Dr.WEB

Mobile Security Suite (Android)

Manuale dell'utente

Dr.Web Mobile Security Suite (Android)
Versione 12.9
Manuale dell'utente
08/11/2024

Doctor Web, Sede centrale in Russia

Indirizzo: 125124, Russia, Mosca, 3a via Yamskogo polya, 2, 12A

Sito web: https://www.drweb.com/

Telefono +7 (495) 789-45-87

Le informazioni sulle rappresentanze regionali e sedi sono ritrovabili sul sito ufficiale della società.

Doctor Web

Doctor Web — uno sviluppatore russo di strumenti di sicurezza delle informazioni.

Doctor Web offre efficaci soluzioni antivirus e antispam sia ad enti statali e grandi aziende che ad utenti privati.

Le soluzioni antivirus Dr.Web esistono a partire dal 1992 e dimostrano immancabilmente eccellenza nel rilevamento di programmi malevoli, soddisfano gli standard di sicurezza internazionali.

I certificati e premi, nonché la vasta geografia degli utenti testimoniano la fiducia eccezionale nei prodotti dell'azienda.

Siamo grati a tutti i nostri clienti per il loro sostegno delle soluzioni Dr.Web!

Sommario

1. Introduzione

Dr.Web Mobile Security Suite (di seguito — Dr.Web) protegge i dispositivi mobili con il sistema operativo Android™, nonché i televisori, i lettori multimediali e le console videogiochi sulla piattaforma Android TV™ dalle minacce di virus create appositamente per questi dispositivi.

> Sui dispositivi con Android TV la modalità di protezione centralizzata non è disponibile. Per controllare se il dispositivo e la versione dell'applicazione Dr.Web in uso supportano il funzionamento in modalità di protezione centralizzata, v. la sezione Modalità di protezione centralizzata.

Nell'applicazione sono utilizzate le progettazioni e tecnologie di Doctor Web per il rilevamento e la neutralizzazione di oggetti malevoli che rappresentano un rischio per la sicurezza informatica del dispositivo e possono influenzare il suo funzionamento.

Dr.Web utilizza la tecnologia Origins Tracing™ for Android che trova programmi malevoli per la piattaforma Android. Questa tecnologia consente di individuare nuove famiglie di virus sulla base delle conoscenze sulle minacce già trovate ed esaminate. Origins Tracing™ for Android è in grado di riconoscere sia i virus ricompilati, per esempio Android.SmsSend, Spy che le applicazioni infettate da Android.ADRD, Android.Geinimi, Android.DreamExploid. I nomi delle minacce rilevate tramite Origins Tracing™ for Android hanno l'aspetto «Android.*VirusName*.origin».

Informazioni sul manuale

Il manuale ha lo scopo di aiutare gli utenti dei dispositivi mobili con sistema operativo Android a installare e configurare l'applicazione, nonché a scoprire le sue funzioni principali.

In questo manuale vengono utilizzati i seguenti simboli:

Simbolo	Commento
⚠	Avviso di possibili situazioni di errore, nonché di punti importanti cui prestare particolare attenzione.
Rete antivirus	Un nuovo termine o un termine accentato nelle descrizioni.
<*indirizzo_IP*>	Campi in cui nomi di funzione vanno sostituiti con valori effettivi.
Salva	Nomi dei pulsanti di schermo, delle finestre, delle voci di menu e di altri elementi dell'interfaccia del programma.
CTRL	Nomi dei tasti della tastiera.
`Internal`	Nomi di file e directory, frammenti di codice.

Simbolo	Commento
`storage/Android/`	
Allegato A	Riferimenti incrociati ai capitoli del documento o collegamenti ipertestuali a risorse esterne.

1.1. Funzioni di Dr.Web

Dr.Web esegue le seguenti funzioni:

- Protegge in tempo reale il file system del dispositivo (verifica file che vengono salvati, le applicazioni che vengono installate ecc.).
- Verifica tutti i file in memoria o singoli file e cartelle a richiesta dell'utente.
- Verifica archivi.
- Verifica la scheda SD o un altro supporto rimovibile.
- Tiene traccia di modifiche nell'area di sistema.
- Rimuove le minacce alla sicurezza rilevate o le sposta in quarantena.
- Sblocca il dispositivo se è stato bloccato da un programma ransomware.
- Filtra le chiamate e i messaggi SMS in arrivo (il filtraggio di messaggi SMS non è disponibile nelle versioni dell'applicazione installate da Google Play).
- Aggiorna a cadenza regolare i database dei virus Dr.Web attraverso internet.
- Registra statistiche delle minacce rilevate e delle azioni dell'applicazione e inoltre il log degli eventi.
- Cerca e blocca in remoto il dispositivo in caso di smarrimento o furto.
- Limita l'accesso ai siti selezionati, nonché alle categorie di siti nel browser standard di Android, in Google Chrome, Yandex.Browser, Microsoft Edge, Firefox, Firefox Focus, Opera, Adblock Browser, Dolphin Browser, Sputnik, Boat Browser e Atom.
- Trova problemi di sicurezza e vulnerabilità e aiuta a risolverli.
- Controlla le connessioni internet, protegge il dispositivo da accessi non autorizzati dall'esterno e previene fughe di dati importanti attraverso la rete.
- Aiuta a limitare l'accesso alle applicazioni installate sul dispositivo.
- Permette di attivare il filtro famiglia per la maggior parte dei motori di ricerca popolari.

