Dr.WEB®

Security Space

per Android

Defend what you create

Manuale dell'utente

Dr.Web Security Space per Android
Versione 10.01.0
Manuale dell'utente
29.10.2015

Doctor Web, Sede centrale in Russia
125124
Russia, Mosca,
via 3 Yamskogo Polya, tenuta 2, edificio 12A

Sito web: www.drweb.com
Telefono: +7 (495) 789-45-87

Le informazioni sulle sedi rappresentative si trovano sul sito ufficiale dell’azienda.

Doctor Web

"Doctor Web" è uno sviluppatore russo di sistemi di sicurezza informatica.

"Doctor Web" offre valide soluzioni di protezione antivirus e antispam per enti pubblici, aziende e utenti privati.

I programmi antivirali della famiglia Dr.Web vengono sviluppati a partire dal 1992, sempre raggiungono i migliori risultati nel rilevamento di malware e corrispondono agli standard internazionali di sicurezza.

I certificati e premi conferiti ai prodotti Dr.Web provano il loro avanzato grado di affidabilità. Gli utenti di Dr.Web si trovano in diverse parti del mondo.

Ringraziamo i nostri utenti per la fiducia che hanno nelle soluzioni della famiglia Dr.Web!

Sommario

Capitolo 1. Introduzione

Grazie per aver scelto **Dr.Web Security Space per Android** (di seguito - **Dr.Web**). Questo prodotto antivirus protegge in un modo sicuro i dispositivi mobili gestiti dal sistema operativo Android™, nonché le TV, i lettori multimediali e le console di gioco che funzionano sulla piattaforma Android TV™ contro varie minacce di virus create appositamente per infettare questi dispositivi.

Questo programma utilizza le tecnologie più recenti di **Doctor Web** per rilevare e neutralizzare oggetti malevoli che potrebbero costituire una minaccia per l'operatività del dispositivo e per la sua sicurezza informatica.

Dr.Web utilizza Origins Tracing™ for Android che è una tecnologia unica di rilevamento ideata per la piattaforma Android. Questa tecnologia consente di individuare nuove famiglie di virus conoscendo i virus precedenti. Origins Tracing for Android è in grado di riconoscere virus ricompilati, quali Android.SMSSend, Android.MobileSpy e applicazioni infettate da Android.ADRD, Android.Geinimi, Android.DreamExploid. I nomi delle minacce rilevate da Origins Tracing for Android hanno la forma Android.VirusName.origin.

Questo manuale ha lo scopo di aiutare gli utenti dei dispositivi mobili SO Android a installare e configurare **Dr.Web**, nonché a conoscere le sue funzioni principali.

Segni convenzionali e abbreviazioni

Questo manuale utilizza le seguenti segnalazioni:

Segno	Commento
Parole in grassetto	Nomi degli elementi dell'interfaccia grafica ed esempi dell'input che deve essere eseguito esattamente come è scritto nel manuale.
Parole in verde e in grassetto	Denominazioni dei prodotti e dei componenti di **Doctor Web**.
Parole in verde sottolineate	Riferimenti incrociati a capitoli del documento o collegamenti ipertestuali alle risorse interne.
Parole in corsivo	Termini e testo sostituito (riportato invece delle informazioni che devono essere inserite dall'utente). In caso di esempi dell'input a riga di comando, parole in corsivo indicano i valori dei parametri.
MAIUSCOLO	Nomi dei tasti della tastiera.
	Avviso di eventuali situazioni di errori, nonché dei momenti importanti, a cui particolarmente prestare attenzione.

Caratteristiche principali dell'applicazione

Dr.Web è una soluzione sicura per la protezione antivirus dei dispositivi gestiti dal sistema operativo Android. L'applicazione esegue le seguenti funzioni:

- protegge continuamente in tempo reale il file system del dispositivo (controlla file che vengono salvati, programmi che vengono installati ecc.);
- esegue la scansione di ogni file nel file system oppure di singoli file e cartelle a richiesta dell'utente;
- esegue la scansione di archivi;
- esegue la scansione della scheda di memoria;
- rileva file di esecuzione automatica Windows;
- rileva minacce in file *.lnk (definite da **Dr.Web** come Exploit.Cpllnk);

- elimina le minacce rilevate oppure le mette in quarantena;
- sblocca il dispositivo bloccato dai programmi ransomware;
- filtra chiamate ed SMS in arrivo sulla base delle black list e white list predefinite e create dall'utente;
- aggiorna i database dei virus **Dr.Web** attraverso la connessione a Internet;
- registra informazioni statistiche delle minacce rilevate e delle azioni del programma e il log di eventi;
- cerca e blocca urgentemente il dispositivo se è stato smarrito o rubato;
- protegge da siti web indesiderati in caso di utilizzo del browser integrato Android, di Google Chrome, Google Chrome Beta, Next, Amazon Silk, Yandex.Browser, Boat Browser e Boat Browser Mini;
- controllo e accorciamento di URL;
- permette di rilevare e di eliminare problemi della sicurezza e vulnerabilità del dispositivo;
- controllo delle connessioni Internet, protezione del dispositivo dall'accesso non autorizzato dall'esterno e prevenzione della perdita di dati importanti attraverso la rete.

Alcune delle funzioni elencate non sono disponibili nell'applicazione installata sui dispositivi che funzionano sulla piattaforma Android TV. Per saperne di più consultare la sezione "Utilizzo di Dr.Web su Android TV".

L'interfaccia grafica del programma consente di configurare tutti i parametri del programma tenendo conto delle esigenze dell'utente e di impostare il livello ottimale di protezione del dispositivo.

Inoltre, **Dr.Web** supporta la modalità Multi-Window che permette di avviare più applicazioni in finestre separate. Il funzionamento in questa modalità è possibile soltanto sui dispositivi Samsung Galaxy S III e superiore, Samsung Galaxy Note 2 e superiore.

Requisiti di sistema

Per l'installazione e per il funzionamento di **Dr.Web** occorre che il dispositivo mobile sia gestito dal sistema operativo Android versione 4.0/4.1/4.2/4.3/4.4/5.0/5.1. **Dr.Web** anche funziona sulle TV, sui lettori multimediali e sulle console di gioco sulla piattaforma Android TV.

Per scaricare gli aggiornamenti dei database dei virus, occorre la connessione Internet. Se si usa un tablet, per il funzionamento del filtraggio di messaggi e dell'**Antifurto Dr.Web**, si deve avere la possibilità di installare e utilizzare una SIM card.

Sui dispositivi con i firmware personalizzati o con i permessi di root (i cosiddetti dispositivi "rooted") il funzionamento corretto di **Dr.Web** non è garantito.Il supporto tecnico non è previsto per tali dispositivi.

Di default, l'applicazione si installa nella memoria interna del dispositivo. Per il corretto funzionamento di **Dr.Web** e, in particolare, della funzione **Antifurto Dr.Web**, non è opportuno trasferire l'applicazione installata su supporti esterni.

Capitolo 2. Concessione di licenze

Per il funzionamento di **Dr.Web** occorre una licenza. La licenza consente di utilizzare a pieno tutte le possibilità del prodotto durante l'intero periodo di validità e regola i diritti dell'utente stabiliti in conformità con il contratto con l'utente.

Se prima di acquistare una licenza si vuole provare il prodotto, si può attivare un periodo di prova. Assicura le complete funzioni dei principali componenti però il periodo di validità è notevolmente limitato.

Se si possiede una licenza valida dei prodotti software **Dr.Web Security Space**, **Dr.Web Desktop Security Suite** oppure di qualsiasi prodotto boxed **Dr.Web**, si può utilizzare la licenza disponibile per il funzionamento di **Dr.Web**.

Se si compra su Google Play e si installa la versione dell'applicazione con la licenza perpetua (**Dr.Web Security Space Life**), la procedura di ottenimento e di registrazione della licenza viene eseguita in maniera automatica.

Se è attivata la modalità di protezione centralizzata, la licenza viene scaricata automaticamente dal server di protezione centralizzata.

È possibile attivare una licenza o un periodo di prova e anche passare all'acquisto della licenza sulla schermata corrispondente (v. Immagini 1a e 1b) che si apre dopo il primo avvio del programma e anche se nessuna licenza valida è rintracciabile.

Per aprire la schermata per l'ottenimento di una licenza:

1. Selezionare la voce **Dr.Web** dal menu dell'applicazione o, se il dispositivo funziona sulla piattaforma Android TV, passare nella sezione **Dr.Web** sulla schermata principale dell'applicazione.
2. Premere sul pulsante **Rinnova la licenza**.

Immagini 1a e 1b. Concessione di licenze

File della chiave di licenza

I diritti dell'utente sull'uso di **Dr.Web** sono conservati in un apposito file, chiamato il *file della chiave di licenza*.

Il file della chiave ha l'estensione *.key e contiene, in particolare, le seguenti informazioni:

- periodo per il quale è permesso utilizzare il prodotto;
- lista dei componenti disponibili all'utente;
- altre limitazioni.

Il file della chiave è *valido* a seguenti condizioni:

- il periodo di validità della licenza non è scaduto;
- la licenza copre tutti i moduli utilizzati dall'applicazione;
- l'integrità della chiave non è violata.

A violazione di qualsiasi condizione il file della chiave diventa *non valido* e l'antivirus cessa di neutralizzare programmi dannosi.

La modifica del file della chiave lo rende non valido. Perciò non è opportuno aprirlo in editor di testo per evitare danni accidentali al file.

Attivazione del periodo di prova

Se si è installato il programma per conoscerne le funzioni, si può attivare un periodo di prova per 14 giorni.

La procedura dell'attivazione del periodo di prova è diversa a seconda del modo attraverso cui **Dr.Web** è stato installato sul dispositivo.

Se l'applicazione è stata installata da Google Play:

1. Sulla schermata di ottenimento della licenza (v. Immagine 1b) selezionare la voce **Ottieni demo**. Il periodo di prova verrà attivato per l'indirizzo e-mail dell'account Google, visualizzato nella sezione **Ottieni demo**. Se si hanno diversi account Google, verrà selezionato il primo di essi.
2. Se non si ha un account Google, si apre una finestra per l'inserimento di un indirizzo e-mail per cui verrà attivato il periodo di prova. Immettere un indirizzo e-mail valido e premere il pulsante **Ottieni demo**. Il periodo di prova verrà attivato.

Se l'applicazione è stata installata dal sito della società Doctor Web:

1. Sulla schermata di ottenimento della licenza (v. Immagine 1a) selezionare la voce **Ottieni demo**.
2. Si apre una finestra per l'inserimento di un indirizzo e-mail per cui verrà attivato il periodo di prova. Immettere un indirizzo e-mail valido.
3. Premere sul pulsante **Ottieni demo**. Il periodo di prova verrà attivato.

Acquisto della licenza

La procedura dell'acquisto della licenza è diversa a seconda del modo attraverso cui **Dr.Web** è stato installato sul dispositivo.

> L'acquisto di una licenza non è disponibile attraverso l'applicazione installata sui dispositivi che funzionano sulla piattaforma Android TV. È possibile acquistare una licenza direttamente in Google Play o nel negozio online di Doctor Web.

Se l'applicazione è stata installata da Google Play:

1. Sulla schermata per l'ottenimento della licenza (v. Immagine 1b) premere **Compra/Scarica**.
2. Se non si ha un account Google, è necessario specificare un indirizzo e-mail valido per registrare la licenza. Questo consentirà successivamente di attivare la licenza se l'applicazione viene reinstallata o viene installata su un altro dispositivo. Immettere un indirizzo e-mail valido e premere il pulsante **Ottieni licenza**.
3. Nella finestra **Acquisto della licenza** si può scegliere una delle varianti della licenza:
   - **Licenza di 1 anno**, **Licenza di 2 anni** o **Licenza di 1 anno senza supporto tecnico**. Dopo che è stata selezionata qualsiasi delle varianti elencate, si apre la finestra standard di acquisto del programma. Qualche tempo dopo aver fatto il pagamento, la licenza si attiverà automaticamente. Se a causa di eventuali errori tecnici avvenuti durante l'acquisto il download non è cominciato, si prega di rivolgersi all'assistenza tecnica della società **Doctor Web**.
   - **Licenza di durata illimitata**. Se è stata scelta la licenza con un periodo di validità illimitato, si apre la finestra di acquisto e installazione **Dr.Web Security Space Life** su Google Play. Se **Dr.Web** si usava in precedenza, è necessario eliminarlo. Premere su **OK** per confermare l'eliminazione. Per conservare le impostazioni del programma che in seguito si vogliono applicare a **Dr.Web Security Space Life**, usare la funzione di esportazione delle impostazioni prima dell'eliminazione del programma.

Se sul dispositivo è abilitata la funzione **Antifurto Dr.Web**, prima di eliminare **Dr.Web**, nelle impostazioni del dispositivo mobile è necessario togliere il flag **Dr.Web Security Space** che si trova nella scheda **Sicurezza** sezione **Amministratori dispositivo** (i nomi delle impostazioni potrebbero variare in diversi modelli di dispositivo e versioni del sistema operativo), in seguito a cui l'**Antifurto Dr.Web** bloccherà il dispositivo. Immettere la password impostata per l'**Antifurto Dr.Web** per procedere con l'eliminazione del programma.

La licenza si attiverà automaticamente.

Se l'applicazione è stata installata dal sito della società Doctor Web:

1. Selezionare l'opzione **Compra** sulla schermata di ottenimento della licenza (v. Immagine 1a) o aprire nel browser la pagina http://estore.drweb.com/mobile. Si apre una pagina del negozio online **Doctor Web**.
2. Scegliere la durata della licenza e il numero di dispositivi da proteggere.
3. Premere sul pulsante **Compra**.

Dopo che è stato fatto l'ordine, il numero di serie o il file della chiave di licenza viene spedito sull'indirizzo e-mail specificato. Inoltre, si può scegliere di ricevere il numero di serie in un SMS inviato al numero di cellulare specificato. In seguito è necessario registrare il numero di serie oppure copiare il file della chiave sul dispositivo mobile.

Attivazione della licenza

Se Lei possiede già una licenza valida dei prodotti Dr.Web Security Space, **Dr.Web Desktop Security Suite** oppure di qualsiasi prodotto **Dr.Web** in scatola, Lei può registrare e utilizzare la Sua licenza nei seguenti modi che dipendono dal modo in cui **Dr.Web** è stato installato sul dispositivo:

Se l'applicazione è stata installata da Google Play:

- Se in precedenza si è già attivata una licenza o un periodo di prova, sulla schermata per l'ottenimento della licenza (v. Immagine 1b) premere **Compra/Scarica**. Se necessari, immettere l'indirizzo e-mail che si già usava in precedenza per ottenere/registrare il file della chiave. La licenza registrata in relazione a questo indirizzo e-mail verrà scaricata dal server e installata in maniera automatica.
- Se si ha un numero di serie, si può registrarlo:
  1. Sulla schermata per l'ottenimento della licenza (v. Immagine 1b) premere **Inserisci numero di serie**.

Un numero di serie ottenuto per attivare un periodo di prova di uno dei prodotti **Dr.Web** per postazioni, non può essere utilizzato per la versione di **Dr.Web** installata da Google Play. In questo caso è necessario prima attivare il periodo di prova del prodotto **Dr.Web** su un PC, dopodiché verrà ottenuto un file della chiave di licenza corrispondente. È quindi possibile copiarlo sul dispositivo. Le istruzioni su come utilizzare su dispositivo il file della chiave di licenza ottenuto verranno spedite tramite e-mail nel processo dell'attivazione del periodo di prova.

  2. Immettere il numero di serie disponibile e premere il pulsante **Ottieni licenza**.

Se l'applicazione è stata installata dal sito della società Doctor Web:

Sono disponibili i modi di attivazione riportati di seguito.

Registrare il numero di serie

1. Sulla schermata per l'ottenimento della licenza (v. Immagine 1a) selezionare la variante **Attiva la licenza**.
2. Premere la voce **Inserisci numero di serie**.
3. Immettere il numero di serie.

4. Se si registra questo numero di serie per la prima volta, si apre una schermata di inserimento di informazioni personali necessarie per attivare la licenza. Compilare tutti i campi.
5. Premere sul pulsante **Ottieni licenza**.

Copiatura del file della chiave sul dispositivo

1. Copiare il file della chiave nella cartella **Android/data/com.drweb/files** che si trova sulla scheda SD.
2. Sulla schermata di ottenimento della licenza (v. Immagine 1a) selezionare la voce **Attiva la licenza**.
3. Premere la voce **Scarica**. Nella finestra di informazioni **Copia da file** premere su **OK**.
4. Il file della chiave verrà installato e sarà pronto all'uso. Si apre una finestra che mostra le informazioni sulla durata della licenza. Premere su **OK**.

Il file della chiave dei programmi **Dr.Web Security Space** o **Dr.Web Desktop Security Suite** può essere utilizzato per **Dr.Web** se esso supporta il componente DrWebGUI.

Per controllare se è possibile utilizzare il file della chiave:

1. Aprire il file della chiave in un editor di testo (per esempio, in Blocco note).
2. Controllare se il componente DrWebGUI è presente nella lista dei valori del parametro Applications dal gruppo [Key]: se questo componente è presente nella lista, il file della chiave può essere utilizzato per **Dr.Web**.

Il file della chiave ha un formato che lo protegge da modifiche. La modifica del file della chiave lo rende non valido. Per evitare il suo danneggiamento, si consiglia di non salvare il file della chiave alla chiusura dell'editor di testo.

Ottenimento del file della chiave con la registrazione del numero di serie sul sito Doctor Web

1. Entrare sul sito di cui l'indirizzo è indicato nella scheda di registrazione allegata al prodotto.
2. Immettere il numero di serie di registrazione ottenuto tramite l'acquisto di **Dr.Web**.
3. Compilare il modulo con le informazioni su acquirente.
4. Il file della chiave verrà spedito sull'indirizzo e-mail indicato sotto forma di un archivio ZIP contenente un file con l'estensione *.key.
5. Estrarre il file della chiave sul computer da cui è possibile copiarlo sul dispositivo.

Rinnovo della licenza

In alcuni casi, per esempio alla scadenza della licenza, potrebbe essere necessario sostituire il file della chiave di licenza già esistente e registrato nel sistema. **Dr.Web** supporta l'aggiornamento del file della chiave "a volo", perciò non è richiesto di reinstallarlo o di interrompere il funzionamento di **Dr.Web**.

