti-virus aziendali. Il database anti-virus di Kaspersky Lab viene aggiornato ogni ora. L'azienda fornisce ai propri clienti un servizio di assistenza tecnica 24 ore su 24, in varie lingue.

Per domande, commenti o suggerimenti, è possibile contattarci tramite i nostri rivenditori oppure rivolgersi direttamente a Kaspersky Lab. È possibile ottenere informazioni dettagliate telefonicamente o tramite posta elettronica. Riceverete risposte complete a tutte le vostre domande.

Sito Web di Kaspersky Lab <http://www.kaspersky.it/>

Enciclopedia dei virus: <http://www.securelist.com/>

Laboratorio anti-virus: newvirus@kaspersky.com
(solo per l'invio di oggetti sospetti agli archivi)
<http://support.kaspersky.com/virlab/helpdesk.html>
(per porre domande agli analisi virus)

Forum Web di Kaspersky Lab: <http://forum.kaspersky.com>

INFORMAZIONI SUL CODICE DI TERZE PARTI

Per la creazione dell'applicazione è stato utilizzato codice di terze parti.

IN QUESTA SEZIONE

Codice del programma distribuito.....	121
Altre informazioni	123

CODICE DEL PROGRAMMA DISTRIBUITO

All'interno dell'applicazione viene distribuito codice di programma di terze parti, in formato sorgente o binario, senza alcuna modifica.

IN QUESTA SEZIONE

ADB.....	121
ADBWINAPI.DLL	121
ADBWINUSBAPI.DLL	121

ADB

ADB

Copyright (C) 2005-2008, The Android Open Source Project

Distributed under the terms of the Apache License, version 2.0 of the License

ADBWINAPI.DLL

ADBWINAPI.DLL

Copyright (C) 2005-2008, The Android Open Source Project

Distributed under the terms of the Apache License, version 2.0 of the License

ADBWINUSBAPI.DLL

ADBWINUSBAPI.DLL

Copyright (C) 2005-2008, The Android Open Source Project

 Apache License

Version 2.0, January 2004

<http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION**1. Definitions.**

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution

incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

ALTRE INFORMAZIONI

Ulteriori informazioni sul codice di terze parti.

Per verificare le firme digitali, Kaspersky Mobile Security utilizza la libreria di software per la sicurezza dei dati Crypto C di CryptoEx LLC.

Sito Web di CryptoEx LLC: <http://www.cryptoex.ru>

INDICE

A

Abilitazione	
Criptaggio	102
Filtro chiamate/SMS	58
Firewall	99
Parental Control	69, 70
Protezione privacy	90
Aggiornamento	
avvio manuale	108
avvio pianificato	109
AGGIORNAMENTO	
VERSIONE DELL'APPLICAZIONE	22
Aggiunta	
elenco di numeri riservati di Protezione privacy	95
Lista bloccati di Filtro chiamate/SMS	59
Lista bloccati di Parental Control	71
Lista consentiti di Filtro chiamate/SMS	62
Lista consentiti di Parental Control	74
Antifurto	77
SIM Watch	83
SMS-Block	78
SMS-Clean	80
SMS-Find	84
Archivi	
Scansioni manuali	50, 51
Attivazione dell'applicazione	24
licenza	32
Avvio	
Aggiornamento	108
applicazione	30
Scansioni manuali	48
Azioni	
Scansioni manuali	52
Azioni da eseguire nei confronti degli oggetti	45, 52

B

Blocco	
chiamate in entrata	59, 62
chiamate in uscita	70, 71
connessioni di rete	99
criptaggio delle informazioni	105
messaggi SMS in uscita	70, 71
SMS in entrata	59
Blocco dell'accesso ai dati criptati	105

C

Consenti	
chiamate in entrata	62
chiamate in uscita	73
connessioni di rete	99
messaggi SMS in uscita	73
SMS in entrata	62
Contratto di licenza	32
Criptaggio	
blocco automatico dell'accesso	105

criptaggio dei dati	102
decriptaggio dei dati	104
D	
Dati	
accesso alla password segreta.....	105
Criptaggio	102
Decriptaggio	104
DATI	
INFORMAZIONI RISERVATE	89
Disabilitazione	
Criptaggio	104
Filtro chiamate/SMS	58
Firewall	99
Parental Control.....	69, 70
Protezione privacy	89, 90
DISINSTALLAZIONE	
APPLICAZIONE	20
E	
Eliminazione	
elenco di contatti riservati di Protezione privacy	96
Lista bloccati di Filtro chiamate/SMS	61
Lista bloccati di Parental Control	73
Lista consentiti di Filtro chiamate/SMS	64
Lista consentiti di Parental Control	75
oggetto dalla quarantena	55
Record del report.....	113
F	
FILTRO	
CHIAMATE IN ENTRATA	57
SMS IN ENTRATA	57
Filtro chiamate/SMS	57
azione per gli SMS	67
azione per le chiamate	67
Lista bloccati.....	59
Lista consentiti	62
mittenti non numerici	66
modalità.....	58
numeri non inclusi nei contatti	65
I	
INSTALLAZIONE DELL'APPLICAZIONE.....	20
INTERFACCIA DELL'APPLICAZIONE.....	39
Invia comando SMS	87
L	
Licenza.....	32
attivazione dell'applicazione	24
Contratto di licenza	32
informazioni	33
rinnovo.....	34
Lista bloccati	
Filtro chiamate/SMS	59
Parental Control.....	70
Lista consentiti	
Filtro chiamate/SMS	62
Parental Control.....	73
Livello di sicurezza	
Firewall	99

M

Menu dell'applicazione41

Modalità

- Filtro chiamate/SMS58
- Parental Control.....69
- Protezione privacy89, 90

Modifica

- elenco di contatti riservati di Protezione privacy95
- Lista bloccati di Filtro chiamate/SMS60
- Lista bloccati di Parental Control72
- Lista consentiti di Filtro chiamate/SMS63
- Lista consentiti di Parental Control75

P

Parental Control

- Lista bloccati.....70
- Lista consentiti.....73
- modalità.....69

Password

- codice di attivazione24, 25, 27
- password segreta dell'applicazione28

Password segreta dell'applicazione28, 29

Pianificazione

- Aggiornamento109
- Scansioni manuali49

Protezione privacy.....89

- avvio automatico.....91
- elenco di contatti riservati94
- modalità.....89
- selezione delle informazioni e degli eventi da nascondere97

Q

Quarantena

- eliminazione di un oggetto55
- ripristino di un oggetto55
- visualizzazione di oggetti54

QUARANTENA54

R

Report eventi.....112

- eliminazione di voci113
- visualizzazione delle voci.....112

Rinnovo della licenza34

Ripristino di un oggetto.....55

S

Scansioni manuali

- archivi51
- avvio48
- avvio pianificato49
- Azioni da eseguire sugli oggetti52
- oggetti da sottoporre a scansione.....50

Stato di protezione.39

V

Visualizzazione

- Finestra Stato della protezione39

Voce

- Lista bloccati di Filtro chiamate/SMS59

Lista consentiti di Filtro chiamate/SMS	62
Lista consentiti di Parental Control	74