Alcune delle funzioni elencate non sono disponibili quando l'applicazione è utilizzata sulla piattaforma Android TV.

2. Requisiti di sistema

Prima dell'installazione verificare che il dispositivo soddisfi i seguenti requisiti e raccomandazioni:

Parametro	Requisito
Sistema operativo	Android versione 4.4 - 15.0 Android TV (su televisori, lettori multimediali e console per videogiochi)
Processore	x86/x86-64/ARMv7/ARMv8/ARMv9
Memoria operativa libera	Almeno 512 MB
Spazio su disco rigido	Almeno 45 MB (per la conservazione dei dati)
Risoluzione schermo	Risoluzione minima 800×480
Altro	Connessione internet (per l'aggiornamento dei database dei virus). Su dispositivi Android TV la modalità di protezione centralizzata non è disponibile

- Per l'uso congiunto con le applicazioni che bloccano l'avvio di altre applicazioni è necessario che queste applicazione di blocco non limitino l'avvio di Dr.Web.
- Se si usa un tablet, per il filtraggio di chiamate e messaggi e per il funzionamento di Antifurto Dr.Web è necessaria la possibilità di installare e utilizzare una SIM.
- Il filtro URL funziona nel browser incorporato di Android, in Google Chrome, Yandex.Browser, Microsoft Edge, Firefox, Firefox Focus, Opera, Adblock Browser, Dolphin Browser, Sputnik, Boat Browser e Atom.
- Sui dispositivi con Android 5.1 o versioni precedenti per il corretto funzionamento del filtro URL è necessario che per il browser in uso sia attivata la funzione di salvataggio della cronologia.

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

Di default l'applicazione viene installata nella memoria interna del dispositivo. Per il corretto funzionamento di Dr.Web l'applicazione installata non dovrebbe essere trasferita su supporti rimovibili.

3. Installazione di Dr.Web Mobile Security Suite

Dr.Web può essere installato:

- Dal disco con licenza.
- Dal sito dell'azienda Doctor Web.
- Da Google Play.
- Da HUAWEI AppGallery.
- Da Xiaomi GetApps.
- Tramite un programma di sincronizzazione con il computer.

Installazione dal disco con licenza

Su alcuni dispositivi al collegamento al computer tramite il cavo USB è necessario consentire il trasferimento dei file.

Per installare Dr.Web, attivare la seguente impostazione di sistema:

- Sui dispositivi con Android 7.1 o versioni precedenti:
  1. Nelle impostazioni del dispositivo aprire la schermata **Sicurezza**.
  2. Spuntare il flag **Origini sconosciute**.
- Sui dispositivi con Android 8.0 o versioni successive:
  1. Nelle impostazioni del dispositivo aprire la schermata **Installazione di applicazioni sconosciute**.
  2. Consentire l'installazione di applicazioni dalla fonte selezionata.

Copiatura del file di installazione dal disco e avvio sul dispositivo

1. Inserire il disco nell'unità.
2. Copiare il file di installazione dal disco al computer.
3. Collegare il dispositivo mobile al computer tramite un cavo USB.
4. Trascinare il file di installazione nella finestra che si è aperta.
5. Scollegare il dispositivo mobile dal computer e scollegare il cavo.
6. Sul dispositivo mobile tramite il file manager trovare ed eseguire il file di installazione.
7. Nella finestra che si è aperta premere il pulsante **Installa**.
8. Premere **Apri** per iniziare a utilizzare l'applicazione.

   Premere **Finito** per chiudere la finestra di installazione e iniziare a utilizzare l'applicazione più tardi.

Per continuare ad usare l'applicazione, è necessario attivare una licenza commerciale o di prova.

Dopo aver installato l'applicazione:

- Sui dispositivi con Android 7.1 o versioni precedenti disattivare nelle impostazioni del dispositivo l'impostazione **Fonti sconosciute**.
- Sui dispositivi con Android 8.0 o versioni successive aprire nelle impostazioni del dispositivo la schermata **Installazione di applicazioni sconosciute** e vietare l'installazione di applicazioni dalla fonte selezionata.