Informazioni sulla licenza

Per leggere le informazioni sulla licenza in uso:

- **su Android**. Quando si trova sulla schermata principale (v. Immagine 2), richiamare il menu dell'applicazione e selezionare la voce **Dr.Web**.
- **su Android TV**. Quando si trova sulla schermata principale (v. Immagine 20), richiamare il menu dell'applicazione e selezionare la voce **Dr.Web**.

Sulla schermata che si è aperta si possono leggere le seguenti informazioni sulla licenza:

- nome del titolare della licenza;
- data di registrazione e data di scadenza della licenza.

Configurazione delle notifiche

Si possono attivare/disattivare le notifiche di prossima scadenza della licenza tramite l'opzione **Notifiche** che si trova nella sezione **Licenza** delle impostazioni dell'**Dr.Web** (v. Immagine 6).

Aggiornamento della licenza

Per rinnovare la licenza, è necessario acquistare ed attivare una nuova licenza.

Inoltre, l'utente può acquistare una licenza nuova o rinnovare la licenza corrente sulla sua pagina personale sul sito web ufficiale di **Doctor Web**. Per passare a questa pagina web, selezionare la voce **Dr.Web** nel menu dell'applicazione ed utilizzare il link **Mio Dr.Web**.

Capitolo 3. Installazione e rimozione

Dr.Web può essere acquistato e installato direttamente da Google Play, oppure si può copiare e avviare sul dispositivo mobile il file di installazione del programma. Inoltre per installare l'applicazione, è possibile utilizzare il programma di sincronizzazione con il PC.

L'applicazione può essere eliminata tramite Google Play oppure con gli strumenti del sistema operativo del dispositivo.

Installazione dell'applicazione

Dr.Web può essere installato tramite Google Play, nonché avviando il file di installazione sul dispositivo o utilizzando il programma di sincronizzazione con il PC.

Installazione del programma tramite Google Play

1. Aprire Google Play sul dispositivo, trovare nella lista delle applicazioni **Dr.Web** e premere il pulsante **Installa** o **Compra** (se viene scelta la versione dell'applicazione con la licenza illimitata **Dr.Web Security Space Life**).

   Se **Dr.Web** non viene visualizzato in Google Play, il dispositivo mobile non soddisfa i requisiti di sistema minimi.

2. Se è stata scelta la versione **Dr.Web Security Space Life**, per continuare l'installazione è necessario effettuare il pagamento.
3. In seguito si apre una schermata con le informazioni sulle funzioni del dispositivo l'accesso alle quali è richiesto per il funzionamento dell'applicazione:
   - se si installa **Dr.Web** per utilizzarlo durante il periodo di prova gratuito (14 giorni), per poter acquistare una licenza dopo questo periodo sarà necessario l'accesso alla funzione di acquisto all'interno dell'applicazione;
   - per registrare l'applicazione e per attivare la licenza, è necessario l'accesso a Internet e all'elenco degli account Google sul dispositivo;
   - per il funzionamento di **SpIDer Guard** e dello **Scanner Dr.Web** occorre l'accesso ai dati delle applicazioni e alla scheda di memoria, nonché la possibilità di lettura e di scrittura di dati;
   - per filtrare chiamate e SMS, l'applicazione deve avere accesso alle funzioni di ricezione e di invio di SMS e di chiamate, nonché la possibilità di leggere la rubrica e il registro chiamate e SMS e la possibilità di modificare la modalità di segnali (per disattivare il suono se la chiamata viene bloccata);
   - per il funzionamento dell'**Antifurto Dr.Web**, è necessario l'accesso alla funzione di invio di SMS (affinché l'**Antifurto Dr.Web** possa mandare SMS in caso di cambio della SIM card e anche SMS in risposta ai comandi inviati dall'utente), di ottenimento delle coordinate del dispositivo, di gestione di GPS e di Wi-Fi, nonché è richiesta la possibilità di eliminare dal dispositivo tutte le informazioni personali dell'utente (se l'applicazione ha ricevuto il comando opportuno dall'utente);
   - per il funzionamento del filtro URL **Cloud Checker**, è necessario l'accesso alla cronologia e ai segnalibri dei browser supportati;
   - per utilizzare una finestra mobile con le informazioni sul traffico dati corrente, occorre consentire la visualizzazione di elementi interfaccia sopra le altre finestre;
   - per l'aggiornamento dei database virali, è necessario l'accesso a Internet e alle impostazioni di rete del dispositivo.

   Premere sul pulsante **Salva**.

4. Per iniziare a usare l'applicazione, premere il pulsante **Apri**.

Per installare l'applicazione non utilizzando Google Play, è necessario consentire questo tipo di installazione. Per farlo, aprire la schermata **Impostazioni** -> **Applicazioni** e spuntare il flag **Origini sconosciute**. Il file d'installazione di **Dr.Web** può essere scaricato dal sito **Doctor Web** sull'indirizzo http://download.drweb.com/android.

Avvio del file d'installazione sul dispositivo

1. Copiare il file di installazione sulla scheda di memoria.
2. Utilizzando il file manager trovare ed eseguire il file d'installazione.
3. Nella finestra che si è aperta premere il pulsante **Installa**.
4. In seguito si apre una schermata con le informazioni sulle funzioni del dispositivo l'accesso alle quali è richiesto per il funzionamento dell'applicazione. Premere il pulsante **Accetta**.

Installazione tramite il programma di sincronizzazione del dispositivo mobile con un computer (per esempio, HTC Sync™ ecc.)

1. Sincronizzare il dispositivo mobile con il computer.
2. Avviare la procedura guidata di installazione programmi che fa parte del pacchetto del programma di sincronizzazione.
3. Indicare il percorso in cui il file d'installazione è memorizzato sul computer e quindi seguire le istruzioni dell'installazione guidata.
4. L'applicazione verrà trasferita sul dispositivo mobile e si potrà leggere le informazioni relative ad essa e confermare l'installazione. Chiudere la procedura guidata di installazione del programma di sincronizzazione.
5. Chiudere l'installazione guidata del programma di sincronizzazione.

Dr.Web è stato installato ed è pronto all'uso. Per continuare ad usare l'applicazione, è necessario attivare una licenza o un periodo di prova (ad eccezione della versione **Dr.Web Security Space Life**).

Eliminazione e aggiornamento dell'applicazione

Si può aggiornare l'applicazione fino alla versione successiva oppure rimuovere l'applicazione dal dispositivo mobile tramite Google Play. L'applicazione può essere rimossa inoltre utilizzando le funzioni del sistema operativo senza collegamento a Internet.

Se sul dispositivo è abilitata la funzione **Antifurto Dr.Web**, prima di eliminare l'applicazione, nelle impostazioni del dispositivo mobile è necessario togliere il flag **Dr.Web Security Space** che si trova nella scheda **Sicurezza** sezione **Amministratori dispositivo** (i nomi delle impostazioni potrebbero variare in diversi modelli di dispositivo e versioni del sistema operativo).

Eliminazione e aggiornamento dell'applicazione tramite Google Play

1. Aprire Google Play e selezionare la voce **Le mie app**.
2. Nell'elenco delle applicazioni installate sul dispositivo selezionare **Dr.Web**.

Se **Dr.Web** è stato installato in un modo diverso dall'installazione tramite Google Play, potrebbe non essere visualizzato nella sezione **Le mie app**. In questo caso si può eliminarlo utilizzando le funzioni del sistema operativo.

3. Sulla schermata con le informazioni su applicazione premere il pulsante **Aggiorna** per installare la nuova versione oppure il pulsante **Elimina** per eliminare l'applicazione.

Il pulsante **Aggiorna** non è disponibile se nessuna nuova versione dell'applicazione è stata rilasciata.

4. Confermare l'aggiornamento/l'eliminazione del programma:
   - In caso di aggiornamento premere il pulsante **Accetta** per consentire l'accesso alle funzioni del dispositivo necessarie per l'applicazione. L'applicazione verrà aggiornata automaticamente. Per iniziare a usare l'applicazione, premere il pulsante **Apri**.
   - In caso di eliminazione dell'applicazione premere il pulsante **OK**. L'applicazione verrà eliminata dal dispositivo.

Eliminazione dell'applicazione senza la connessione Internet

1. Aprire la schermata **Impostazioni** -> **Applicazioni**.
2. Nell'elenco delle applicazioni installate sul dispositivo selezionare **Dr.Web**.
3. Sulla schermata con le informazioni relative al programma premere sul pulsante **Disinstalla**. L'applicazione verrà eliminata dal dispositivo.
4. Portata a termine l'eliminazione, premere sul pulsante **OK** per tornare all'elenco delle applicazioni installate.

La quarantena e il log di eventi programma memorizzato non vengono eliminati per l'impostazione predefinita. Se necessario, essi possono essere eliminati manualmente dalla cartella Android/data/com.drweb/files sulla scheda SD.

Controllare la disponibilità di una nuova versione del programma

Se **Dr.Web** è stato scaricato e installato dal sito di **Doctor Web**, si può impostare una funzione che controlla la disponibilità di una nuova versione del programma a ogni aggiornamento dei database dei virus. Per farlo, spuntare il flag **Nuova versione dell'applicazione** nella configurazione dell'aggiornamento del programma. Quando è uscita una nuova versione del programma, si riceverà una notifica corrispondente e si potrà scaricare e installare presto la nuova versione.

Capitolo 4. Per iniziare

Questa sezione descrive le procedure di avvio e di chiusura di **Dr.Web** e l'interfaccia utente dell'applicazione.

Avvio e arresto dell'applicazione

Avvio dell'applicazione

Per avviare **Dr.Web**:

- **su Android**. Aprire la schermata **Applicazioni** e premere l'icona di **Dr.Web** .
- **su Android TV**. Passare alla sezione **Applicazioni** e selezionare **Dr.Web** nella lista delle applicazioni disponibili.

Al primo avvio, l'applicazione visualizza il Contratto di licenza che Lei deve accettare per continuare a utilizzare l'applicazione. Inoltre, nella stessa finestra Lei può conoscere il programma volto a migliorare la qualità del software e accettare di parteciparci acconsentendo di inviare sui server delle società **Doctor Web** e Google informazioni anonime su minacce rilevate e siti web visitati. Lei può rifiutare di inviare queste informazioni in qualsiasi momento accedendo alle impostazioni dell'applicazione nelle quali è necessario deselezionare il flag **Invio delle statistiche** situato nella sezione **Impostazioni generali**.

Se **Dr.Web** è stato installato tramite l'installer fornito dall'amministratore della rete antivirus aziendale, il Contratto di licenza non verrà aperto.

Per uscire dall'applicazione

Per chiudere l'applicazione, premere sul tasto **Home** del dispositivo.

Per riavviare l'applicazione, si può premere sull'icona **Dr.Web** nella sezione delle applicazioni avviate di recente.

Al primo avvio **Dr.Web** apre la sua schermata principale. All'avvio successivo, si apre l'ultima schermata attiva del programma.

Interfaccia

La schermata principale di **Dr.Web** (v. Immagine 2) contiene le informazioni sullo stato attuale di protezione e consente di impostare le seguenti funzioni del programma:

- **SpIDer Guard** – consente di attivare/disattivare la protezione continua contro virus;
- **Filtraggio chiamate e messaggi** – consente di scegliere la modalità di filtraggio e di guardare elenchi di chiamate e di messaggi bloccati;

Su dispositivi senza il supporto di SIM card, la funzione filtraggio chiamate ed SMS e l'**Antifurto Dr.Web** non sono disponibili, e quindi le sezioni corrispondenti non ci sono sulla schermata principale dell'applicazione. Sui dispositivi che funzionano sulla piattaforma Android TV, inoltre non è disponibile il **Firewall Dr.Web**.

- **Scanner** – esegue la scansione del sistema a richiesta dell'utente (sono possibili 3 tipi di scansione: scansione rapida, completa, personalizzata);

- **Aggiornamento** – contiene le informazioni sulla data dell'ultimo aggiornamento del programma e consente di avviare l'aggiornamento del programma se necessario;
- **Antifurto** – consente di configurare le funzioni dell'**Antifurto Dr.Web**;
- **Cloud Checker** – consente di configurare il filtraggio URL per limitare l'accesso dell'utente a siti web;
- **Firewall** – consente di configurare funzioni del controllo di connessioni Internet e di trasmissione dati attraverso la rete;
- **Auditor di sicurezza** – consente di analizzare il sistema e di rimuovere problemi della sicurezza e vulnerabilità trovati.

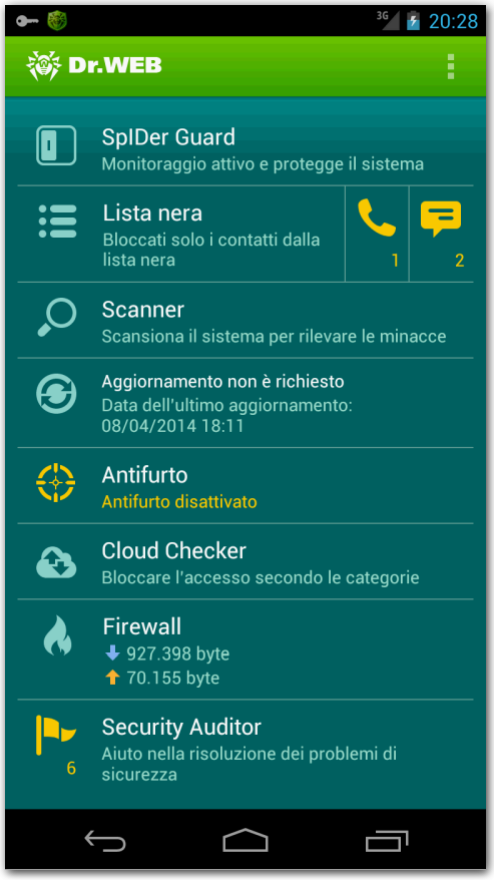


Immagine 2. La schermata principale dell'applicazione

Accesso al menu dell'applicazione e navigazione sulle schermate

Sulle schermate dell'applicazione con le opzioni disponibili, la funzione che consente di richiamare il menu si trova nell'angolo superiore destro della schermata. Per ritornare sulla schermata principale, si usa il pulsante nella forma del logotipo dell'applicazione che si trova nell'angolo superiore sinistro dello schermo.

Il menu chiamato sulla schermata principale consente di configurare l'applicazione, di accedere alla quarantena e alle statistiche di funzionamento, di aprire un manuale sul web che descrive dettagliatamente tutte le impostazioni e funzioni,nonché di aprire una schermata con le informazioni sul programma.

Sulla schermata con le informazioni sul programma, si possono leggere le informazioni sulla versione dell'applicazione, sul titolare della licenza in uso e sulle date dell'attivazione e della scadenza della licenza. Inoltre, su questa schermata sono disponibili i link al sito ufficiale dell'azienda **Doctor Web** e alla pagina personale dell'utente su questo sito, nonché i link alle pagine dell'azienda nei social network Twitter, Facebook, Instagram e sul canale Youtube. Se **Dr.Web** funziona nella modalità di protezione centralizzata del servizio antivirus **Dr.Web AV-Desk**, su questa schermata vengono visualizzate anche la data della scadenza dell'abbonamento al servizio o la data a partire dalla quale l'utilizzo del servizio è stato bloccato per questo dispositivo (postazione).

Sui dispositivi che funzionano sulla piattaforma Android TV, il menu dell'applicazione non è disponibile. Le informazioni circa la versione dell'applicazione, il titolare della licenza in uso e il periodo di validità della stessa sono ritrovabili nella sezione **Dr.Web** sulla schermata principale dell'applicazione.

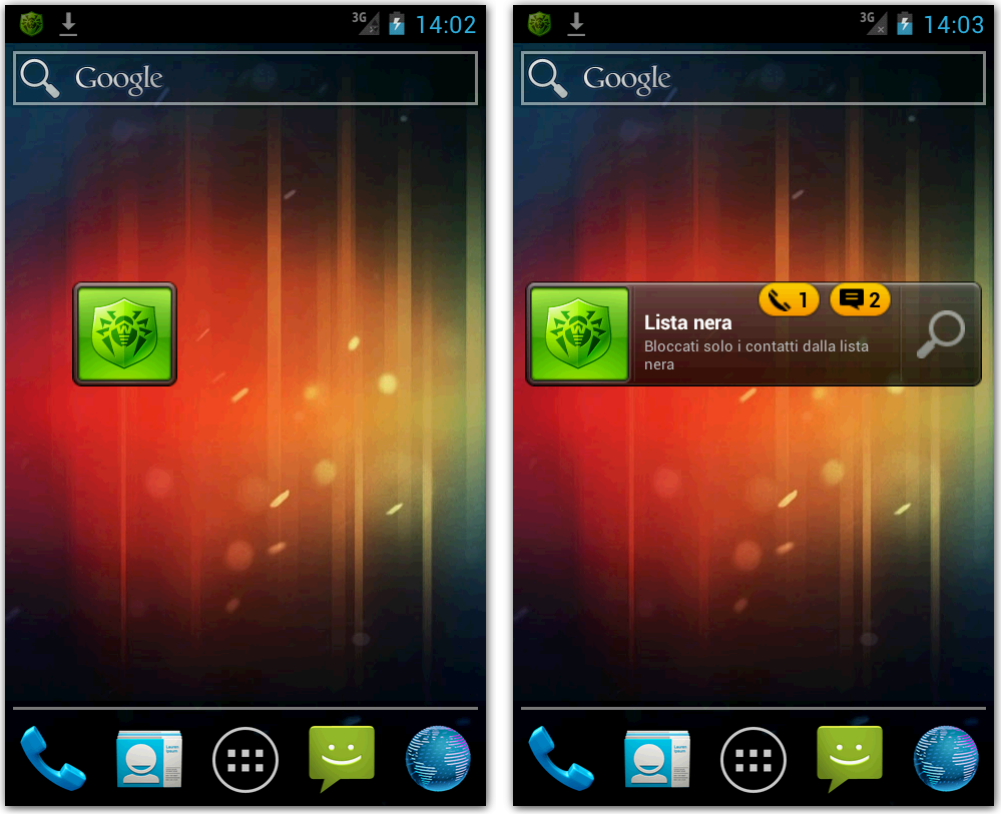
Widgets

Per rendere più comodo l'utilizzo di **Dr.Web**, si possono aggiungere alla **Schermata iniziale** del dispositivo widget speciali che consentono di gestire le funzioni principali del programma.

Sui dispositivi che funzionano sulla piattaforma Android TV, l'aggiunzione dei widget non è disponibile.