Installazione dal sito dell'azienda Doctor Web

Per installare Dr.Web, attivare la seguente impostazione di sistema:

- Sui dispositivi con Android 7.1 o versioni precedenti:
  1. Nelle impostazioni del dispositivo aprire la schermata **Sicurezza**.
  2. Spuntare il flag **Origini sconosciute**.
- Sui dispositivi con Android 8.0 o versioni successive:
  1. Nelle impostazioni del dispositivo aprire la schermata **Installazione di applicazioni sconosciute**.
  2. Consentire l'installazione di applicazioni dalla fonte selezionata.

Il file di installazione Dr.Web può essere scaricato sul sito dell'azienda Doctor Web sull'indirizzo https://download.drweb.com/android/.

Avvio del file di installazione sul dispositivo

1. Copiare il file di installazione sulla scheda di memoria.
2. Utilizzando il file manager, trovare ed eseguire il file di installazione.
3. Nella finestra che si è aperta premere il pulsante **Installa**.
4. Premere **Apri** per iniziare a utilizzare l'applicazione.

   Premere **Finito** per chiudere la finestra di installazione e iniziare a utilizzare l'applicazione più tardi.

Per continuare ad usare l'applicazione, è necessario attivare una licenza commerciale o di prova.

Dopo aver installato l'applicazione:

- Sui dispositivi con Android 7.1 o versioni precedenti disattivare nelle impostazioni del dispositivo l'impostazione **Fonti sconosciute**.
- Sui dispositivi con Android 8.0 o versioni successive aprire nelle impostazioni del dispositivo la schermata **Installazione di applicazioni sconosciute** e vietare l'installazione di applicazioni dalla fonte selezionata.

Installazione da Google Play

Per installare Dr.Web da Google Play, assicurarsi che:

- Si abbia un account Google.
- Il dispositivo sia associato all'account Google.
- Sul dispositivo sia disponibile l'accesso a internet.
- Il dispositivo soddisfi i requisiti di sistema.

Per installare l'applicazione

1. Aprire Google Play sul dispositivo, trovare Dr.Web nella lista delle applicazioni e premere il pulsante **Installa**.

   

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

2. In seguito si apre una schermata con informazioni sulle funzioni del dispositivo l'accesso a cui è richiesto per il funzionamento dell'applicazione.

   Leggere la lista dei permessi richiesti e premere **Accetta**.
3. Per iniziare a usare l'applicazione, premere il pulsante **Apri**.

Per continuare ad usare l'applicazione, è necessario attivare una licenza commerciale o di prova.

Installazione da HUAWEI AppGallery

Per installare Dr.Web da HUAWEI AppGallery, assicurarsi che:

- Si abbia un account Huawei.
- Il dispositivo sia associato all'account Huawei.
- Sul dispositivo sia disponibile l'accesso a internet.
- Il dispositivo soddisfi i requisiti di sistema.

Per installare l'applicazione

1. Aprire HUAWEI AppGallery sul dispositivo, trovare nella lista delle applicazioni Dr.Web e premere il pulsante **Installa**.

   

   Se Dr.Web non viene visualizzato in HUAWEI AppGallery, il dispositivo non soddisfa i requisiti di sistema.

2. In seguito si apre una schermata con informazioni sulle funzioni del dispositivo l'accesso a cui è richiesto per il funzionamento dell'applicazione.

Leggere la lista dei permessi richiesti e premere **Accetta**.

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

Per continuare ad usare l'applicazione, è necessario attivare una licenza commerciale o di prova.

Installazione da Xiaomi GetApps

Per installare Dr.Web da Xiaomi GetApps, assicurarsi che:

- Si abbia un account Xiaomi.
- Il dispositivo sia associato all'account Xiaomi.
- Sul dispositivo sia disponibile l'accesso a internet.
- Il dispositivo soddisfi i requisiti di sistema.

Per installare l'applicazione

1. Aprire Xiaomi GetApps sul dispositivo, trovare Dr.Web nella lista delle applicazioni e premere il pulsante **Ottieni**.

   

   Se Dr.Web non viene visualizzato in Xiaomi GetApps, il dispositivo non soddisfa i requisiti di sistema.

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

Installazione tramite un programma di sincronizzazione

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

1. Sincronizzare il dispositivo mobile con un computer.
2. Avviare la procedura guidata di installazione di applicazioni 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 dove sarà possibile visualizzare le relative informazioni e confermare l'installazione. Dopo la conferma l'applicazione verrà installata automaticamente.
5. Chiudere l'installazione guidata del programma di sincronizzazione.

Dr.Web è stato installato ed è pronto per l'uso. Per continuare ad usare l'applicazione, è necessario attivare una licenza commerciale o di prova.