Aggiunzione dei widget

1. Un widget dell'applicazione può essere aggiunto tramite il metodo standard del sistema operativo in uso. Aprire la lista dei widget disponibili per l'aggiunzione sul dispositivo.
2. Nella lista dei widget disponibili selezionare uno dei widget di **Dr.Web**:
   - **Dr.Web 1×1 (piccolo)** – mostra lo stato attuale di protezione e consente di attivare/disattivare il monitor **SpIDer Guard** (v. Immagine 3).
   - **Dr.Web 4×1 (medio)** – mostra lo stato attuale di protezione, il profilo corrente di filtraggio, il numero di chiamate e messaggi bloccati, nonché consente di attivare/disattivare il monitor **SpIDer Guard**, di avviare la scansione (v. Immagine 4).



Immagini 3 e 4. Widget Dr.Web

Avvisi

Per un accesso rapido alle funzioni principali di **Dr.Web** si può usare un'apposita barra che si trova nell'area di notifica dello schermo (v. Immagine 5). Questa barra può essere attivata/disattivata tramite l'opzione **Barra delle notifiche** nella sezione **Impostazioni generali** (v. Immagine 6).

Sui dispositivi che funzionano sulla piattaforma Android TV, la barra delle notifiche non è disponibile.

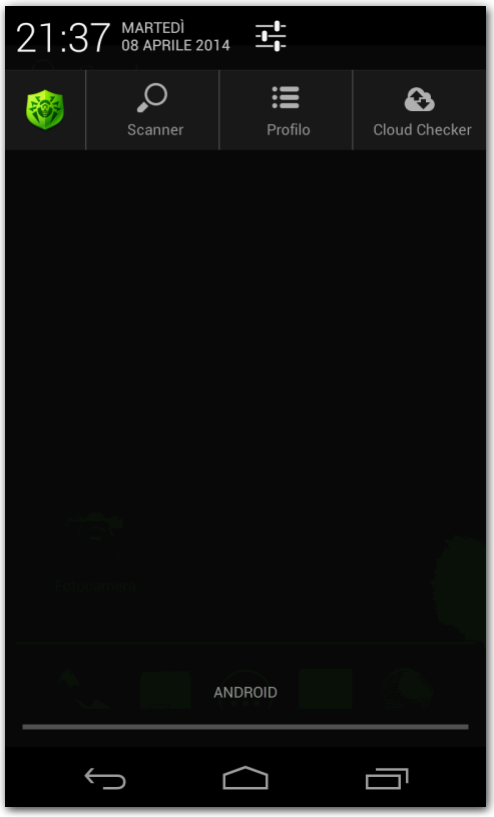


Immagine 5. Barra delle notifiche

Questa barra consente di eseguire le seguenti azioni:

- passare alla schermata di **Dr.Web**. A questo fine, premere sull'icona **Dr.Web**;
- avviare la scansione rapida, completa o personalizzata selezionando l'opzione **Scanner**, quindi il tipo di scansione;
- scegliere un profilo di filtraggio delle chiamate e degli sms nell'impostazione **Profilo**;
- passare alla schermata di configurazione del filtro URL selezionando l'opzione **Cloud Checker**.

Se il dispositivo non supporta l'utilizzo delle SIM card, invece dell'opzione **Profilo**, nella barra delle notifiche sarà presente l'opzione **I download** che consente di avviare una scansione degli oggetti scaricati sul dispositivo.

Se **Dr.Web** funziona nella modalità di protezione centralizzata e l'utente non ha i permessi per modificare le impostazioni di filtraggio di chiamate e di messaggi e/o di **Cloud Checker**, le opzioni **Profilo** e/o **Cloud Checker** saranno non disponibili nella barra delle notifiche.

In caso di rilevamento delle minacce, le corrispondenti icone nella barra degli avvisi cambiano:

- – se le minacce sono state rilevate dallo scanner;
- – se le minacce sono state rilevate dal file monitor **SpIDer Guard**.

Su Android 5.0 e superiori quando viene rilevata una minaccia, la barra delle notifiche sarà aperta fino a quando un'azione non verrà applicata alla minaccia.

Mio Dr.Web

Il servizio online **Mio Dr.Web** è una pagina personale dell'utente sul sito della società **Doctor Web**. Su questa pagina l'utente può consultare le informazioni della licenza (scadenza, numero di serie), rinnovare la licenza, guardare la data e l'ora dell'ultimo aggiornamento dei database virali e il numero di record nei database, nonché può conoscere notizie e offerte speciali, fare domande al servizio di supporto tecnico ed eseguire altre azioni.

Per aprire questa pagina, sulla schermata principale (v. Immagine 2) richiamare il menu dell'applicazione e selezionare la voce **Dr.Web**. Sulla schermata che si è aperta, premere sul **Mio Dr.Web**.

Capitolo 5. Funzioni dell'applicazione

Questa sezione descrive le funzioni principali di **Dr.Web** che consentono di configurare la scansione antivirus, il filtraggio di chiamate e di messaggi, l'**Antifurto Dr.Web**, il filtraggio di URL e di organizzare così la protezione del dispositivo.

Sui dispositivi che funzionano sulla piattaforma Android TV, leimpostazioni dell'applicazione non sono disponibili.

Per passare alla schermata di configurazione dell'applicazione (v. Immagine 6), sulla schermata principale dell'applicazione richiamare il menu dell'applicazione e, quindi scegliere la voce **Impostazioni**.

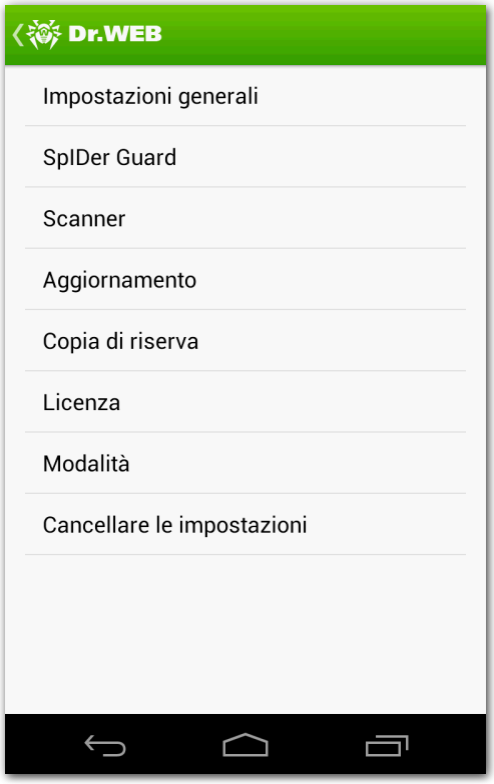


Immagine 6. Impostazioni dell'applicazione

Se è attivato l'Antifurto Dr.Web, se vengono modificate alcune impostazioni dell'applicazione (**Reset delle impostazioni**, **Copia di riserva** e **Modalità**), sarà necessario immettere la password dell'**Antifurto Dr.Web**.

Ripristino delle impostazioni predefinite

È possibile in qualsiasi momento resettare le impostazioni personalizzate dell'applicazione, tra cui quelle di filtraggio di chiamate e di messaggi, di **Antifurto Dr.Web**, **di Firewall Dr.Web** e di **Cloud Checker**, e ripristinare le impostazioni standard. Per farlo, eseguire le seguenti azioni:

1. Sulla schermata delle impostazioni (v. Immagine 6) nella sezione **Reset delle impostazioni** selezionare la voce **Ripristina le impostazioni**.

2. Confermare di voler ritornare alle impostazioni predefinite.

Importazione ed esportazione delle impostazioni

Tutte le impostazioni correnti dell'applicazione possono inoltre essere salvate in un file sulla scheda SD. In seguito se necessario (per esempio, se **Dr.Web** viene reinstallato o viene utilizzato su un altro dispositivo), esse possono essere importate da questo file.

- Per esportare la configurazione attuale del programma in un file, sulla schermata delle impostazioni (v. Immagine 6) nella sezione **Copia di riserva** scegliere **Esportazione delle impostazioni**. Si apre una finestra in cui si deve immettere una password per proteggere il file di configurazione e poi premere su **OK**. Tutte le impostazioni ed informazioni dell'applicazione si memorizzano nel file **Android/data/com.drweb/files/DrWebPro.bkp** sulla scheda SD.
- Per importare le impostazioni dal file, sulla schermata delle impostazioni (v. Immagine 6) nella sezione **Copia di riserva** scegliere **Importazione delle impostazioni**. Confermare di voler importare le impostazioni dal file e immettere la password del file di configurazione. Tutte le impostazioni correnti del programma verranno cancellate e sostituite con le impostazioni importate dal file.

Protezione da virus

La funzione primaria di **Dr.Web** è la scansione continua del file system che si effettua in tempo reale. Inoltre **Dr.Web** esegue la scansione del sistema a richiesta dell'utente. Se si rilevano minacce per la sicurezza, ci vengono applicate le azioni selezionate dall'utente.

Protezione continua da virus

La scansione continua del file system in tempo reale viene eseguita per il tramite del file monitor **SpIDer Guard**. Questo modulo controlla ogni file al tentativo della sua registrazione nella memoria del dispositivo e così difende il sistema da minacce informatiche.

Nella modalità di protezione centralizzata, le impostazioni del componente **SpIDer Guard** potrebbero essere cambiate o bloccate a seconda dei criteri di sicurezza aziendali o della lista dei servizi pagati.

Attivazione della protezione continua

Al primo avvio di **Dr.Web** la protezione continua si lancia automaticamente dopo che l'utente ha accettato il Contratto di licenza. Per disattivarla o per attivarla di nuovo, premere sulla sezione **SpIDer Guard** sulla schermata principale del programma.

Una volta attivato, **SpIDer Guard** comincia a proteggere il sistema. Il monitor continua a funzionare, anche se l'applicazione stessa non è in esecuzione.

Se il file monitor SpIDer Guard rileva minacce per la sicurezza, nella parte superiore dello schermo compare l'icona  (per Android 5.0 e superiori - ) e l'avviso di minacce trovate. Sul pannello delle notifiche è possibile visualizzare le informazioni sul numero di minacce trovate e aprire l'elenco delle minacce per applicarci le azioni di neutralizzazione.

SpIDer Guard viene terminato se la memoria del dispositivo viene ripulita completamente tramite il Task manager incorporato. In questo caso, per ripristinare la protezione continua, sarà necessario riaprire **Dr.Web**.

Impostazioni di SpIDer Guard

Per accedere alle impostazioni di **Dr.Web**, sulla schermata principale dell'applicazione richiamare il menu dell'applicazione e selezionare la voce **Impostazioni**. Per configurare **SpIDer Guard**, sulla schermata delle impostazioni (v. Immagine 6) eseguire le seguenti azioni:

- per attivare il controllo di file compressi in archivi, spuntare il flag **File in archivi** nella sezione **SpIDer Guard**;

Di default archivi non vengono controllati. L'attivazione del controllo di archivi potrebbe rallentare le prestazioni del sistema e aumentare il consumo della batteria. La disattivazione del controllo di archivi non influisce sul livello di difesa perché **SpIDer Guard** controlla comunque file di installazione *.apk, a prescindere dal valore impostato per il parametro **File in archivi**.

- per attivare il controllo della scheda SD ogni volta quando essa si connette al dispositivo, spuntare il flag **Connessione della scheda SD** nella sezione **SpIDer Guard;**
- per attivare/disattivare il controllo del sistema alla ricerca di adware e riskware (compresi hacktool e joke), selezionare la voce **Avanzate** nella sezione **SpIDer Guard** e spuntare/rimuovere i flag rispettivi **Adware** e **Riskware**;
- per controllare se sulla scheda SD sono presenti file di esecuzione automatica Windows, spuntare il flag **File di esecuzione automatica** nella sezione **Impostazioni generali**. Quest'impostazione si userà anche nella scansione a richiesta dell'utente;
- per attivare la visualizzazione dell'icona dell'applicazione  (per Android 5.0 e superiori - ) nella barra di stato all'accensione del monitor, spuntare il flag **Icona Dr.Web** nella sezione **Impostazioni generali**.

Statistiche

Il programma registra eventi relativi al funzionamento di **SpIDer Guard** (attivazione/disattivazione, risultati di scansione della scheda SD e delle applicazioni che si installano, rilevamento di minacce). Le azioni dell'applicazione e, in particolare, di **SpIDer Guard** vengono visualizzate nella sezione **Azioni** nella scheda **Statistiche**, ordinate per data.

Scansione a richiesta dell'utente

La scansione del sistema a richiesta dell'utente viene eseguita tramite il componente **Scanner Dr.Web**. Consente di eseguire una scansione rapida o completa del file system e anche di controllare singoli file e cartelle.

Si consiglia di utilizzare periodicamente la funzione di scansione di file system se **SpIDer Gate** è stato inattivo per qualche tempo. Di solito in questo caso è sufficiente eseguire una scansione rapida del sistema.

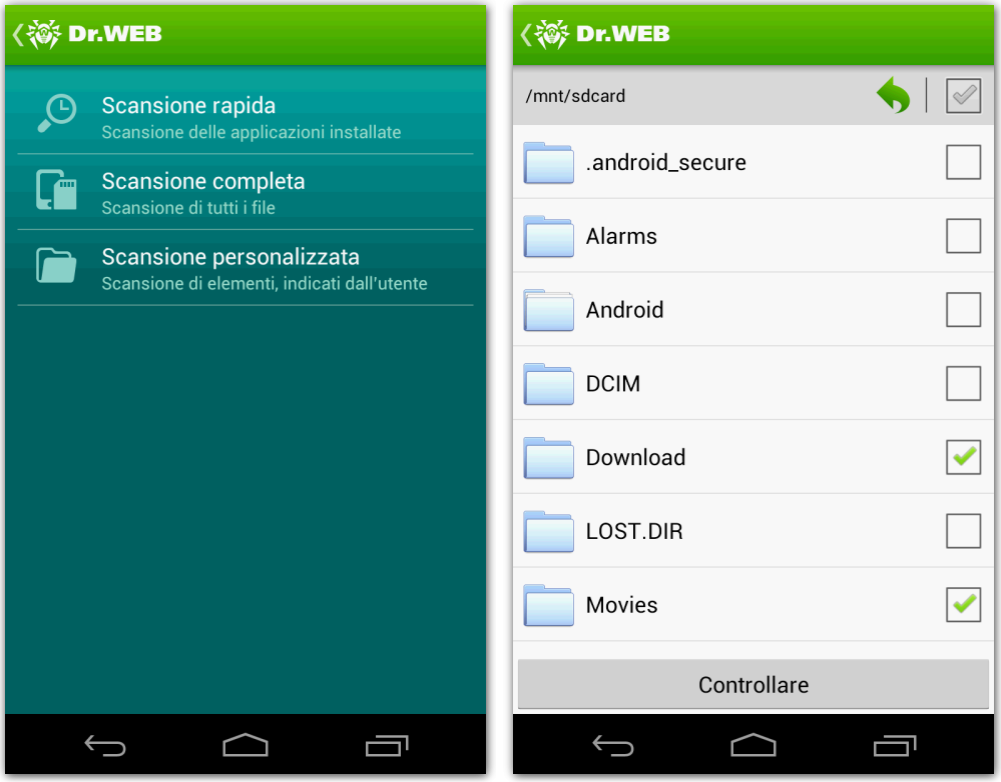
Nella modalità di protezione centralizzata, le impostazioni di Scannerpotrebbero essere cambiate o bloccate a seconda dei criteri di sicurezza aziendali o della lista dei servizi pagati. La scansione può essere avviata secondo un calendario impostato sul server di protezione centralizzata.

Scansione

Per eseguire la scansione del sistema, sulla schermata principale selezionare la voce **Scanner** e nella finestra che si è aperta (v. Immagine 7) effettuare una delle seguenti azioni:

- per avviare la scansione di sole applicazioni installate, scegliere la voce **Scansione rapida**;
- per avviare la scansione di tutti i file del sistema, scegliere la voce **Scansione completa**;
- per controllare singoli file e cartelle, scegliere la voce **Scansione personalizzata**, poi selezionare nella lista degli oggetti del file system gli oggetti che si vogliono controllare (v. Immagine 8) e premere sul pulsante **Controlla**. Selezionando oggetti nella lista, si possono usare le opzioni locate sopra la lista a destra che consentono di evidenziare tutti gli oggetti nella lista o di salire di un livello per cercare tra le cartelle.

Portata a termine la scansione, sullo schermo vengono visualizzate le minacce rilevate e vengono proposte le azioni per neutralizzarle.



Immagini 7 e 8. Scanner e la finestra dove vengono selezionati oggetti da scansionare

Invio dei file sospetti al laboratorio di Doctor Web

È possibile inviare al laboratorio **Doctor Web** inattendibili Archivi ZIP (compresi file con l'estensione *.jar e *.apk), che presumibilmente contengono virus, o archivi ZIP evidentemente puliti che provocano il cosiddetto "falso positivo":

1. Premere e tenere premuto il file nella lista degli oggetti del file system (v. Immagine 8), quindi premere su **Invia al laboratorio**.
2. Sulla schermata successiva immettere un indirizzo e-mail se si desidera ricevere i risultati di analisi dopo che il file inviato è stato analizzato.
3. Scegliere una delle categorie di richiesta:
   - **Probabile virus**, se si ritiene che il file sia una minaccia;

- **Falso positivo** o **Falso positivo da parte di Origins Tracing**, se si ritiene che il file sia stato classificato erroneamente come minaccia.

In caso di falso positivo la categoria di richiesta si sceglie secondo il nome della presunta minaccia: se il nome contiene il postfisso ".origin", si deve scegliere la categoria **Falso positivo da parte di Origins Tracing**, altrimenti la categoria giusta è **Falso positivo**.

4. Premere sul pulsante **Invia**.

Al laboratorio **Doctor Web** è possibile inviare archivi ZIP di cui la dimensione non superi i 10 MB.

Impostazioni dello Scanner Dr.Web

Per accedere alle impostazioni dello **Scanner Dr.Web**, sulla schermata principale invocare il menu dell'applicazione, selezionare la voce **Impostazioni**. Sono disponibili le seguenti impostazioni:

- per attivare il controllo di file compressi in archivi, spuntare il flag **File in archivi** nella sezione **Scanner**;

Di default archivi non vengono controllati. L'attivazione del controllo di archivi potrebbe rallentare le prestazioni del sistema e aumentare il consumo della batteria. La disattivazione del controllo di archivi non influisce sul livello di difesa perché **SpIDer Guard** controlla comunque file di installazione *.apk, a prescindere dal valore impostato per il parametro **File in archivi**.

- affinché durante la scansione su dispositivi a più nuclei, i percorsi a file da controllare si mostrino separatamente per ciascun nucleo, spuntare il flag **Indicazione per nucleo nella sezione Scanner**;
- per attivare/disattivare il controllo del sistema alla ricerca di adware e riskware (compresi hacktool e joke), selezionare la voce **Avanzate** nella sezione **Scanner** e spuntare/rimuovere i flag rispettivi **Adware** e **Riskware**;
- per controllare se sulla scheda SD sono presenti file di esecuzione automatica Windows, spuntare il flag **File di esecuzione automatica** nella sezione **Impostazioni generali**.

Statistiche

L'applicazione registra gli eventi relativi al funzionamento dello scanner (tipo e risultati di scansione, rilevamento di minacce alla sicurezza). Le azioni dell'applicazione e, in particolare, di SpIDer Guard vengono visualizzate nella sezione **Azioni** nella scheda **Statistiche**, ordinate per data.

Neutralizzazione di minacce

Visualizzazione della lista delle minacce

Se il componente **SpIDer Guard** rileva minacce alla sicurezza, nella barra di stato nella parte superiore dello schermo appare l'icona di avviso  (in caso di Android 5.0 e superiori - ) e un messaggio su minacce trovate. Sul pannello delle notifiche è possibile visualizzare le informazioni sul numero di minacce trovate e aprire l'elenco delle minacce per applicarci le azioni di neutralizzazione.

Su Android 5.0 e superiori quando viene rilevata una minaccia, la barra delle notifiche verrà visualizzata sopra tutte le applicazioni fino a quando un'azione non verrà applicata alla minaccia o l'avviso di minaccia non verrà spostato dalla barra delle notifiche. Inoltre, su Android 5.0 e superiori l'avviso di minaccia anche compare sulla schermata di blocco del dispositivo, da cui si può passare alla lista delle minacce rilevate.

Quando il dispositivo viene controllato dallo Scanner Dr.Web, l'elenco delle minacce rilevate si apre automaticamente dopo la fine della scansione. Si può chiudere la lista delle minacce solo dopo aver applicato un'azione a ciascuna delle minacce.

Per ciascuna minaccia, l'elenco contiene le seguenti informazioni:

- nome della minaccia;
- percorso al file che comprende la minaccia.

Accanto alle minacce che non sono virus tra parentesi viene indicato il tipo: adware, riskware, joke o hacktool.

Applicare le azioni alle minacce

Premere una minaccia nella lista e selezionare una delle azioni disponibili:

- **Elimina** – la minaccia viene eliminata completamente dalla memoria del dispositivo;
- **In quarantena** – la minaccia viene messa in una cartella speciale per essere isolata dal resto del sistema;

Se una minaccia è stata rilevata in un'applicazione installata, non è possibile metterla in quarantena. In questo caso l'azione **In quarantena** non è disponibile nella lista delle azioni da applicare.

- **Salta** – nessun'azione viene applicata alla minaccia che rimane così com'è;
- **Segnala falso positivo** – si propone di inviare la minaccia al **Laboratorio antivirale di Doctor Web** informandolo che questa non è una minaccia ed è stata classificata per errore dall'antivirus come un oggetto sospetto. Per ricevere i risultati di analisi del file inviato, inserire un indirizzo e-mail nel campo opportuno e premere sul pulsante **Invia**.

L'azione **Segnala falso positivo** è disponibile solo per le versioni delle minacce con il postfisso ".origin", rilevate nell'area di sistema del dispositivo.

Si possono impostare avvisi sonori per segnalare che una minaccia è stata rilevata, eliminata o messa in quarantena. Per farlo, sulla schermata principale del programma richiamare il menu dell'applicazione e selezionare la voce **Impostazioni**, dopodiché nella sezione **Impostazioni generali** sulla schermata delle impostazioni (v. Immagine 6) spuntare il flag **Suoni**.

Rilevamento di minacce in applicazioni di sistema

Le applicazioni installate nell'area di sistema in alcuni casi potrebbero eseguire le funzioni tipiche di programmi malevoli, perciò nel corso di una scansione del sistema **Dr.Web** potrebbe identificare tali applicazioni come minacce. Se queste applicazioni sono state installate dal produttore del dispositivo, non è possibile applicare ad esse le azioni standard della neutralizzazione di minacce, ma è possibile utilizzare i seguenti suggerimenti:

Se le applicazioni di sistema, identificate come minacce, non sono state installate dal produttore del dispositivo, è possibile applicare ad esse le azioni standard della neutralizzazione di minacce a condizione che sul dispositivo sono disponibili i permessi di root.

- terminare l'applicazione attraverso le impostazioni del dispositivo (sulla schermata **Impostazioni** -> **Applicazioni** nella lista delle applicazioni installate premere sul nome dell'applicazione identificata come minaccia, dopo di che sulla schermata con le informazioni su di essa premere sul pulsante **Termina**);

Sarà necessario eseguire quest'operazione dopo ogni riavvio del dispositivo.

- disattivare l'applicazione attraverso le impostazioni del dispositivo (nella lista delle applicazioni installate sulla schermata **Impostazioni -> Applicazioni** premere il nome dell'applicazione identificata come una minaccia, dopodiché sulla schermata con le informazioni su di essa premere il pulsante **Disattiva**);
- se si utilizza il software ufficiale del produttore del dispositivo mobile, cercare di rivolgersi all'azienda-produttrice per le ulteriori informazioni su quest'applicazione;
- se si usa il software ufficiale del produttore del dispositivo mobile, cercare di contattare il produttore per ricevere ulteriori informazioni su quest'applicazione;
- se sul dispositivo sono disponibili i permessi di root, cercare di eliminare tali applicazioni tramite le apposite utility.

Inoltre, si possono disattivare gli avvisi di rilevamento di minacce nelle applicazioni di sistema conosciute tramite l'opzione **Applicazioni di sistema** nella sezione **Impostazioni generali** -> **Avanzate** sulla schermata delle impostazioni (v. Immagine 6).

Elaborazione dei programmi-locker dei dispositivi

Dr.Web consente di proteggere il dispositivo mobile contro i programmi ransomware per la piattaforma mobile Android che si sono diffusi su larga scala. Questi programmi sono molto pericolosi. Possono cifrare file conservati sui supporti rimovibili dello smartphone o del tablet, bloccare lo schermo del dispositivo mobile e visualizzare su di esso messaggi con la richiesta di pagare il riscatto per la decifratura dei file e per lo sblocco del dispositivo.

Questi programmi possono compromettere fotografie, video e documenti conservati sulle schede rimovibili del dispositivo mobile. Inoltre, rubano e trasmettono sui server dei malintenzionati diverse informazioni sul dispositivo mobile (compreso l'identificatore IMEI), informazioni dalla rubrica (nomi dei contatti, numeri di telefono e indirizzi email), tengono traccia delle chiamate in entrata e in uscita e sono in grado di bloccarle. Tutte le informazioni raccolte, comprese quelle relative alle chiamate, anche vengono trasmesse sul server di controllo.

Dr.Web riconosce ed elimina i programmi-ransomware quando cercano di penetrare sul dispositivo protetto. Tuttavia, il numero e la diversità di tali programmi sono in continuo aumento. Pertanto, un programma-locker potrebbe installarsi sul dispositivo soprattutto se i database dei virus **Dr.Web** non venivano aggiornati per qualche tempo e non includono le informazioni sui nuovi esemplari del malware.

Se il dispositivo mobile è stato bloccato da un programma-ransomware e se il file monitor **SpIDer Guard** è attivato, si può sbloccare il dispositivo attraverso le seguenti azioni:

1. Entro 5 secondi mettere in carica il dispositivo e scollegarlo dalla presa.
2. Entro i successivi 10 secondi collegare le cuffie.
3. Entro i successivi 5 secondi scollegare le cuffie.
4. Entro i successivi 10 secondi agitare vigorosamente il dispositivo.

5. **Dr.Web** termina tutti i processi attivi sul dispositivo, compreso il processo avviato dal programma-locker, dopodiché viene acceso un breve segnale di vibrazione (sui dispositivi che hanno questa funzione). In seguito si apre la schermata di **Dr.Web**.

Notare che con la terminazione dei processi attivi, i dati delle altre applicazioni in esecuzione al momento del blocco del dispositivo potrebbero andare perse.

6. Dopo lo sblocco del dispositivo, si consiglia di aggiornare i database dei virus **Dr.Web** e di eseguire la scansione rapida del sistema o di eliminare l'applicazione malevola.

Filtraggio di chiamate e di messaggi

Dr.Web esegue il filtraggio di messaggi SMS e di chiamate e consente di bloccare messaggi e chiamate indesiderate, per esempio, messaggi pubblicitari indesiderati, nonché chiamate e messaggi che arrivano da numeri sconosciuti.

Nel sistema operativo Android 4.4 e superiori non è garantito il corretto funzionamento del filtraggio dei messaggi SMS.

Sui dispositivi con due SIM card il filtraggio di chiamate e di messaggi potrebbe non funzionare correttamente.

L'applicazione include la possibilità di scegliere la modalità di filtraggio di chiamate e di messaggi. Oltre ai profili predefiniti che determinano la modalità di filtraggio, si possono creare profili personalizzati che contengono impostazioni personalizzati di filtraggio.

Nella modalità di protezione centralizzata, le impostazioni di filtraggio potrebbero essere cambiate o bloccate a seconda dei criteri di sicurezza aziendali o della lista dei servizi pagati.

Per visualizzare le chiamate e i messaggi bloccati, premere la relativa icona sulla schermata principale dell'applicazione.

Scelta della modalità di filtraggio

Il filtraggio di chiamate e messaggi può essere in una delle seguenti modalità:

- **Lascia passare tutto**. In questa modalità il filtraggio è disattivato e si lasciano passare tutte le chiamate ed SMS in arrivo;
- **Blocca tutto**. In questa modalità si bloccano tutte le chiamate ed SMS in arrivo;
- **Rubrica**. Selezionata questa modalità, il filtraggio lascia passare solo le chiamate e i messaggi che arrivano dai numeri telefonici registrati nella rubrica del telefonino;
- **Black list**. Selezionata questa modalità, il filtraggio blocca chiamate ed SMS che arrivano dai numeri telefonici inseriti nella black list.

Inoltre, si può scegliere una modalità di filtraggio personalizzata che si definisce tramite un profilo configurabile. **Dr.Web** permette di creare un numero illimitato di profili, e per ciascun profilo è possibile compilare una lista dei numeri telefonici e definire l'azione (consentire/bloccare) da applicare a chiamate e messaggini che arrivano dai numeri di questa lista.

Se viene selezionata una modalità di filtraggio personalizzata, vengono bloccate anche le chiamate e i messaggi che arrivano dai numeri della black list.

Black list

Nella black list si possono inserire numeri telefonici in modo da bloccare chiamate e messaggi che arrivano da essi. Le chiamate e i messaggi che arrivano dai numeri inseriti nella black list vengono bloccati sia nella modalità **Black list** che nella modalità impostata da qualsiasi profilo personalizzato. In quest'ultimo caso la black list e la lista dei numeri personalizzata sono attive nello stesso tempo.

Le chiamate e gli SMS in arrivo dai numeri aggiunti alla black list possono essere accettati se:

- questi numeri sono inclusi nella lista di un profilo personalizzato e per essi è selezionata l'azione **Consenti solo i contatti dalla lista**;
- è attivata la modalità **Lascia passare tutto**.

Creazione della black list

1. Per creare la black list, premere sulla sezione di filtraggio sulla schermata principale del programma. Compare il menu in cui si può selezionare un profilo, quindi premere su **Configura**.
2. Passare alla scheda **Black list**.
3. Premere su **Aggiungi** per creare la black list. Numeri telefonici e contatti possono essere selezionati nei seguenti modi:
   - dalla rubrica del telefonino;
   - dai registri di chiamate e di messaggi;
   - inserire numeri telefonici e le relative informazioni manualmente.

   Per cercare contatti e numeri nella rubrica e nei registri di chiamate e di messaggi, si può usare la funzione di ricerca disponibile tramite il tasto **Ricerca** del dispositivo. In ciascun caso è possibile scegliere uno o più numeri telefonici da aggiungere alla black list.

   Per inserire nella black list i numeri selezionati, premere sul pulsante **Aggiungi**.
4. Per ciascun numero che è stato aggiunto alla black list si può scegliere una delle seguenti azioni:
   - **Blocca le chiamate e i messaggi** – per bloccare tutte le chiamate e messaggi che arrivano da questo numero;
   - **Blocca solo le chiamate** – per bloccare solo le chiamate in arrivo da questo numero. Nello stesso tempo il filtraggio lascia passare messaggi inviati da questo numero;
   - **Blocca solo i messaggi** – per bloccare solo i messaggi inviati da questo numero. Nello stesso tempo il filtraggio lascia passare chiamate che arrivano da questo numero.

   Di default per ogni numero aggiunto alla black list viene impostata l'azione **Blocca le chiamate e i messaggi**. Se necessario, l'azione può essere cambiata.
5. Per modificare qualche informazione relativa a un contatto inserito nella black list, premere e tenere premuto il contatto o spostarlo a destra o a sinistra. Nel menu che si è aperto, premere su **Modifica**. Modificare i campi **Nome** e **Numero**. Premere su **Salva**.

   La possibilità di modifica non è prevista per contatti aggiunti dalla rubrica del telefonino e per numeri privati.
6. Per eliminare un numero dalla black list, premere e tenere premuto il numero o spostarlo a destra o a sinistra e quindi nel menu che si apre premere su **Elimina**.

7. Inoltre è possibile creare una lista delle parole chiave che verrà utilizzata per bloccare tutti gli SMS che contengono queste parole. Per farlo, nel menu in cui vengono selezionate le opzioni di come aggiungere numeri alla black list, selezionare l'opzione **Parola chiave**. Sulla schermata **Blocco degli SMS per parole chiave** inserire una parola chiave e premere sul pulsante **Aggiungi**.

Svuotamento della black list

Per eliminare tutti i contatti dalla black list, premere sul pulsante menu del dispositivo e selezionare la voce **Cancella la lista**.

Creazione di un profilo di filtraggio

Dr.Web consente di creare profili personalizzati per filtrare chiamate e messaggi.

Creazione di un profilo nuovo

1. Nella lista dei profili disponibili premere su **Configura**.
2. Nella scheda **Profili** premere **Aggiungi profilo**.
3. Impostare il nome del profilo.
4. Selezionare l'azione che deve essere applicata a chiamate e messaggini che arrivano dai numeri telefonici inclusi nell'elenco di questo profilo. Si può selezionare una delle seguenti azioni:
   - **Consenti solo i contatti dalla lista** – per lasciar passare solo le chiamate e i messaggi che arrivano dai numeri inclusi nell'elenco di questo profilo; Le chiamate e gli SMS in arrivo dai numeri inclusi in questa lista verranno accettati anche se questi numeri siano inclusi nella black list.
   - **Proibisci i contatti dalla lista** – per bloccare chiamate e messaggi in arrivo dai numeri inclusi nell'elenco di questo profilo.
5. Premere su **Aggiungi contatto** per creare una lista dei contatti. Numeri telefonici possono essere aggiunti alla lista nei seguenti modi:
   - dalla rubrica del telefonino;
   - dai registri di chiamate e di messaggi;
   - inserire numeri telefonici e le relative informazioni manualmente.

   Per cercare contatti e numeri nella rubrica e nei registri di chiamate e di messaggi, si può usare la funzione di ricerca disponibile tramite il tasto **Ricerca** del dispositivo. In ciascun caso è possibile scegliere uno o più numeri telefonici da aggiungere alla lista del profilo.

   Per inserire i numeri selezionati nella lista del profilo, premere sul pulsante **Aggiungi**. Tra parentesi a destra del nome del profilo viene mostrato quanti contatti vi sono nella lista.

   L'elenco di contatti di un profilo non può essere lasciato vuoto.

6. Per modificare qualche informazione relativa a un contatto inserito nell'elenco, premere e tenere premuto il contatto o spostarlo a destra o a sinistra. Nel menu che si è aperto, premere su **Modifica**. Modificare i campi **Nome** e **Numero**. Premere su **Salva**.

La possibilità di modifica non è prevista per contatti aggiunti dalla rubrica del telefonino e per numeri privati.

7. Per eliminare un numero dall'elenco del profilo, premere e tenere premuto il numero o spostarlo a destra o a sinistra e quindi nel menu che si apre premere su **Elimina**.

Quando contatti si eliminano dall'elenco di un profilo personalizzato di filtraggio, essi non si eliminano dalla rubrica del telefono.

Visualizzazione di chiamate e messaggi bloccati

Sulla schermata principale del programma, nella sezione filtraggio viene mostrato il numero di chiamate e messaggi bloccati. Per vedere chiamate e messaggi bloccati, premere sull'icona rispettiva:

-  – per vedere chiamate bloccate;
-  – per vedere messaggi bloccati.

Tra parentesi a destra del titolo di ciascuna lista viene mostrato il numero di chiamate/messaggi non ancora visti. Per ogni chiamata/messaggio la lista contiene le seguenti informazioni:

- data e ora della chiamata/dell'arrivo del messaggio;
- numero telefonico e nome della persona che ha chiamato/inviato il messaggio.

Affinché le informazioni sulla presenza di chiamate e sms bloccati vengano visualizzate sulla **Schermata iniziale** del dispositivo, aggiungere il widget **Dr.Web 4×1 (medio)**.

Azioni da applicare a chiamate/messaggi bloccati

1. Si può richiamare il numero della chiamata bloccata. Per farlo, premere sulla chiamata nella lista. Si apre una schermata con il numero telefonico digitato. Per effettuare una chiamata a questo numero, premere sul pulsante **Chiama**.
2. Se si preme su un messaggio nell'elenco di messaggi bloccati, si aprono il testo e le informazioni del messaggio. Inoltre è possibile eseguire con il messaggio una delle seguenti azioni:
   - **Ripristina** – per spostare il messaggio nell'elenco di messaggi in entrata del telefono;

     La voce **Ripristina** non è disponibile per il sistema operativo Android 4.4 e superiori.

   - **Elimina** – per eliminare il messaggio.