4. Aggiornamento e rimozione di Dr.Web Mobile Security Suite

Aggiornamento di Dr.Web

Configurazione di aggiornamento automatico per la versione dal sito Doctor Web

Se la versione Dr.Web in uso è stata scaricata dal sito dell'azienda Doctor Web, è possibile attivare gli avvisi di disponibilità della nuova versione. Per questo scopo:

1. Sulla schermata principale di Dr.Web premere **Menu** e selezionare la voce **Impostazioni**.
2. Sulla schermata **Impostazioni** selezionare **Aggiornamento dei database dei virus**.
3. Sulla schermata **Aggiornamento dei database dei virus** spuntare la casella **Nuova versione**.

Se questo flag è spuntato, Dr.Web verifica la disponibilità di una nuova versione dell'applicazione ad ogni aggiornamento dei database dei virus. Quando compare una nuova versione dell'applicazione, si riceverà un avviso e si potrà scaricarla prontamente e installarla.

Aggiornamento attraverso Google Play in maniera manuale

Se per le applicazioni da Google Play non è configurato l'aggiornamento automatico, è possibile avviare l'aggiornamento in maniera manuale:

1. Aprire l'applicazione **Play Store**.
2. Premere l'icona del proprio profilo Google nell'angolo superiore destro dello schermo.
3. Selezionare la voce **Gestisci app e dispositivo**.
4. Passare alla scheda **Gestisci**.
5. Premere la lista **Aggiornamenti disponibili** ed eseguire una delle azioni:
   - Selezionare **Dr.Web** e premere **Aggiorna**.
   - Spuntare il flag di fronte a **Dr.Web** e premere l'icona .

   L'applicazione si trova nella lista **Aggiornamenti disponibili** se è già stata rilasciata una nuova versione dell'applicazione.
6. Quando viene aggiornata, l'applicazione potrebbe richiedere nuovi permessi. In questo caso si aprirà una finestra per la conferma.

   Premere il pulsante **Accetta** per consentire l'accesso alle funzioni del dispositivo necessarie per l'applicazione.

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

Aggiornamento attraverso HUAWEI AppGallery

È possibile configurare l'aggiornamento automatico delle applicazioni installate da HUAWEI AppGallery, tra cui anche di Dr.Web. Per questo scopo, nell'applicazione HUAWEI AppGallery nella scheda **Gestisci** utilizzare l'interruttore **Aggiornamento automatico tramite Wi-Fi**.

L'aggiornamento può anche essere avviato manualmente:

1. Aprire l'applicazione **HUAWEI AppGallery** e premere **Gestisci**.
2. Nella lista delle applicazioni installate trovare Dr.Web e premere **Aggiorna**.

Il pulsante **Aggiorna** è disponibile se una nuova versione dell'applicazione è già stata rilasciata.

3. Quando viene aggiornata, l'applicazione potrebbe richiedere nuovi permessi. In questo caso si aprirà una finestra per la conferma.

   Premere il pulsante **Accetta** per consentire l'accesso alle funzioni del dispositivo necessarie per l'applicazione.

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

Rimozione di Dr.Web

Antifurto Dr.Web rende difficile la rimozione dell'applicazione Dr.Web dal dispositivo. Se Antifurto è configurato, disattivarlo ed escludere Dr.Web dagli amministratori del dispositivo prima di rimuovere l'applicazione.

Per rimuovere Dr.Web

1. Nelle impostazioni del dispositivo selezionare **Applicazioni** o **Gestione delle applicazioni**.
2. Nell'elenco delle applicazioni installate selezionare **Dr.Web** e premere **Elimina**.

La cartella quarantena e i file di log non vengono rimossi in maniera automatica. È possibile rimuoverli manualmente dalla cartella `Android/data/com.drweb/files` nella memoria interna del dispositivo.

Sui dispositivi con Android 11.0 o versioni successive i log vengono salvati nella cartella `Download/DrWeb`.

Gestione di Dr.Web attraverso HUAWEI AppGallery

Se Dr.Web è stato installato da HUAWEI AppGallery, l'applicazione può essere disinstallata seguendo questi passaggi:

1. Aprire l'applicazione HUAWEI AppGallery.
2. Premere **Gestisci**.
3. Sulla schermata che si è aperta premere **Gestione installazione**.
4. Nell'elenco delle applicazioni installate selezionare Dr.Web e premere **Elimina**.
5. Confermare l'azione.

5. Concessione di licenze

La licenza consente di utilizzare le funzionalità dell'applicazione durante l'intero periodo di validità e regola i diritti dell'utente stabiliti in conformità al contratto d'uso.

La licenza è richiesta per il funzionamento di tutti i componenti di Dr.Web nelle seguenti versioni dell'applicazione:

- Le versioni scaricate dall'area personale del fornitore del servizio "Antivirus Dr.Web".
- Le versioni fornite dall'amministratore della rete antivirus aziendale dell'utente.
- Per i dispositivi con Android TV.

La licenza è richiesta per il funzionamento di tutti i componenti tranne SpIDer Guard, Scanner e Auditor di sicurezza nelle seguenti versioni dell'applicazione:

- Le versioni scaricate dal sito dell'azienda Doctor Web https://download.drweb.com/android/.
- Nella versione di Dr.Web installata da Google Play.
- Nella versione installata da HUAWEI AppGallery.