Aggiornamento

Per rilevare le minacce alla sicurezza, **Dr.Web** utilizza specifici database dei virus che contengono informazioni su tutte le minacce informatiche ai dispositivi SO Android, conosciute dagli specialisti **Doctor Web**. I database devono essere aggiornati regolarmente perché nuovi programmi malevoli potrebbero emergere. Per essere sempre attuale, l'applicazione può aggiornare i database dei virus tramite Internet.

Sulla schermata principale dell'applicazione nella sezione **Aggiornamento** si vede la data dell'ultimo aggiornamento dei database dei virus.

Nella modalità di protezione centralizzata, è bloccata la possibilità di avvio manuale di aggiornamento, gli aggiornamenti vengono caricati automaticamente dal server di protezione centralizzata. Se sul server di protezione centralizzata è consentito l'avvio di applicazione in modalità mobile, in caso di una rottura della connessione con il server di protezione centralizzata, l'aggiornamento dei database dei virus può essere avviato manualmente.

Aggiornamento

1. Per aggiornare i database dei virus, sulla schermata principale dell'applicazione premere sulla sezione che contiene le informazioni sugli aggiornamenti.
2. L'aggiornamento si avvia in maniera automatica.

Subito dopo l'installazione del programma si consiglia di aggiornare i database dei virus affinché **Dr.Web** possa utilizzare le definizioni antivirali più attuali. Le definizioni antivirali e le informazioni sulle caratteristiche delle minacce e sul loro comportamento vengono aggiornate appena le minacce sono state rilevate dal team del Laboratorio antivirale di **Doctor Web**, talvolta più volte all'ora.

Impostazioni di aggiornamento

Di default, gli aggiornamenti si scaricano in maniera automatica quattro volte al giorno. Nella sezione **Aggiornamento** sulla schermata delle impostazioni (v. Immagine 6) si può consentire/proibire l'utilizzo delle reti mobile per il download degli aggiornamenti. Per non utilizzare reti mobile al download degli aggiornamenti, spuntare il flag **Non utilizzare Internet mobile per scaricare gli aggiornamenti**. Se non sono state trovate reti Wi-Fi attive, si propongono reti 3G o GPRS. La modifica di quest'impostazione non influisce sull'utilizzo di reti mobile dalle altre funzioni dell'applicazione e del dispositivo mobile.

I dati di aggiornamento vengono scaricati tramite Internet. È possibile che per il trasferimento di dati venga addebitato un costo aggiuntivo. Si prega di chiedere dettagli dall'operatore di telefonia mobile.

Nella modalità di protezione centralizzata, le impostazioni di aggiornamento potrebbero essere cambiate o bloccate a seconda dei criteri di sicurezza aziendali o della lista dei servizi pagati.

Quarantena

Dr.Web offre la possibilità di mettere le minacce rilevate in quarantena – una cartella speciale in cui isolarle e conservarle in modo sicuro.

Operazioni con le minacce isolate in quarantena

1. Per guardare l'elenco di minacce messe in quarantena, sulla schermata principale del programma selezionare la voce **Quarantena**.
2. Si apre l'elenco di tutte le minacce che si trovano in quarantena (v. Immagine 9).
3. Premere su una minaccia dall'elenco per leggere le seguenti informazioni su di essa:
   - nome del file;
   - percorso al file;
   - data quando la minaccia è stata messa in quarantena.

   Inoltre si può usare il link dalla sezione **Informazioni nella rete** per leggere le informazioni dettagliate su questo tipo di minacce, disponibili al sito web della società **Doctor Web**.

4. A ciascuna minaccia è possibile applicare una delle seguenti azioni:
   - **Ripristina** – per ripristinare il file nella cartella, dove si trovava prima di essere spostato in quarantena (si prega di utilizzare questa funzione solo se si è sicuri che il file non è dannoso);
   - **Elimina** – per eliminare il file da quarantena e dal sistema.

Immagine 9. Quarantena

Dimensione della quarantena

Si può controllare quanta memoria occupa la cartella di quarantena e quanto spazio è disponibile sulla scheda SD. Per farlo, nella scheda **Quarantena** richiamare il menu dell'applicazion e selezionare la voce **Dimensione di quarantena**.

Statistiche

Dr.Web registra le statistiche delle minacce rilevate e delle azioni dell'applicazione. Per leggere le statistiche del funzionamento del programma, sullo schermo principale del programma selezionare la voce **Statistiche**.

Nella scheda **Statistiche** sono disponibili due sezioni di informazioni (v. Immagine 10):

- la sezione **Per tutto il tempo** che contiene le informazioni sul numero totale di file controllati e di minacce rilevate e neutralizzate;
- la sezione **Azioni** che contiene le informazioni circa l'inizio/la fine di una scansione tramite lo **Scanner Dr.Web**, l'attivazione/la disattivazione di **SpIDer Guard**, le minacce rilevate e le azioni eseguite per neutralizzarle. Premere sul nome della minaccia per aprire la sua descrizione sul sito della società **Doctor Web**.

Immagine 10. Statistiche

Cancellare le statistiche

Per cancellare tutte le informazioni statistiche raccolte dal programma, richiamare il menu dell'applicazione e selezionare la voce **Cancella le statistiche**.

Log di eventi

Dall'applicazione è prevista la registrazione di eventi in un log che può essere salvato sulla scheda SD per essere inviato successivamente al servizio di supporto tecnico di **Doctor Web** in caso di problemi con l'uso dell'applicazione.

Per salvare il log di eventi:

1. Premere sul tasto Menu del dispositivo quando ci si trova nella scheda **Statistiche** e scegliere la voce **Salva il log**.
2. Il log si salva nel file DrWeb_Log.txt situato nella cartella **Android/data/com.drweb/files** sulla scheda SD.

Antifurto Dr.Web

L'**Antifurto Dr.Web** consente di localizzare il dispositivo mobile e di bloccare prontamente le sue funzioni in caso di smarrimento o furto.

Nella modalità di protezione centralizzata, le impostazioni dell'**Antifurto Dr.Web** potrebbero essere cambiate o bloccate a seconda dei criteri di sicurezza aziendali o della lista dei servizi pagati.

L'**Antifurto Dr.Web** viene gestito tramite appositi comandi via SMS. Per accedere alle impostazioni dell'**Antifurto Dr.Web**, è necessario inserire la password che è stata impostata durante la

configurazione iniziale. Si deve ricordare la password perché viene usato per gestire tutte le funzioni dell'**Antifurto Dr.Web**, nonché per sbloccare il dispositivo se verrà bloccato. Se si è dimenticata la password impostata per l'**Antifurto Dr.Web**, avvalersi di un apposito servizio per resettare la password e sbloccare il dispositivo.

L'**Antifurto Dr.Web** consente di creare una lista degli amici (fino a 5 numeri telefonici) da cui dispositivi si possono inviare comandi SMS, anche se si sia dimenticato la password impostata per l'**Antifurto Dr.Web**.

Sui dispositivi con due SIM card l'**Antifurto Dr.Web** potrebbe non funzionare correttamente.

Se è attivato l'**Antifurto Dr.Web**, se vengono modificate alcune impostazioni dell'applicazione (**Reset delle impostazioni**, **Copia di riserva** e **Modalità**), sarà necessario immettere la password dell'**Antifurto Dr.Web**.

Configurazione iniziale

Al primo avvio dell'**Antifurto Dr.Web** si apre la finestra della Procedura guidata di configurazione attraverso cui è possibile impostare le funzioni principali:

- premere su **Continua** per procedere con la configurazione delle funzioni principali dell'**Antifurto Dr.Web**;
- premere su **Annulla** se si vuole configurare l'**Antifurto Dr.Web** più tardi.

Configurazione iniziale dell'Antifurto Dr.Web tramite la Procedura guidata

1. Nel primo passo della Procedura guidata di configurazione dell'**Antifurto Dr.Web** immettere una password (la password deve essere composta da almeno 4 caratteri). Questa password viene usata per gestire tutte le funzioni dell'**Antifurto Dr.Web**. Se necessario, è possibile attivare un'opzione che permette di visualizzare i caratteri della password durante l'inserimento. Per fare questo, premere sull'icona  a destra del campo di input. Per nascondere la password inserita, premere sull'icona . Premere su **Continua**.
2. Confermare la password immessa. Premere su **OK**.
3. Impostare la lista degli amici. Premere su **Continua**.

   Su Android 4.4 e superiori è necessario che la lista degli amici comprenda almeno un numero di telefono.

4. Se non si ha un account Google, quindi si apre una finestra di immissione di un indirizzo e-mail necessario per registrare l'**Antifurto Dr.Web** sul server di **Doctor Web**. La registrazione occorre per inviare all'utente un codice che permette di sbloccare il dispositivo o di impostare una nuova password se si è dimenticata la password impostata per l'**Antifurto Dr.Web**. Immettere un indirizzo e-mail valido e premere su **Continua**.

   Per registrare l'indirizzo e-mail sul server è necessaria una connessione attiva a Internet.

5. Immettere il testo che verrà visualizzato sul display del dispositivo in caso di blocco. Premere su **Continua**.
6. Qui si finisce la configurazione iniziale dell'**Antifurto Dr.Web**. Le viene proposto di registrare l'indirizzo e-mail del Suo account Google (o l'indirizzo e-mail specificato al passo precedente) sul server di **Doctor Web**. Premere su **Finito** per avviare la procedura di registrazione:

- se la registrazione è riuscita, la Procedura guidata di configurazione si chiude e si apre la schermata delle impostazioni dell'**Antifurto Dr.Web** (v. Immagine 11);
- in caso di problemi con la registrazione, sul display si visualizza la descrizione del problema. In questo caso l'**Antifurto Dr.Web** non verrà attivato sul dispositivo.

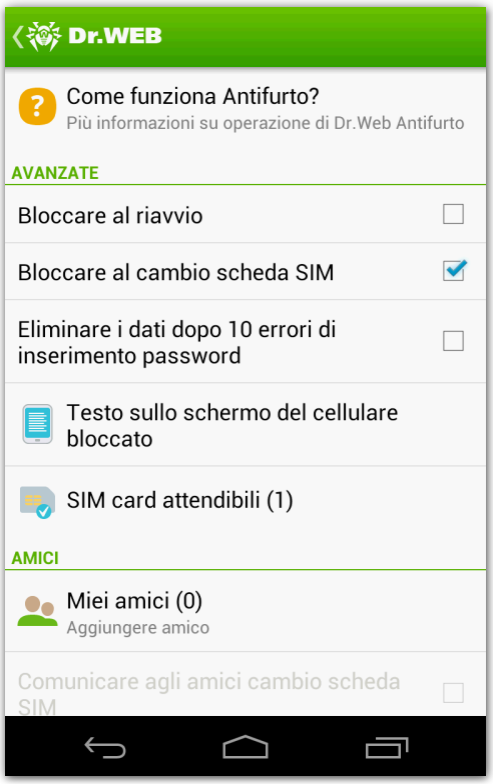


Immagine 11. Impostazioni dell'Antifurto Dr.Web

Quando si passa alla schermata principale di configurazione dell'**Antifurto Dr.Web**, potrebbe comparire un avviso che propone di attribuire a **Dr.Web** i permessi di amministratore del dispositivo. Accettare quest'assegnazione per assicurare una completa operatività dell'**Antifurto Dr.Web**.

Consultazione della guida

Per consultare la guida all'**Antifurto Dr.Web**, sulla schermata delle impostazioni dell'**Antifurto Dr.Web** (v. Immagine 11) selezionare la voce **Come funziona Antifurto?**

Cambio della password

Per cambiare la password impostata per l'**Antifurto Dr.Web**, sulla schermata delle impostazioni dell'**Antifurto Dr.Web** (v. Immagine 11) eseguire le seguenti azioni:

1. Nella sezione **Password e amministrazione** su **Cambia password**.
2. Immettere la password corrente. Premere su **OK**.
3. Immettere la password nuova. Premere su **Continua**.
4. Confermare la password nuova. Premere su **OK**.

Registrazione di un nuovo indirizzo e-mail

Per cambiare l'indirizzo e-mail registrato sul server di **Doctor Web** per l'**Antifurto Dr.Web**, sulla schermata delle impostazioni dell'**Antifurto Dr.Web** (v. Immagine 11) eseguire le seguenti azioni:

1. Nella sezione **Password e amministrazione** su **Cambia l'indirizzo email**.

2. Immettere l'indirizzo e-mail che si vuole registrare sul server di **Doctor Web**. Premere su **OK**.
3. All'indirizzo e-mail originario verrà inviato un messaggio con la conferma delle modifiche apportate.

Disattivazione dell'Antifurto Dr.Web

Per disattivare l'**Antifurto Dr.Web** sul dispositivo, sulla schermata delle impostazioni dell'**Antifurto Dr.Web** (v. Immagine 11) eseguire le seguenti azioni:

1. Nella sezione **Password e amministrazione** su **Disattiva Antifurto Dr.Web**.
2. Immettere la password impostata per l'**Antifurto Dr.Web** e premere **Disattiva Antifurto Dr.Web**.

Se l'**Antifurto Dr.Web** viene disattivato, questo abbassa notevolmente il livello di sicurezza del dispositivo.

Configurazione delle funzioni avanzate

Per impostare l'**Antifurto Dr.Web**, sulla schermata principale dell'applicazione selezionare la sezione **Antifurto**. Per accedere alla schermata delle impostazioni dell'**Antifurto Dr.Web** (v. Immagine 11), è necessario immettere la password definita per l'**Antifurto Dr.Web** a primo avvio. Se si è dimenticata la password, inviare via SMS al proprio cellulare il comando **#RESETPASSWORD#** da un numero telefonico incluso nella lista degli amici o utilizzare il relativo servizio.

Impostazioni avanzate

Per configurare l'**Antifurto Dr.Web**, nella sezione **Avanzate** sulla schermata delle impostazioni dell'**Antifurto Dr.Web** (v. Immagine 11) eseguire le seguenti azioni:

- per bloccare il cellulare se viene riavviato, attivare l'opzione **Blocca dopo il riavvio**;
- per bloccare il cellulare se viene cambiata la scheda SIM , attivare l'opzione **Blocca dopo il cambio della SIM card**;
- per cancellare completamente le informazioni personali dalla scheda SD dopo 10 inserimenti errati della password, attivare l'opzione **Elimina i dati dopo 10 errori di inserimento di password**;
- per impostare un testo che verrà visualizzato sul display del cellulare bloccato, premere su **Testo sullo schermo del cellulare bloccato**, inserire un testo (per esempio, indicare le informazioni per il contatto per restituire il telefonino), quindi premere sul pulsante **Salva**;
- per visualizzare e modificare la lista delle SIM card attendibili, premere su **Le SIM card attendibili**.

SIM card attendibili

Le SIM card che si usano sul dispositivo mobile possono essere aggiunte alla lista delle SIM card attendibili dell'**Antifurto Dr.Web**. Se una SIM card attendibile dalla lista viene cambiata a un'altra, l'**Antifurto Dr.Web** non bloccherà il dispositivo. Le nuove SIM attendibili possono essere aggiunte alla lista al riavvio del dispositivo o all'avvio di **Antivirus Dr.Web**. Inoltre, alla lista può essere aggiunta come attendibile la modalità di funzionamento senza SIM card.

La modalità di funzionamento senza SIM card può attivarsi quando non vi è una SIM card nel dispositivo, ma anche quando il dispositivo impedisce alle applicazioni installate di accedere alle informazioni sulla SIM card. In questo caso, si può ricevere un avviso erroneo sull'assenza di una SIM card, ma se si rende tale modalità attendibile, tutte le funzioni dell'**Antifurto Dr.Web** saranno a completa disposizione.

Per visualizzare e modificare la lista delle SIM card attendibili, premere su **Le SIM card attendibili** nella sezione impostazioni avanzate dell'**Antifurto Dr.Web**:

1. Di default, le SIM card si aggiungono alla lista con i nomi SIM1, SIM2 ecc. Per rinominare una SIM card, premere il suo nome nella lista (o premere e tenere premuto il suo nome, quindi selezionare **Modifica** dal menu aperto). Nella finestra aperta delle informazioni sulla SIM card, immettere un nome nuovo della SIM card nel campo **Nome** e premere su **Salva**.
2. Per eliminare una SIM card dalla lista delle SIM card attendibili, premere e tenere premuto il suo nome, quindi selezionare **Elimina** dal menu aperto.

La SIM card attualmente usata sul dispositivo non può essere rimossa dalla lista delle SIM card attendibili.

Lista degli amici

L'**Antifurto Dr.Web** consente di includere nella lista degli amici fino a 5 numeri telefonici. È possibile impostare l'invio di comandi SMS da questi numeri al Suo cellulare senza inserimento della password. Inoltre, da questi numeri è possibile inviare un comando SMS per disattivare l'**Antifurto Dr.Web** e per resettare la password.

Su Android 4.4 e superiori è necessario che la lista degli amici comprenda almeno un numero di telefono.

Configurazione della lista degli amici

1. Sulla schermata delle impostazioni dell'**Antifurto Dr.Web** (v. Immagine 11) nella sezione **Amici** premere **Miei amici**.
2. Premere su **Aggiungi** per creare una lista degli amici. Numeri telefonici e contatti possono essere selezionati nei seguenti modi:
   - dalla rubrica del telefonino;
   - dai registri di chiamate e di messaggi;
   - inserire numeri telefonici e le relative informazioni manualmente.

   Per cercare contatti e numeri nella rubrica e nei registri di chiamate e di messaggi, si può usare la funzione di ricerca disponibile tramite il tasto **Ricerca** del dispositivo. In ciascun caso è possibile scegliere uno o più numeri telefonici da aggiungere alla lista degli amici.

   Per inserire i numeri selezionati nella lista del profilo, premere sul pulsante **Aggiungi**.
3. Per modificare qualche informazione di un contatto dalla lista, premere su questo contatto nella lista, dopodiché modificare i dati nei campi **Nome** e **Numero**. Premere sul pulsante **Salva**.
4. Per eliminare un numero dalla lista, premere e tenere premuto questo numero e quindi nel menu che si apre premere su **Elimina**.

Su Android 4.4 è possibile cancellare tutti i numeri di telefono dalla lista degli amici, però non è possibile salvare la lista vuota.

5. Per informare gli amici sul cambio della SIM del cellulare, attivare l'opzione **Comunica agli amici il cambio della SIM card**.
6. Per abilitare l'invio di comandi SMS dai numeri telefonici degli amici senza l'inserimento della password impostata per l'**Antifurto Dr.Web**, attivare l'opzione **Accetta i comandi SMS senza la password**.

Anche quando l'opzione **Accetta i comandi SMS senza la password** non è attivata, i Suoi amici possono inviarLe il comando **#RESETPASSWORD#** senza necessità di inserire la password. Questo comando serve per sbloccare il dispositivo e per resettare la password dell'**Antifurto Dr.Web**.

Su Android 4.4 e superiori non è possibile disattivare l'opzione **Accetta i comandi SMS senza la password** .

Comandi SMS

L'**Antifurto Dr.Web** viene gestito tramite appositi comandi inviati via SMS che consentono di localizzare il dispositivo mobile, bloccare le sue funzioni e cancellare le informazioni personali.

Tabella di comandi SMS

Si possono usare i seguenti comandi SMS per gestire l'**Antifurto Dr.Web**:

Comando	Azione
#LOCK#*Password#*	Per bloccare il telefono.
#SIGNAL#*Password#*	Per bloccare il telefono e per attivare un segnale acustico che continua a suonare dopo il riavvio del telefono.
#LOCATE#*Password#*	Per ricevere le coordinate GPS del telefono in un messaggio SMS. L'SMS ricevuto contiene un link con le coordinate della presunta posizione del dispositivo sulla mappa. Quando l'utente preme sul link ricevuto, la posizione del dispositivo viene indicata tramite **Dr.Web Anti-theft Locator** - uno servizio speciale di **Doctor Web** che visualizza nel browser una mappa dell'area e la posizione del dispositivo su di essa. La precisione con cui vengono determinate le coordinate del dispositivo dipende dalla disponibilità del ricevitore GPS, dalla visibilità delle reti Wi-Fi circostanti e delle stazioni più vicine di trasmissione GSM. Così, a seconda dei dati ottenuti, le coordinate verranno determinate esattamente (una posizione sulla mappa) o approssimativamente (un cerchio di un raggio determinato). Nella parte superiore della schermata con la mappa, l'utente può selezionare il servizio di mappe più adatto.
#UNLOCK#*Password#*	Per sbloccare il dispositivo senza resettare la password dell'**Antifurto Dr.Web**.
#WIPE#*Password#*	Per ripristinare le impostazioni di fabbrica sul telefono ed eliminare tutte le informazioni dalla scheda SD. Questo comando verrà eseguito anche dopo 10 inserimenti di una password errata in caso se il dispositivo è bloccato e nelle impostazioni dell'**Antifurto Dr.Web** è attivata l'opzione **Elimina i dati dopo 10 errori di inserimento di password**.

Comando	Azione
#RESETPASSWORD#	Per sbloccare il dispositivo e per resettare la password impostata per l'**Antifurto Dr.Web**. Questo comando può essere inviato solo da un numero di telefono incluso nella lista degli amici.

I comandi SMS non dipendono dalle lettere maiuscole e minuscole. Per esempio, il comando di blocco del telefono **#LOCK#***Password***#** può essere scritto come **#Lock#***Password***#**, **#lock#***Password***#**, **#lOck#***Password***#** ecc.

Affinché siano più precisi i risultati ottenuti dopo l'invio del comando SMS #LOCATE#, nelle impostazioni del dispositivo mobile consentire di usare reti wireless per la localizzazione.

Invio di comandi SMS tramite l'interfaccia dell'Antifurto Dr.Web

Si possono inviare comandi SMS direttamente dall'**Antifurto Dr.Web** ai dispositivi su cui anche funziona l'**Antifurto Dr.Web**. Per farlo, eseguire le seguenti azioni:

1. Sulla schermata delle impostazioni dell'**Antifurto Dr.Web** (v. Immagine 11) nella sezione **Amici** premere **Invia comando SMS**.
2. Immettere il numero telefonico a cui si vuole inviare un comando SMS.
3. Selezionare un comando dalla lista:
   - **Blocca** – corrisponde al comando #LOCK#;
   - **Blocca ed accendi il segnale acustico** – corrisponde al comando #SIGNAL#;
   - **Trova la posizione** – corrisponde al comando #LOCATE#;
   - **Sblocca** – corrisponde al comando #UNLOCK#;
   - **Elimina tutti i dati** – corrisponde al comando #WIPE#;
   - **Resetta password** – corrisponde al comando #RESETPASSWORD#.
4. Inserire la password impostata per l'**Antifurto Dr.Web** sul dispositivo del destinatario del comando. Se il Suo numero telefonico è incluso nella lista degli amici impostata sul telefono del destinatario del comando, la password potrebbe essere anche non necessaria.
5. Premere sul pulsante **Invia**.

Sblocco dell'Antifurto Dr.Web

Se si è dimenticata la password impostata per l'**Antifurto Dr.Web** e il dispositivo mobile è bloccato, eseguire le seguenti azioni:

1. Andare alla pagina https://antitheft.drweb.com/.
2. Immettere il codice visualizzato sullo schermo del dispositivo bloccato e l'indirizzo email che si è utilizzato per registrare l'**Antifurto Dr.Web** sul server **Doctor Web** nei campi corrispondenti (v. Immagine 12).
3. Premere il pulsante **Ottieni il codice**. Un codice che serve a sbloccare il dispositivo e disabilitare l'**Antifurto Dr.Web** verrà spedito sull'indirizzo e-mail specificato.
4. Immettere il codice ricevuto nel campo **Inserire la password di Antifurto** sullo schermo del dispositivo bloccato.

Il dispositivo verrà sbloccato e l'**Antifurto Dr.Web** verrà disattivato. Per riprendere l'utilizzo dell'**Antifurto Dr.Web** è necessario attivarlo e configurarlo di nuovo.

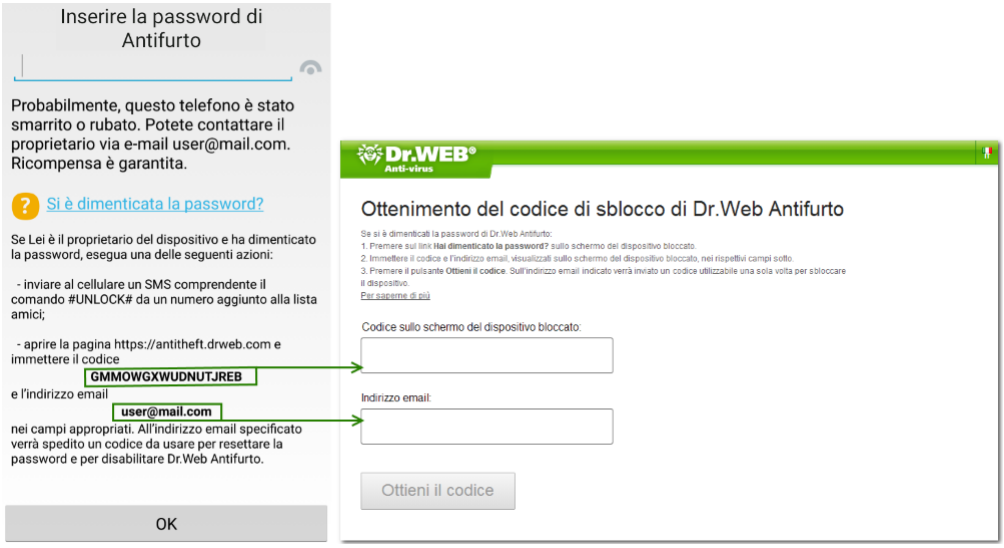


Immagine 12. Sblocco dell'Antifurto Dr.Web

Limitazione dell'accesso a Internet

L'accesso alle risorse di Internet viene controllato dal filtraggio degli URL **Cloud Checker**. Il filtraggio consente di proteggere l'utente del dispositivo mobile da siti web indesiderati.

Cloud Checker controlla l'accesso alle risorse di Internet solo se si usano il browser integrato del sistema Android, nonché Google Chrome, Google Chrome Beta, Next, Amazon Silk, Yandex.Browser, Boat Browser e Boat Browser Mini.

Nella modalità di protezione centralizzata, le impostazioni di **Cloud Checker** potrebbero essere cambiate o bloccate a seconda dei criteri di sicurezza aziendali o della lista dei servizi pagati.

Utilizzando il filtro **Cloud Checker**, si può impedire l'accesso a diverse categorie di siti web sconsigliati o potenzialmente pericolosi:

- Siti sconsigliati;
- Siti per adulti;
- Violenza;
- Armi;
- Giochi d'azzardo;
- Droga;
- Linguaggio osceno;
- Chat;
- Terrorismo;
- Posta elettronica;
- Social network;
- URL aggiunti a richiesta del titolare dei diritti d'autore.

Di default, **Cloud Checker** blocca l'accesso ai siti noti come fonti di diffusione dei virus.

Per il corretto funzionamento di **Cloud Checker** è necessario che nel browser in uso sia attivata la funzione di salvataggio della cronologia.

Attivazione/disattivazione del filtraggio URL

1. Sulla schermata principale dell'applicazione (v. Immagine 2) selezionare l'opzione **Cloud Checker**. Si apre la schermata delle impostazioni del filtraggio URL (v. Immagine 13).

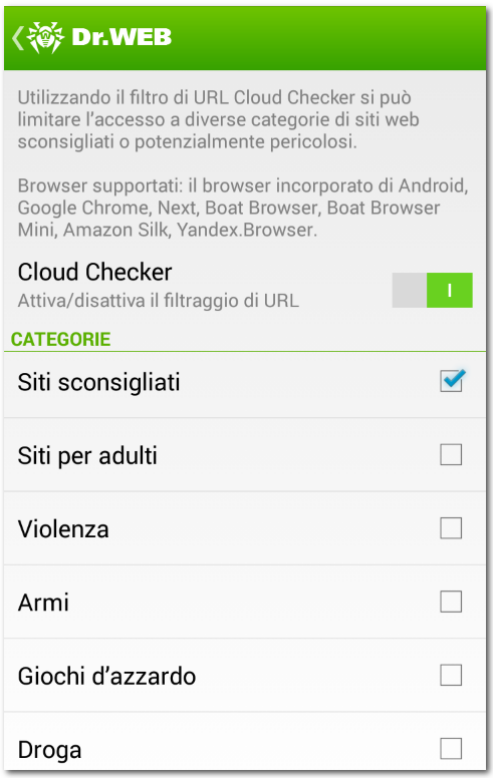


Immagine 13. Schermata delle impostazioni del filtraggio Cloud Checker

2. La funzione di filtraggio di risorse del web può essere attivata/disattivata tramite l'opzione **Cloud Checker**. Di default, il filtraggio di risorse del web è attivato.
3. Dall'elenco **Categorie** scegliere le categorie di siti web a cui si vuole impedire l'accesso.

Firewall Dr.Web

Il **Firewall Dr.Web** è progettato per la protezione del dispositivo mobile contro l'accesso da fuori non autorizzato e per la prevenzione della fuga di informazioni importanti attraverso la rete. Questo componente consente di controllare le connessioni a Internet e la trasmissione di dati via rete e di impedire connessioni non attendibili.

Il **Firewall Dr.Web** utilizza per il funzionamento la tecnologia delle VPN per Android. Su alcuni dispositivi il protocollo di utilizzo delle VPN può essere disattivato dal produttore e non è disponibile per le altre applicazioni. In tale caso, le funzioni del firewall non sono disponibili. Per maggiori informazioni, rivolgersi al produttore del dispositivo.

Attivare/disattivare il Firewall Dr.Web

1. Sulla schermata principale dell'applicazione (v. Immagine 2) selezionare l'opzione **Firewall**. Si apre la schermata di configurazione del firewall (v. Immagine 14).

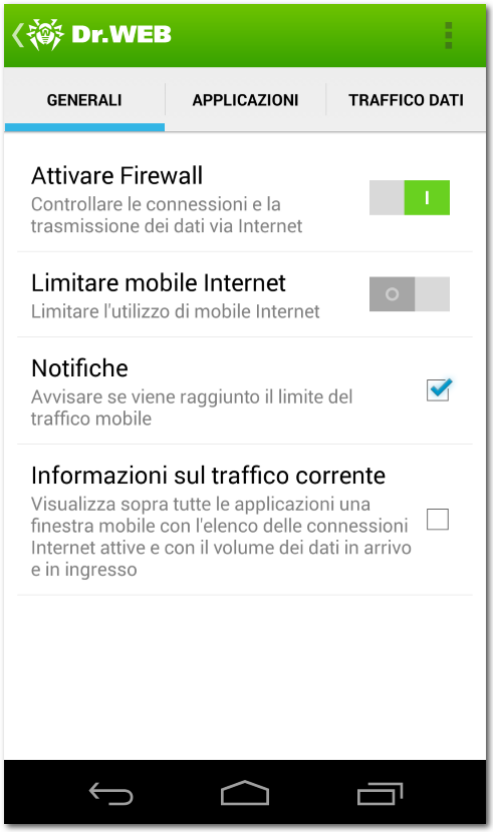


Immagine 14. Schermata di configurazione del firewall. Scheda Generali

2. Il Firewall può essere attivato/disattivato tramite l'opzione **Attiva Firewall**. Di default, il firewall è disattivato. Quando il firewall viene attivato, si visualizza una richiesta che chiede di permettere a **Dr.Web** di utilizzare le VPN. Affinché il firewall possa funzionare, è necessario permettere questa possibilità.

Se nel processo di funzionamento il diritto di utilizzare le VPN passa a un'altra applicazione, il **Firewall Dr.Web** viene disattivato e un avviso corrispondente compare nella sezione delle notifiche. Per attivare nuovamente il **Firewall Dr.Web**, basta premere su questo avviso.

Particolarità dell'utilizzo

Il **Firewall Dr.Web** è realizzato sulla base della tecnologia delle VPN per Android perciò può funzionare senza ottenimento dei permessi di root sul dispositivo. La realizzazione della tecnologia delle VPN su Android è legata a determinate restrizioni:

- Primo, in qualsiasi momento soltanto un'applicazione sul dispositivo può usare le VPN. Di conseguenza, quando un'applicazione richiede l'utilizzo delle VPN, si apre una finestra che chiede di permettere all'applicazione di utilizzare le VPN. Se l'utente accetta la richiesta, l'applicazione comincia a utilizzare le VPN, mentre un'altra applicazione che poteva utilizzare le VPN fino a questo momento non ha più questa possibilità. Tale richiesta compare al primo avvio del **Firewall Dr.Web** e poi a ciascun riavvio del dispositivo. Inoltre, tale richiesta potrebbe comparire quando le altre applicazioni richiedono l'utilizzo delle VPN. Si deve condividere nel tempo la possibilità di utilizzare le VPN tra le applicazioni. Il firewall è in grado di funzionare solo quando ha il completo permesso di utilizzare le VPN.

- Un'altra particolarità relativa all'utilizzo della tecnologia delle VPN è che il **Firewall Dr.Web** è in grado di impedire soltanto le connessioni con le reti esteriori (con Internet). Questo dipende dal modello del dispositivo e dalle applicazioni utilizzate per la connessione.

La tecnologia delle VPN per Android viene utilizzata soltanto per la realizzazione delle funzioni del firewall, mentre nessun Tunnel VPN viene creato e il traffico Internet non viene cifrato.

Limitare l'utilizzo di mobile Internet

Con l'ausilio del **Firewall Dr.Web**, si può limitare il consumo di traffico dati del mobile Internet.

1. Per attivare/disattivare la funzione di limitazione del mobile Internet, selezionare l'opzione **Limita Internet mobile** nella scheda **Generali** della schermata di configurazione del firewall (v. Immagine 14).
2. Attivando la limitazione, impostare un limite di consumo del traffico mobile (in megabyte o gigabyte). Si può scegliere il periodo di limitazione: un giorno, una settimana o un mese.
3. Se necessario, indicare la quantità di traffico consumata dall'inizio del periodo di limitazione scelto:
   - se il periodo di limitazione è di un giorno, il tempo viene contato dalle 00:00 del giorno corrente;
   - se il periodo di limitazione è di una settimana, il tempo viene contato dalle 00:00 del giorno corrente;
   - se il periodo di limitazione è di un mese, il tempo viene contato dalle 00:00 del primo giorno del mese di calendario corrente.

Quando il consumo di traffico dati del mobile Internet viene limitato, nella scheda **Generali** della schermata di configurazione del firewall compare un diagramma che visualizza la quantità di traffico residua. Accanto al diagramma si visualizza il limite stabilito e il conto alla rovescia del tempo mancante alla fine del periodo di limitazione (v. Immagine 15).

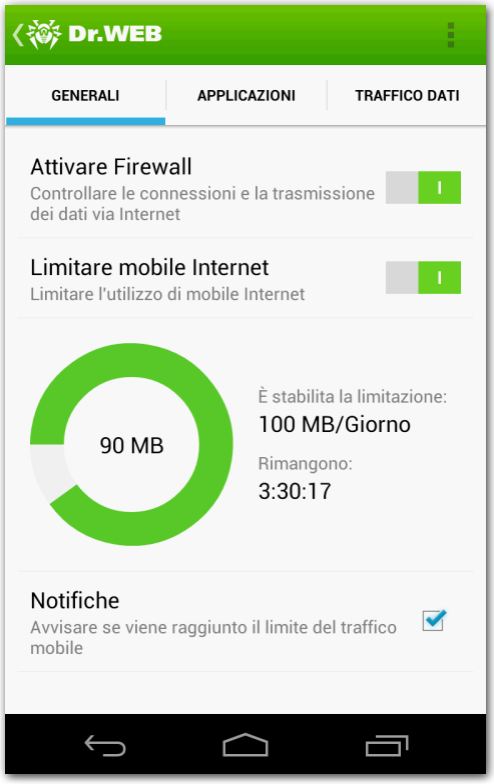


Immagine 15. Schermata di configurazione del firewall con l'attivata limitazione del mobile Internet

Quando si usa la limitazione del traffico dati mobile, il limite stabilito potrebbe essere oltrepassato di una piccola quantità non più di 4 Kb.

Avvisi

È possibile configurare le notifiche per essere avvisati se è stato raggiunto il limite di traffico dati mobile. Per fare questo, spuntare il flag **Notifiche** nella scheda **Generali** della schermata di configurazione del firewall (v. Immagine 14).