Se prima di acquistare una licenza si vuole provare il prodotto, è possibile attivare una licenza di prova.

Se si ha già una licenza valida dei prodotti software Dr.Web Security Space o Antivirus Dr.Web (forniti in confezione o in forma di licenza elettronica), è possibile attivare tale licenza.

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

5.1. Schermata Licenza

Sulla schermata **Licenza** (vedi Immagine 1) è possibile acquistare o attivare una licenza commerciale, e inoltre ottenere una licenza di prova.

Per passare alla schermata **Licenza**, aprire l'applicazione ed eseguire una delle seguenti azioni:

- Nelle versioni di Dr.Web che richiedono la licenza per il funzionamento di tutti i componenti:
  - Premere **Più nel dettaglio** nell'avviso di assenza della licenza nella parte superiore della schermata principale di Dr.Web.
  - Sulla schermata principale di Dr.Web premere **Menu** e selezionare la voce **Licenza**.
- Nelle versioni di Dr.Web che richiedono la licenza per il funzionamento di alcuni componenti:
  - Sulla schermata principale di Dr.Web selezionare uno dei componenti che richiedono l'acquisto della licenza.
  - Sulla schermata principale di Dr.Web premere **Menu** e selezionare la voce **Licenza**.

Immagine 1. Schermata Licenza

5.2. Licenza di prova

Se si desidera conoscere le funzionalità dell'applicazione prima di acquistare una licenza, è possibile attivare una licenza di prova per 14 giorni.

Per attivare una licenza di prova

1. Aprire l'applicazione.
2. Andare alla schermata Licenza.
3. Selezionare **Ottieni una versione di prova per 14 giorni**.
4. Indicare i dati personali (vedi Immagine 2):
   - Nome e cognome.
   - Un indirizzo email valido.
   - Paese.
5. Se lo si desidera, spuntare il flag **Ricevi notizie via email**.

   A questo passaggio l'applicazione può chiedere l'accesso ai contatti. Se si consente l'accesso, i campi **Indirizzo email** e **Paese** verranno compilati automaticamente. Se si rifiuta la richiesta, sarà necessario compilare i campi manualmente.
6. Premere **Ottieni versione di prova**. Una licenza di prova verrà attivata.

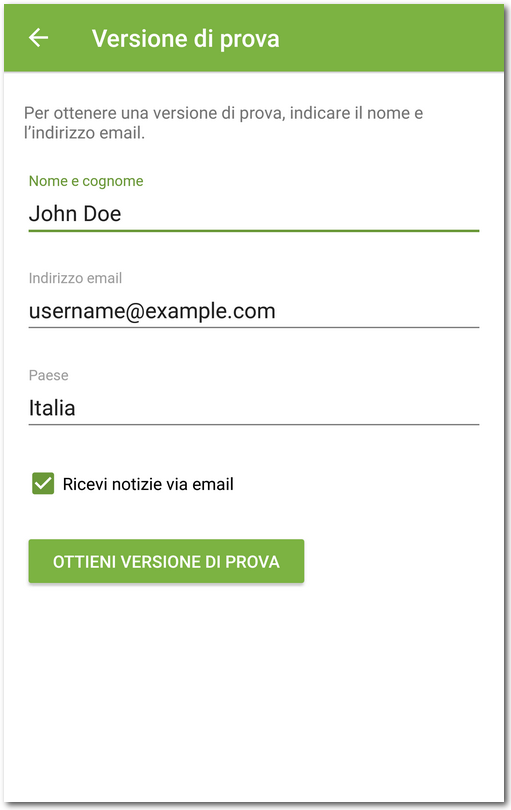

Immagine 2. Ottenimento della licenza di prova

5.3. Acquisto della licenza

Se l'applicazione è stata installata da Google Play

1. Aprire l'applicazione.
2. Andare alla schermata Licenza.
3. Selezionare **Acquista licenza**.

   Se non si ha un account Google, indicare un indirizzo email su cui verrà registrata la licenza. Nel caso di reinstallazione dell'applicazione o installazione su un altro dispositivo si può ripristinare la licenza utilizzando questo indirizzo.

   A questo passaggio l'applicazione può chiedere l'accesso ai contatti. Se si consente l'accesso, il campo con l'indirizzo email verrà compilato automaticamente. Se si nega l'accesso, sarà necessario immettere l'indirizzo manualmente.
4. Sulla schermata **Acquisto della licenza** (v. Immagine 3) selezionare una delle seguenti varianti:
   - **Abbonamento mensile**. L'abbonamento mensile consente di utilizzare la licenza per un mese dalla data di pagamento dell'abbonamento. Successivamente, l'abbonamento viene automaticamente rinnovato e pagato una volta al mese.
   - **Licenza di 1 anno**. La licenza è valida per un anno dalla data di acquisto della licenza.