Elaborazione del traffico dati delle applicazioni

Il **Firewall Dr.Web** consente di configurare l'elaborazione del traffico Internet a livello delle applicazioni e in questo modo consente di controllare l'accesso di determinati programmi e processi alle risorse di rete. Si può accedere alle informazioni sul traffico Internet consumato da parte delle applicazioni installate sul dispositivo e configurare per esse le regole di accesso alle risorse di rete nella scheda **Applicazioni** della schermata di configurazione del firewall (v. Immagine 16).

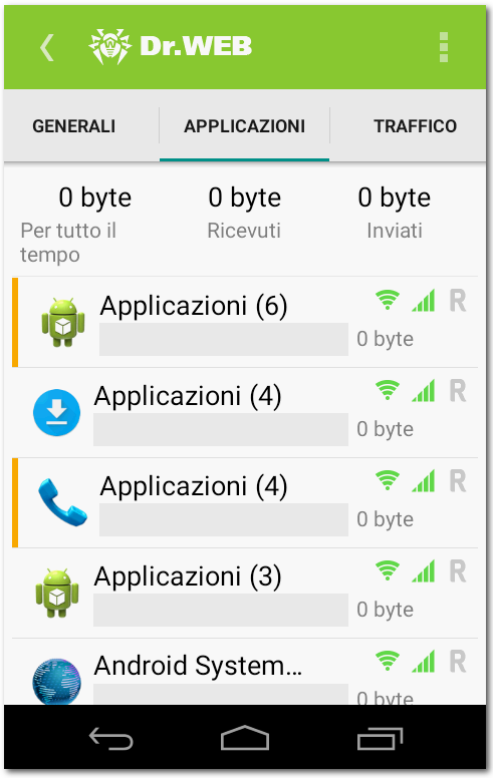


Immagine 16. Schermata di configurazione del firewall. Scheda Applicazioni

Nella scheda **Applicazioni** è visualizzata la quantità totale di dati trasmessi attraverso la rete, nonché la dimensione di dati ricevuti e inviati.

Quindi è riportata una lista delle applicazioni (gruppi di applicazioni) per ciascuna delle quali è indicata la quantità di traffico Internet consumata. Per vedere la lista di tutte le applicazioni installate sul dispositivo, comprese quelle con un consumo di traffico pari a zero, spuntare il flag **Tutte le applicazioni** nel menu nella scheda **Applicazioni**.

Per ciascuna applicazione, si può consentire/proibire l'utilizzo delle reti Wi-Fi, del mobile Internet e di Internet in roaming con l'ausilio delle opzioni opportune situate a destra del nome dell'applicazione.

Le applicazioni con impostazioni modificate vengono segnate nella lista.

Per vedere le informazioni dettagliate sull'utilizzo di Internet da parte di un'applicazione (gruppo di applicazioni) dalla lista, premere su quest'applicazione nella lista. Nella finestra che si è aperta è possibile eseguire le seguenti azioni:

- consentire/proibire all'applicazione (gruppo di applicazioni) di utilizzare reti Wi-Fi, mobile Internet e Internet in roaming;
- visualizzare il log dell'applicazione (gruppo di applicazioni);
- visualizzare le statistiche di consumo di traffico Internet da parte di quest'applicazione (gruppo di applicazioni);
- configurare le regole di connessione per quest'applicazione (gruppo di applicazioni).

Statistiche di consumo di traffico Internet

Sulla schermata con le informazioni dettagliate sul traffico dati dell'applicazione (gruppo di applicazioni)

sono disponibili le statistiche di utilizzo di Internet da parte di quest'applicazione, visualizzate in un diagramma (v. Immagine 17).

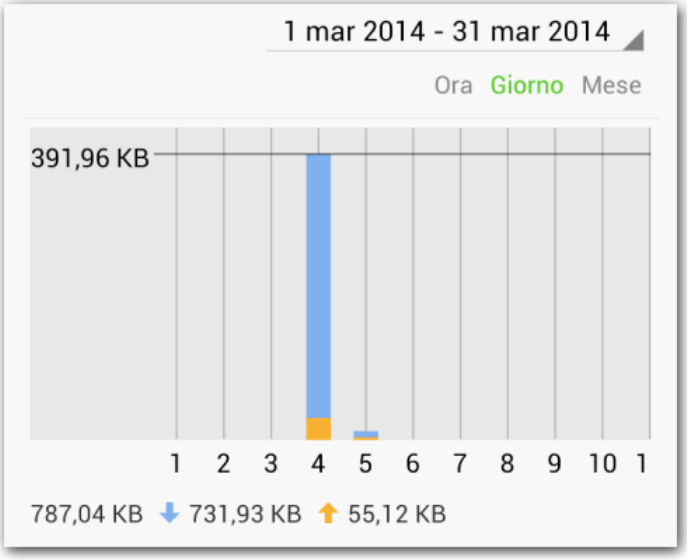


Immagine 17. Statistiche di consumo di traffico Internet da un'applicazione

Nel diagramma i dati dell'applicazione in uscita sono contrassegnati con il giallo, i dati in arrivo con il blue. Sotto il diagramma sono riportati i valori numerici di traffico consumati (generali, in uscita e in arrivo).

Per la visualizzazione delle statistiche di consumo di traffico Internet sono disponibili le seguenti azioni:

- selezionare un periodo per la visualizzazione delle statistiche da un apposito elenco. Le statistiche possono essere mostrate per il giorno corrente, per l'ultima settimana, per il mese corrente, per il mese precedente oppure si può impostare un periodo indicando la data di inizio e di fine;
- nel periodo selezionato, le statistiche possono essere visualizzate per ora, giorno o mese.

Cancellare le statistiche

Se necessario, si possono cancellare tutti i dati statistici di funzionamento del firewall oppure le statistiche riguardanti singole applicazioni.

Per eliminare le statistiche per tutte le applicazioni:

1. In qualsiasi scheda della schermata di configurazione del firewall (v. Immagine 14) selezionare nel menu l'opzione **Cancellare**.
2. Nella finestra che si è aperta spuntare il flag **Cancella le statistiche**. Premere su **OK**.

Per eliminare le statistiche per una singola applicazione:

1. Nella scheda **Applicazioni** della schermata di configurazione del firewall (v. Immagine 16) selezionare l'applicazione per il quale si desiderano cancellare le statistiche.
2. Dal menu sulla schermata con le informazioni dettagliate sul traffico dati dell'applicazione selezionare l'opzione **Cancellare**.
3. Nella finestra che si è aperta spuntare il flag **Cancella le statistiche per quest'applicazione**. Premere su **OK**.

Regole di connessione

Inoltre, sulla schermata con le informazioni dettagliate sul traffico dati dell'applicazione (gruppo di applicazioni) si possono configurare le regole che determinano la connessione di quest'applicazione a determinati indirizzi IP e porte.

Creare un set di regole

1. Per creare una regola, premere sul pulsante **Aggiungi regola**. Si possono aggiungere le regole di permesso e di divieto a seconda del valore dell'opzione corrispondente nella sezione **Regole di connessione**:
   - se è stato selezionato il valore **Blocca le connessioni dalla lista**, viene aggiunta una regola di divieto;
   - se è stato selezionato il valore **Consenti solo le connessioni dalla lista**, viene aggiunta una regola di divieto.
2. Nella finestra di creazione della regola, nel campo **Indirizzo IP** indicare un indirizzo IP valido (in formato a.b.c.d), un intervallo di indirizzi IP (in formato a1.b1.c1.d1-a2.b2.c2.d2) o una rete intera (in formato a.b.c.0/n, dove n è un numero da 1 a 32) o lasciare vuoto questo campo (in tale caso è necessario definire obbligatoriamente la porta di connessione). Nel campo **Porta** indicare il numero di una porta valida o lasciare vuoto questo campo (in tale caso è necessario definire obbligatoriamente l'indirizzo IP di connessione). Se uno dei campi è lasciato vuoto, la regola verrà applicata rispettivamente a qualsiasi indirizzo IP o porta. Premere su **OK** per confermare l'eliminazione.
3. Per modificare una regola esistente, premerla e tenerla premuta nella lista e quindi premere il pulsante **Modifica**.

Inoltre, si possono aggiungere le regole di divieto e di permesso quando si visualizzano i log delle applicazioni o la lista delle connessioni correnti.

Eliminazione di regole di connessione

- Per eliminare una regola, premerla e tenerla premuta nella lista e quindi premere il pulsante **Elimina**.
- Per eliminare tutte le regole per una determinata applicazione:
  1. Selezionare quest'applicazione dalla lista (v. Immagine 16).
  2. Nel menu dell'applicazione selezionare la voce **Cancellare**.
  3. Nella finestra che si è aperta spuntare il flag **Cancella le regole per quest'applicazione**.
- Per eliminare tutte le regole per tutte le applicazioni:
  1. Sulla schermata con la lista delle applicazioni (v. Immagine 16) aprire il menu dell'applicazione e selezionare la voce **Cancellare**.
  2. Nella finestra che si è aperta spuntare il flag **Cancella le regole per le applicazioni**.

Connessioni in ingresso

Tramite il flag **Consenti quelle in entrata** che si trova nel menu sulla schermata con le informazioni sul traffico dati dell'applicazione si può impostare che il firewall non controlli le connessioni in ingresso. Nel log dell'applicazione e nelle statistiche di funzionamento del firewall vengono registrate soltanto le informazioni parziali sulle connessioni che gli indirizzi remoti stabiliscono con la porta aperta dall'applicazione. Inoltre, si può impostare che il firewall non controlli le connessioni che le altre applicazioni stabiliscono con questi indirizzi. Tale modalità di utilizzo non è sicura e, in generale, non è consigliabile.

Tale modalità è giustificata quando non è possibile evitare la disattivazione del firewall in nessun altro modo, per esempio, se sul dispositivo è configurato un server che accetta connessioni dalle reti esteriori.

Attività corrente delle connessioni di rete

Le informazioni sulle connessioni di rete attive a dato momento possono essere ottenute nei seguenti modi:

1. Nella scheda **Traffico** della schermata delle impostazioni del firewall (v. Immagine 14).

   Nella scheda viene visualizzata in tempo reale una lista delle connessioni iniziate dalle applicazioni installate sul dispositivo. Per vedere le informazioni dettagliate sulle connessioni di un'applicazione (indirizzi IP e porte di connessione, dimensione dei dati trasmessi/ricevuti), premere su quest'applicazione nella lista.

   Si possono creare le regole di permesso e di divieto per le connessioni presenti nella lista. Premere e tenere premuta una connessione nella lista, dopodiché scegliere l'opzione desiderata:

   - **Aggiungi regola di permesso**, si usa per creare una regola che permette le connessioni dell'applicazione selezionata con i corrispondenti indirizzo IP e porta;
   - **Aggiungi regola di divieto**, si usa per creare una regola che blocca tutte le connessioni dell'applicazione selezionata con i corrispondenti indirizzo IP e porta.

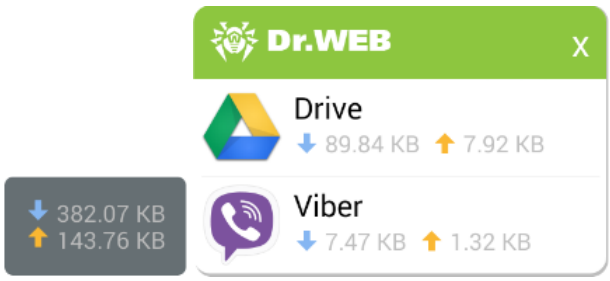
2. Tramite la finestra mobile con le informazioni su traffico dati attuale.

   Per visualizzare una finestra mobile, spuntare il flag **Informazioni sul traffico dati corrente** sulla schermata delle impostazioni del firewall (v. Immagine 14). Sopra tutte le applicazioni verrà visualizzata una finestra mobile con la dimensione dei dati in arrivo e in uscita (v. Immagine 18a).

La dimensione del traffico dati viene calcolata dal momento dell'apertura della finestra mobile.

Utilizzo della finestra mobile

- Per aprire la lista delle applicazioni che stanno utilizzando le connessioni Internet (v. Immagine 18b), premere sulla finestra mobile. Quando un'applicazione viene selezionata dalla lista, viene aperta la scheda **Traffico** con le informazioni dettagliate sulle connessioni correnti.
- Per chiudere la lista delle applicazioni, premere X.
- Per nascondere la finestra mobile, togliere il flag **Informazioni sul traffico dati corrente**.



Immagini 18a e 18b. Finestra mobile del traffico corrente

Registrazione degli eventi

L'applicazione registra gli eventi relativi al funzionamento del **Firewall Dr.Web**. L'utente può visualizzare l'elenco generale degli eventi oppure soltanto gli eventi relativi alle connessioni di rete di singole applicazioni.

Log del Firewall Dr.Web

Per visualizzare l'elenco di tutti gli eventi relativi al funzionamento del **Firewall Dr.Web**, selezionare l'opzione **Log** dal menu in qualsiasi scheda della schermata di configurazione del firewall (v. Immagine 14).

Visualizzazione del log degli eventi

Per rendere più facile la ricerca delle informazioni nell'elenco degli eventi, si possono utilizzare le funzioni di ordinamento dei record e di scorrimento rapido (che si usa spostando un apposito elemento grafico nella parte destra della schermata). Per ordinare i record nel log, scegliere un criterio di ordinamento dal menu sulla schermata del log.

La descrizione di ogni evento include le seguenti informazioni:

- data e ora di connessione (per il TCP) o tempo in cui sono stati ricevuti i pacchetti di dati con i valori corrispondenti di traffico (per lo UDP). Ad esempio: 18/02/2014 2:07:11 - 18/02/2014 2:07:12;
- indirizzo locale e porta locale. Ad esempio: src: 10.2.3.5:6881;
- dati in ingresso e in uscita (in byte) o numero di pacchetti bloccati. Ad esempio: in:103 out:112 o blocked packets:1;
- l'identificatore dell'applicazione sul dispositivo, connessa con questo traffico dati (User ID). Ad esempio: uid=10071;
- numero di traffic jams (congestione di traffico dati) (solo per il TCP). Ad esempio: traffic jam=0. I traffic jams sono una situazione quando il programma client non fa in tempo a scaricare il buffer di ricezione TCP, di conseguenza si forma un "ingorgo" che potrebbe rallentare il trasferimento di dati attraverso la rete.

Cancellare il log

Per cancellare l'elenco di tutti gli eventi relativi al funzionamento del **Firewall Dr.Web**:

1. In qualsiasi scheda della schermata di configurazione del firewall (v. Immagine 14) selezionare nel menu l'opzione **Cancellare**.
2. Nella finestra che si è aperta spuntare il flag **Cancella il log**. Premere su **OK**.

Dimensione del log

Di default, il file di log ha la dimensione massima, pari ai 5 MB. Per modificare la dimensione massima consentita del file di log:

1. In qualsiasi scheda della schermata di configurazione del firewall (v. Immagine 14) selezionare nel menu l'opzione **Cancellare**.
2. Nella finestra che si è aperta modificare il valore indicato nel campo **Dimensione massima del file di log**. Premere su **OK**.

Log delle applicazioni

Per visualizzare l'elenco degli eventi relativi alle connessioni di rete di un'applicazione installata sul dispositivo, sulla schermata con le informazioni dettagliate sul traffico dati di quest'applicazione premere sulla sezione **Log**.

Visualizzazione del log dell'applicazione

Tutti gli eventi nel log dell'applicazione sono raggruppati per data. Per visualizzare gli eventi accaduti in un determinato giorno, selezionarlo dall'elenco. La descrizione di ogni evento include le seguenti informazioni:

- data e ora di connessione (per il TCP) o tempo in cui sono stati ricevuti i pacchetti di dati con i valori

corrispondenti di traffico (per lo UDP);
- indirizzo locale e porta locale;
- dati in ingresso e in uscita (in byte) o numero di pacchetti bloccati.

Si possono creare le regole di permesso e di divieto per le connessioni riportate nel log dell'applicazione. Premere e tenere premuta una connessione nella lista, dopodiché scegliere l'opzione desiderata:

- **Aggiungi regola di permesso**, si usa per creare una regola che permette le connessioni dell'applicazione selezionata con i corrispondenti indirizzo IP e porta;
- **Aggiungi regola di divieto**, si usa per creare una regola che blocca tutte le connessioni dell'applicazione selezionata con i corrispondenti indirizzo IP e porta.

Cancellare il log dell'applicazione

Per cancellare il log dell'applicazione:

1. Dal menu sulla schermata con le informazioni dettagliate sul traffico dati dell'applicazione selezionare l'opzione **Cancellare**.
2. Nella finestra che si è aperta spuntare il flag **Cancella il log per quest'applicazione**. Premere su **OK**.

Disattivare la registrazione degli eventi per un'applicazione

Se necessario, si può disattivare il logging per singole applicazioni. Per farlo, eseguire le seguenti azioni:

1. Dal menu sulla schermata con le informazioni dettagliate sul traffico dati dell'applicazione selezionare l'opzione **Cancellare**.
2. Nella finestra che si è aperta spuntare il flag **Non registrare il log per quest'applicazione**. Premere su **OK**.

Aiuto nella risoluzione dei problemi di sicurezza

Con l'ausilio di un apposito componente - **Security Auditor** - **Dr.Web** consente di valutare lo stato di sicurezza del dispositivo mobile e di rimuovere i problemi e le vulnerabilità rilevati. Questo componente inizia a funzionare automaticamente una volta avviata l'applicazione e registrata la licenza. Il numero di problemi rilevati è mostrato nella sezione **Auditor di sicurezza** sulla schermata principale dell'applicazione.

Se analizzando il sistema, il **Security Auditor** non scopre alcuni problemi o vulnerabilità, la sezione corrispondente non si visualizza sulla schermata principale dell'applicazione.

Possibili problemi e modi per risolverli

Per vedere l'elenco dei problemi di sicurezza rilevati (v. Immagine 19), premere sulla sezione **Auditor di sicurezza** sulla schermata principale dell'applicazione.