- **Licenza di 2 anni**. La licenza è valida per due anni dalla data di acquisto della licenza.

Alla selezione di una qualsiasi delle varianti si aprirà la schermata di acquisto della licenza. Qualche tempo dopo l'effettuazione del pagamento la licenza verrà attivata automaticamente.

Come conferma dell'acquisto di una licenza di 1 o 2 anni all'indirizzo email dell'utente verrà inviato un file della chiave di licenza. Se a causa di possibili problemi tecnici la licenza non viene attivata, contattare il servizio di supporto tecnico: https://support.drweb.com/.

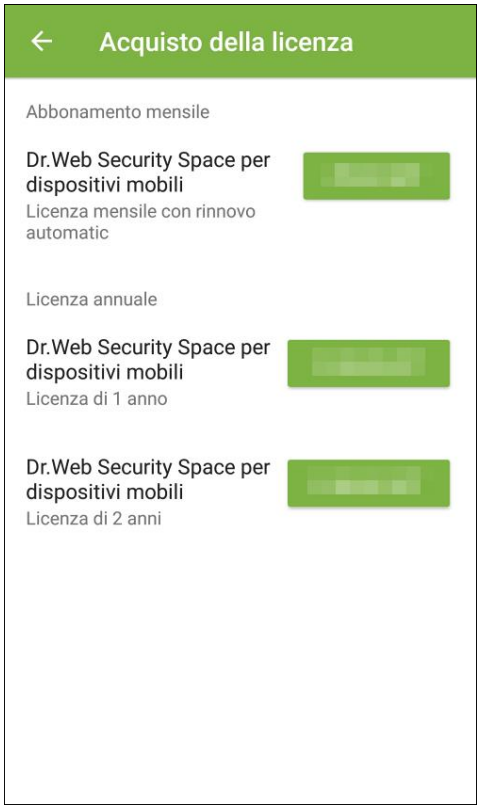

Immagine 3. Acquisto della licenza

Se l'applicazione è stata installata dal sito dell'azienda Doctor Web o da Xiaomi GetApps

1. Aprire l'applicazione.
2. Andare alla schermata Licenza.
3. Selezionare **Acquista licenza**. Si apre una pagina del negozio online Doctor Web.

   È inoltre possibile andare al negozio tramite il link https://estore.drweb.com/mobile/.
4. Scegliere la durata della licenza e il numero di dispositivi da proteggere.
5. Premere **Acquista**.
6. Compilare il modulo di acquisto e premere **Fai l'ordine**.

   Dopo che l'ordine viene fatto, un numero di serie viene inviato sull'indirizzo email specificato durante l'acquisto. Inoltre, si può scegliere la variante di ricezione del numero di serie in un SMS sul numero di telefono specificato.

7. Registrare il numero di serie ricevuto.

Se l'applicazione è stata installata da HUAWEI AppGallery

1. Aprire l'applicazione.
2. Andare alla schermata Licenza.
3. Selezionare **Acquista licenza**.

   Creare un account Huawei o accedere a uno esistente. Dopo aver effettuato l'accesso all'account, concedere all'applicazione i permessi necessari.

   A questo passaggio l'applicazione può chiedere l'accesso ai dati dell'account Huawei. Se si consente l'accesso, il campo con l'indirizzo email verrà compilato automaticamente. Se si nega l'accesso, verrà chiesto di selezionare l'indirizzo dalla lista in una finestra a comparsa.
4. Sulla schermata **Acquista licenza** selezionare una delle seguenti varianti:
   - **Licenza di 1 anno**
   - **Licenza di 2 anni**

   Quando si sceglie una delle varianti, si apre la schermata di acquisto della licenza. Qualche tempo dopo il pagamento, la licenza viene attivata automaticamente. Come conferma dell'acquisto, un file della chiave di licenza viene inviato sull'indirizzo email dell'utente. Se a causa di possibili errori tecnici la licenza non viene attivata, contattare il servizio di supporto tecnico: https://support.drweb.com/.

5.4. Attivazione della licenza

L'attivazione di una licenza è necessaria se l'applicazione è stata installata dal sito dell'azienda Doctor Web. L'attivazione può inoltre essere necessaria se si possiede già una licenza valida dei prodotti software Dr.Web, che include Dr.Web Mobile Security Suite.

A partire dal 01.09.2024 Dr.Web Mobile Security Suite non è più incluso nelle licenze dei prodotti software Dr.Web per PC. Se tale licenza è stata acquistata dopo il 31.08.2024, per utilizzare Dr.Web Mobile Security Suite, sarà necessario acquistare una licenza separata.

Per attivare la licenza

- Registrare il numero di serie:
  - Nell'applicazione, se sul dispositivo con l'applicazione installata c'è una connessione internet attiva.
  - Sul sito Doctor Web, se sul dispositivo con l'applicazione installata non c'è connessione internet.
- Utilizzare il file della chiave (solo per l'applicazione installata dal sito Doctor Web).

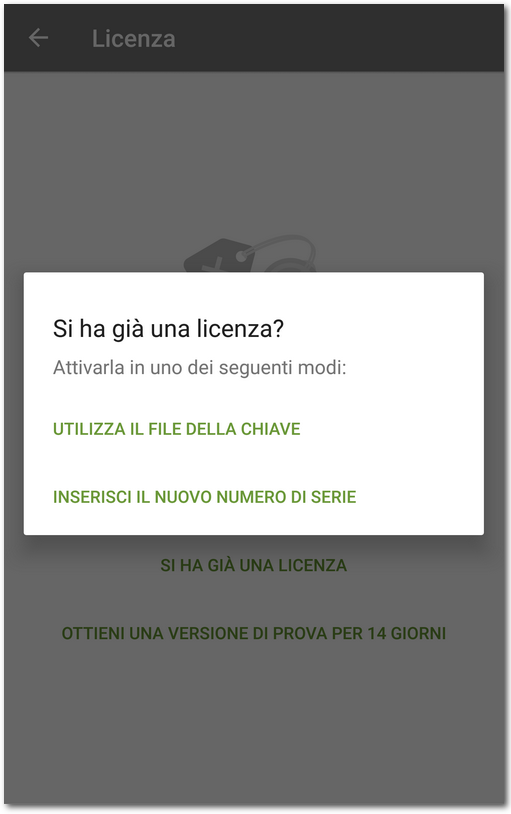

Immagine 4. Attivazione della licenza

Registrazione del numero di serie nell'applicazione

Per registrare il numero di serie e attivare la licenza nell'applicazione

1. Aprire l'applicazione.
2. Andare alla schermata Licenza.
3. Selezionare la voce **Si ha già una licenza**.
4. Nella finestra successiva (vedi Immagine 4) premere **Inserisci il nuovo numero di serie**.
5. Nella schermata **Attivazione della licenza** (vedi Immagine 5) immettere il numero di serie che si è ottenuto dopo l'acquisto.
6. Premere il pulsante **Attiva**.

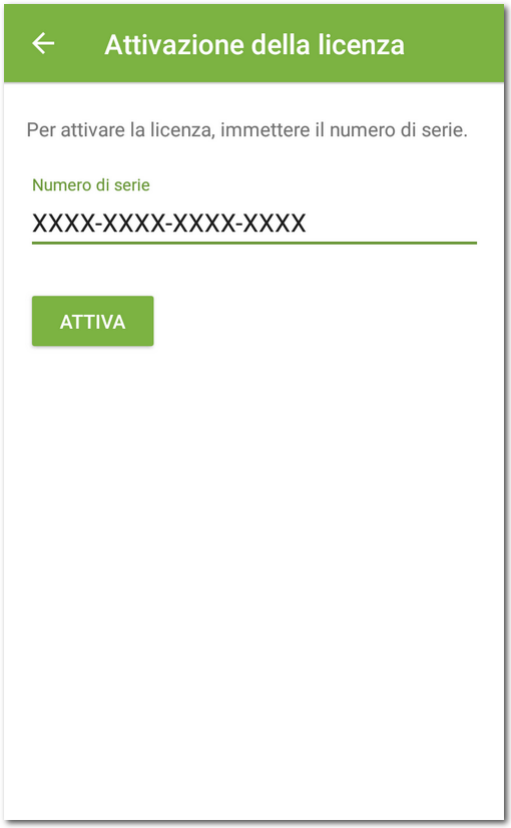

Immagine 5. Registrazione del numero di serie

7. Indicare i dati personali:
   - Nome e cognome.
   - Un indirizzo email valido.
   - Paese.
8. Se lo si desidera, spuntare il flag **Ricevi notizie via email**.
9. Premere il pulsante **Attiva**.

Si aprirà la schermata principale di Dr.Web. In fondo allo schermo comparirà un messaggio che informa che la licenza è stata attivata.

Registrazione del numero di serie sul sito

Se sul dispositivo con l'applicazione installata non c'è la connessione internet, è possibile registrare il numero di serie utilizzando un computer o un altro dispositivo con una connessione internet attiva. In questo caso all'utente verrà inviato un file della chiave di licenza che deve essere copiato sul dispositivo per attivare la licenza.

Per registrare il numero di serie sul sito

1. Andare al sito https://products.drweb.com/register/.

2. Inserire il numero di serie ottenuto all'acquisto di Dr.Web.
3. Compilare il modulo con le informazioni sull'acquirente.
4. Un file della chiave di licenza in archivio ZIP verrà inviato sull'indirizzo email indicato dall'utente.