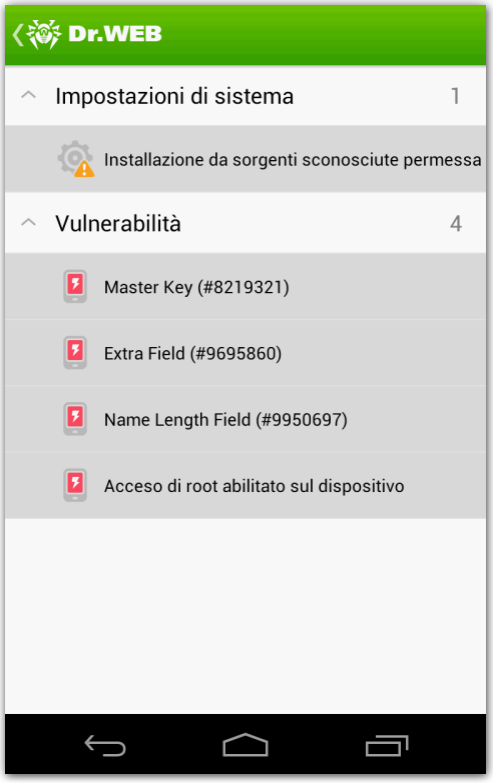


Immagine 19. Aiuto nella risoluzione dei problemi di sicurezza

Dr.Web consente di rilevare i seguenti tipi di problemi di sicurezza: la presenza delle applicazioni con la più alta priorità di elaborazione degli SMS, la presenza degli amministratori del dispositivo nascosti, la presenza delle vulnerabilità e delle impostazioni di sistema che influiscono sulla sicurezza del dispositivo. Per vedere le informazioni dettagliate su un problema e sul modo per risolverlo, aprire l'elenco della categoria richiesta e premere sul problema/sulla vulnerabilità nell'elenco.

Applicazioni con la più alta priorità di elaborazione degli SMS

In questa categoria è riportato un elenco delle applicazioni che hanno una priorità di elaborazione degli SMS più alta di **Dr.Web**. Tali applicazioni potrebbero impedire il funzionamento dell'Antifurto Dr.Web e il filtraggio degli SMS dato che esse intercettano tutti i messaggio e comandi in arrivo. In alcuni casi, tali applicazioni sono malevole e potrebbero minacciare la sicurezza del dispositivo.

Se si è accorti che i messaggi SMS non vengono filtrati o che l'**Antifurto Dr.Web** non funziona, cercare di modificare, se possibile, le impostazioni relative delle applicazioni riportate nell'elenco, in seguito a cui queste applicazioni dovrebbero scomparire dall'elenco dei problemi e delle vulnerabilità. Se non si è sicuri che queste applicazioni siano assolutamente attendibili, è consigliabile rimuoverle. Per rimuovere un'applicazione, premere sul pulsante **Elimina** sulla schermata con le informazioni dettagliate sul problema connesso con quest'applicazione oppure utilizzare gli strumenti standard del sistema operativo.

Amministratori del dispositivo nascosti

Le applicazioni che sono attivate come amministratori del dispositivo ma non sono elencate nella lista amministratori nella sezione corrispondente delle impostazioni del dispositivo non possono essere rimosse con gli strumenti standard del sistema operativo. È molto probabile che tali applicazioni non siano sicure.

Se non si sa perché un'applicazione nasconde la sua presenza nella lista degli amministratori del dispositivo, è consigliabile rimuoverla. Per rimuovere un'applicazione, premere sul pulsante **Elimina** sulla schermata con le informazioni dettagliate sul problema connesso con quest'applicazione.

Impostazioni di sistema

Le impostazioni di sistema che influiscono sulla sicurezza del dispositivo sono la modalità di debugging e il permesso di installare applicazioni da sorgenti sconosciute. Anche l'utilizzo di programmi in conflitto non è sicuro:

- **Il debugging tramite USB** è progettato per gli sviluppatori e consente di copiare dati dal computer a un dispositivo Android e viceversa, di installare applicazioni sul dispositivo, di visualizzare log delle applicazioni installate e di rimuoverle in alcuni casi. Se non si è sviluppatori e non si usa la modalità di debugging, è consigliabile disattivarla. Per passare alla sezione corrispondente delle impostazioni di sistema, premere sul pulsante **Impostazioni** sulla schermata con le informazioni dettagliate su questo problema.
- **L'installazione** delle applicazioni da sorgenti sconosciute è la principale causa di propagazione delle minacce mobile. Con un'elevata probabilità, le applicazioni scaricate non dal catalogo ufficiale delle applicazioni (Google Play) potrebbero rivelarsi non sicure e potrebbero causare un danno al dispositivo. Per ridurre il rischio di installazione delle applicazioni non sicure, è consigliabile vietare l'installazione delle applicazioni da sorgenti sconosciute. Per passare alla sezione corrispondente delle impostazioni di sistema, premere sul pulsante **Impostazioni** sulla schermata con le informazioni dettagliate su questo problema. Inoltre, è consigliabile controllare tramite l'antivirus tutte le applicazioni che si vogliono installare. Prima di eseguire un controllo, è necessario verificare se i **database dei virus Dr.Web** siano aggiornati.
- **Conflitti dei programmi**. L'utilizzo di programmi in conflitto, in particolare, l'utilizzo dei browser non supportati dal filtraggio degli URL Cloud Checker riduce la sicurezza del dispositivo. In caso di utilizzo di tali browser, l'utente non è protetto contro i siti web indesiderati e malevoli. Pertanto, si consiglia di utilizzare, anche come il browser predefinito, il browser incorporato di Android, Google Chrome, Google Chrome Beta, Next, Amazon Silk, Yandex.Browser, Boat Browser e Boat Browser Mini.

Vulnerabilità

Dr.Web consente di rilevare le vulnerabilità nel sistema del dispositivo, quali per esempio Master Key (#8219321), Extra Field (#9695860), Name Length Field (#9950697), Fake ID (#13678484), ObjectInputStream Serialization (CVE-2014-7911), PendingIntent (CVE-2014-8609), Android Installer Hijacking, OpenSSLX509Certificate (CVE-2015-3825) e Sragefright. Sfruttando queste vulnerabilità, i malintenzionati potrebbero aggiungere un codice di programma ad alcune applicazioni senza modificarne le firme crittografiche, e in seguito a ciò queste applicazioni potrebbero avere funzioni che rappresentano una minaccia per il dispositivo. Inoltre, **Dr.Web** rileva la presenza nel sistema della vulnerabilità Heartbleed, cioè di un errore nel software crittografico OpenSSL che consente ai malintenzionati di accedere alle informazioni confidenziali dell'utente.

Se vengono rilevate una o più vulnerabilità da quelle elencate, controllare la disponibilità degli aggiornamenti del sistema operativo del dispositivo sul sito del produttore poiché nelle versioni nuove la falla potrebbe essere riparata. Se gli aggiornamenti non sono disponibili, è consigliabile installare applicazioni solo da fonti attendibili.

Inoltre, il dispositivo potrebbe diventare vulnerabile nei confronti di diversi tipi di minacce, se su di esso sono disponibili i permessi di root, cioè sono state fatte modifiche per ottenere i permessi di superuser (root). Tali permessi consentono di modificare e di rimuovere file di sistema, il che potrebbe causare il malfunzionamento del dispositivo. Se queste modifiche sono state fatte dall'utente, è consigliabile annullarle per motivi di sicurezza. Se i permessi di root sono una caratteristica tecnica del dispositivo o servono all'utente per fare qualche attività, è consigliabile essere molto attenti installando applicazioni da fonti non attendibili.

Sevizio accorciamento URL

In alcuni casi, per esempio, se è limitato il numero di caratteri in SMS o in messaggi di social network, potrebbero essere utili gli URL accorciati. **Dr.Web** consente di accorciare link e di controllarne i contenuti tramite un servizio speciale di accorciamento URL così difendendo gli utenti da minacce informatiche.

Utilizzo del servizio accorciamento URL

Per controllare e accorciare un URL:

1. Selezionare l'URL che si desidera controllare e accorciare e quindi utilizzare la funzione del browser che consente di condividere un link.
2. Dal menu che si è aperto, selezionare la voce **Accorcia URL**. La pagina situata all'indirizzo indicato viene controllata alla ricerca di minacce informatiche e se è sicura, l'URL viene accorciato e aggiunto agli appunti. Se la pagina contiene minacce alla sicurezza, il servizio restituisce un avviso corrispondente.

Capitolo 6. Funzionamento nella modalità di protezione centralizzata

Se **Dr.Web** è stato installato dal sito web di **Doctor Web**, il programma può essere usato in una rete di protezione centralizzata, organizzata tramite il **Pannello di controllo Dr.Web**, oppure può essere collegato al servizio antivirale **Dr.Web AV-Desk** se fornito dall'Internet Service Provider. Per mettere la protezione antivirale nella modalità centralizzata non è richiesto di installate altri moduli di software o rimuovere **Dr.Web**.

Per la versione **Dr.Web** installata da Google Play, non è prevista la possibilità di utilizzo nella modalità di protezione centralizzata.

Componenti controllati dal server di protezione centralizzata

Le impostazioni dei componenti di **Dr.Web** potrebbero essere cambiate o bloccate a seconda dei criteri di sicurezza aziendali o della lista dei servizi pagati.

Dal server di protezione centralizzata possono essere controllati i seguenti componenti di **Dr.Web**:

- Scanner Dr.Web. Scansione del dispositivo on demand e secondo un calendario. Inoltre, è supportata la possibilità di avviare una scansione antivirus delle postazioni su remoto dal server di protezione centralizzata;
- SpIDer Guard;
- Filtraggio di chiamate e di messaggi;
- Antifurto Dr.Web;
- Cloud Checker;
- Filtro delle applicazioni.

Concessione di licenze nella modalità di protezione centralizzata

Il file della chiave necessario per il funzionamento in questa modalità si riceve automaticamente dal server di protezione centralizzata, mentre la chiave di licenza personale non si usa. Se la licenza è scaduta o è stata bloccata ed è comparso un avviso corrispondente, contattare l'amministratore della rete antivirus aziendale per ottenere una nuova licenza, o rinnovare l'abbonamento al servizio **Dr.Web AV-Desk**.

Aggiornamento nella modalità di protezione centralizzata

Nella modalità di protezione centralizzata, è bloccata la possibilità di avvio manuale di aggiornamento, gli aggiornamenti vengono caricati automaticamente dal server di protezione centralizzata. Le impostazioni di aggiornamento potrebbero essere cambiate o bloccate a seconda dei criteri di sicurezza aziendali o della lista dei servizi pagati. Se sul server di protezione centralizzata è consentito l'avvio di applicazione in modalità mobile, in caso di una rottura della connessione con il server di protezione centralizzata, l'aggiornamento dei database dei virus può essere avviato manualmente.

Passaggio alla modalità di protezione centralizzata

Per iniziare a utilizzare la modalità di protezione centralizzata, è necessario connettersi al server di protezione centralizzata.

Aggiornamento automatico

Se **Dr.Web** è stato installato tramite l'installer fornito dall'amministratore della rete antivirus, si

connette automaticamente al server di protezione centralizzata. A tale scopo è necessario che il dispositivo si trovi nella stessa rete Wi-Fi del server di protezione centralizzata.

Connessione con l'inserimento di parametri

Per connettersi al server di protezione centralizzata, occorrono parametri di connessione che vengono forniti dall'amministratore della rete antivirus aziendale o dal fornitore di servizi IT.

Eseguire le seguenti azioni:

1. Assicurarsi della disponibilità di una connessione alla rete.
2. Sulla schermata delle impostazioni (v. Immagine 6) nella sezione **Modalità** spuntare il flag **Agent Dr.Web**.

Nell'applicazione installata tramite l'installer fornito dall'amministratore della rete antivirus, il flag **Agent Dr.Web** è selezionato di default.

3. Quando si attiva la modalità di protezione centralizzata, vengono ripristinati gli ultimi parametri di connessione al server. Se si connette al server per la prima volta o se i parametri di connessione sono cambiati, è necessario indicare i seguenti parametri:
   - l'indirizzo IP del server di protezione centralizzata, fornito dall'amministratore della rete antivirus;
   - parametri addizionali per l'autenticazione della postazione: l'identificatore (attribuito al dispositivo mobile per la registrazione sul server) e la password. I valori indicati dei parametri vengono salvati e quando si riconnette al server, non sarà necessario inserirli di nuovo. Per connettersi come una nuova postazione ("Nuovo arrivo"), richiamare il menu dell'applicazione e selezionare l'opzione **Connessione della postazione come "Nuovo arrivo"**.
4. Premere sul pulsante **Connettiti**.

Connessione con il file di configurazione

Le impostazioni di connessione a server di protezione centralizzata sono contenute nel file install.cfg che viene fornito dall'amministratore della rete antivirus aziendale o dal fornitore di servizi IT.

Eseguire le seguenti azioni:

1. Assicurarsi della disponibilità di una connessione alla rete.
2. Mettere il file install.cfg nella cartella radice o in qualsiasi delle cartelle di primo livello di nidificazione sulla scheda SD o nella memoria interna del dispositivo.
3. Sulla schermata delle impostazioni (v. Immagine 6) nella sezione **Modalità** spuntare il flag **Agent Dr.Web**. Se il file è stato caricato sul dispositivo, i campi di inserimento di parametri di connessione a server vengono compilati in automatico.

Nell'applicazione installata tramite l'installer fornito dall'amministratore della rete antivirus, il flag **Agent Dr.Web** è selezionato di default. L'applicazione inizia a cercare il file di configurazione e a tentare di connettersi al server subito dopo l'installazione. Se il file non è stato trovato o se esso contiene parametri di connessione non validi, è necessario togliere e mettere nuovamente il flag **Agent Dr.Web** ed inserire i parametri manualmente oppure utilizzare un file di configurazione con le impostazioni corrette.

4. Premere sul pulsante **Connettiti**.

Reset dei parametri di connessione

Per resettare i parametri di connessione:

1. Aprire il menu dell'applicazione sulla schermata di inserimento di parametri di connessione.
2. Selezionare l'opzione **Resetta i parametri di connessione**.

Dopo il reset dei parametri, il file install.cfg, che contiene i parametri di connessione in uso, verrà

cancellato. Se sul dispositivo è disponibile un altro file install.cfg, verranno utilizzati i parametri di connessione da questo file. Cioè, i parametri di connessione verranno resettati soltanto dopo che verranno cancellati tutti i file install.cfg.

Errori di connessione

Opzione non supportata. L'errore si verifica se sul server sono attivate le opzioni di cifratura e/o compressione di traffico dati, non supportate da **Dr.Web**. Contattare l'amministratore della rete antivirus o il fornitore di servizi IT per risolvere il problema.

È scaduta la licenza (l'abbonamento). Per connettersi al server di protezione centralizzata, contattare l'amministratore della rete antivirus per ottenere una licenza, o rinnovare l'abbonamento al servizio **Dr.Web AV-Desk**.

L'abbonamento è bloccato. Per connettersi al server di protezione centralizzata, contattare il fornitore di servizi IP, che fornisce il servizio **Dr.Web AV-Desk**, per sbloccare l'abbonamento.

Connessione non stabilita. L'esecuzione di Dr.Web per Android è proibita sul server di protezione centralizzata.L'errore si verifica se il piano tariffario non prevede l'uso di **Dr.Web** per Android o l'esecuzione di **Dr.Web** per Android è proibitadall'amministratore della rete antivirus.

Filtro delle applicazioni

Se sul server di protezione centralizzata è attivata la possibilità di configurare il filtro delle applicazioni, è possibile configurare una lista delle applicazioni che possono essere eseguite sul dispositivo. Per farlo, eseguire le seguenti azioni:

1. Sulla schermata principale dell'applicazione aprire la sezione **Amministratore**.
2. Selezionare le applicazioni che saranno disponibili sul dispositivo.
3. Premere sul pulsante **Consenti quelle selezionate**. Le impostazioni configurate verranno trasmesse sul server e salvate come le impostazioni individuali del dispositivo.

Se si è amministratori della rete antivirus, sul server di protezione centralizzata si possono configurare liste delle applicazioni disponibili per tutti i dispositivi nella rete sulla base delle proprie impostazioni individuali salvate sul server.

Passaggio alla modalità autonoma

Per passare alla modalità autonoma del funzionamento di **Dr.Web**, togliere il flag **Agent Dr.Web** sulla schermata delle impostazioni (v. Immagine 6) nella sezione **Modalità**.

Con l'attivazione della modalità autonoma, si ripristinano tutte le impostazioni dell'antivirus definite prima del passaggio alla modalità centralizzata oppure le impostazioni predefinite. Inoltre, si recupera l'accesso a tutte le funzioni di **Dr.Web**.

Per funzionare nella modalità autonoma, l'antivirus richiede una licenza personale valida. In questa modalità non si può usare la licenza ricevuta automaticamente dal server di protezione centralizzata. Se necessario, ottenere o aggiornare una licenza personale.

Capitolo 7. Utilizzo di Dr.Web su Android TV

Sui dispositivi gestiti da Android TV, sono disponibili le seguenti possibilità di **Dr.Web**:

- Protezione continua da virus
- Scansione a richiestadell'utente
- Aggiornamento
- Statistiche
- Quarantena
- Aiuto nella risoluzione dei problemi di sicurezza

Immagine 20. Dr.Web per Android TV

Caratteristiche dell'utilizzo di Dr.Web sui dispositivi sulla base di Android TV

Concessione di licenze

- Non è disponibile la possibilità di acquisto di una licenza direttamente dall'applicazione.
- Per aggiornare la licenza, è necessario passare alla sezione **Dr.Web** e premere il pulsante **Rinnova la licenza**.

Interfaccia

- Non è possibile creare dei widget per il desktop.
- Non è disponibile la barra delle notifiche.
- Non è disponibile il menu dell'applicazione e, di conseguenza, non sono disponibili le impostazioni dei componenti di **Dr.Web**.

Allegati

Questa sezione contiene le informazioni addizionali su utilizzo di **Dr.Web**:

Allegato A. Supporto tecnico

In caso di problemi con l'installazione e il funzionamento dei prodotti della società, prima di rivolgersi al supporto tecnico per l'assistenza, si prega calorosamente di cercare la soluzione in uno dei seguenti modi:

- leggere le ultime versioni della documentazione e delle guide che si trovano all'indirizzo http://download.drweb.com/doc/;
- leggere la sezione FAQ all'indirizzo http://support.drweb.com/show_faq/;
- visitare i forum **Dr.Web** all'indirizzo http://forum.drweb.com/;
- fare una domanda oppure leggere la lista delle domande ricorrenti sulla pagina personale Mio Dr.Web.

Se consultando queste risorse non si è riusciti a risolvere il problema, si prega di compilare il modulo web di richiesta nella sezione opportuna http://support.drweb.com/.

Per trovare la rappresentanza più vicina di **Doctor Web** e tutti i riferimenti requisiti, rivolgersi all'indirizzo http://company.drweb.com/contacts/moscow.

Indice analitico

Indice analitico

Indice analitico