File della chiave di licenza

Il file della chiave di licenza contiene i permessi dell'utente per utilizzare i prodotti Dr.Web.

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

- Periodo per cui è consentito l'uso dell'applicazione.
- Lista dei componenti consentiti per l'uso.
- Altre limitazioni.

Il file della chiave di licenza è valido se sono soddisfatte contemporaneamente le seguenti condizioni:

- La licenza non è scaduta.
- La licenza copre tutti i moduli utilizzati dall'applicazione.
- L'integrità del file della chiave di licenza non è violata.

Se è violata qualsiasi delle condizioni, il file della chiave di licenza diventa non valido e l'antivirus interrompe la neutralizzazione di programmi malevoli.

La modifica del file della chiave di licenza lo rende non valido. Pertanto, per evitare danni accidentali al file, non è consigliato aprirlo in editor di testo, se non assolutamente necessario.

Utilizzo del file della chiave

Il file della chiave può essere utilizzato solo con l'applicazione installata dal sito Doctor Web.

Per utilizzare il file della chiave

1. Copiare il file della chiave sul dispositivo in una cartella nella memoria interna.

   Si può decomprimere l'archivio e copiare solo il file con l'estensione .key o trasferire sul dispositivo l'archivio ZIP per intero.
2. Nella schermata Licenza selezionare la voce **Si ha già una licenza**.
3. Selezionare la voce **Utilizza il file della chiave** (vedi Immagine 4).
4. Trovare la cartella in cui è locato il file della chiave o l'archivio ZIP con il file e selezionarlo.

Il file della chiave verrà installato e sarà pronto per l'uso. Si aprirà la schermata principale di Dr.Web. In fondo allo schermo comparirà un messaggio che informa che la licenza è stata attivata.

Il file della chiave dei programmi Dr.Web Security Space o Antivirus Dr.Web può essere utilizzato per Dr.Web se supporta l'uso dei componenti DrWebGUI e Update.

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 i componenti DrWebGUI e Update sono presenti nella lista dei valori del parametro Applications nel gruppo [Key]: se questi componenti ci sono nella lista, il file della chiave può essere utilizzato per il funzionamento di Dr.Web.

La modifica del file della chiave lo rende non valido. Per evitare il danneggiamento del file, evitare di salvarlo alla chiusura dell'editor di testo.

5.5. Ripristino della licenza

Il ripristino della licenza potrà essere necessario se l'applicazione viene reinstallata o se si vuole utilizzare Dr.Web su un altro dispositivo.

Se l'applicazione è stata installata da Google Play

1. Aprire l'applicazione.
2. Andare alla schermata Licenza.
3. Sulla schermata **Licenza** selezionare **Si ha già una licenza**.
4. Premere **Ripristina l'acquisto su Google Play**.
5. Indicare l'indirizzo email utilizzato per registrare la licenza e inoltre i dati personali.

   La licenza registrata per questo indirizzo email verrà attivata in maniera automatica.

Se l'applicazione è stata installata dal sito Doctor Web o da Xiaomi GetApps

È possibile ripristinare la licenza in due modi:

- Registrare il numero di serie.
- Utilizzare il file della chiave.

Se l'applicazione è stata installata da HUAWEI AppGallery

1. Aprire l'applicazione.
2. Andare alla schermata Licenza.
3. Sulla schermata **Licenza** selezionare **Si ha già una licenza**.
4. Premere **Ripristina l'acquisto su HUAWEI AppGallery**.
5. Indicare l'indirizzo email utilizzato per registrare la licenza e inoltre i dati personali.

La licenza registrata per questo indirizzo email verrà attivata in maniera automatica.

Ripristino della licenza di prova

1. Aprire l'applicazione.
2. Andare alla schermata Licenza.
3. Sulla schermata **Licenza** selezionare **Ottieni una versione di prova per 14 giorni**.
4. Indicare l'indirizzo email utilizzato nel corso dell'attivazione della licenza di prova e inoltre i dati personali.
5. Premere **Ottieni versione di prova**.

5.6. Sospensione e annullamento dell'abbonamento

Se viene utilizzata una licenza in abbonamento, se necessario, è possibile sospendere l'abbonamento per un periodo di tempo impostato o annullare l'abbonamento tramite l'applicazione Play Store.

Sospensione dell'abbonamento

L'abbonamento verrà sospeso al termine del periodo di riferimento corrente. La licenza resterà valida fino al momento della sospensione dell'abbonamento.

Per sospendere l'abbonamento

1. Aprire l'applicazione **Play Store**.
2. Premere l'icona del proprio profilo Google nell'angolo superiore destro dello schermo.
3. Selezionare **Pagamenti e abbonamenti** > **Abbonamenti**.
4. Selezionare l'applicazione Dr.Web nella lista degli abbonamenti.
5. Sulla schermata **Gestisci abbonamento** selezionare **Sospendi i pagamenti**.
6. Impostare il periodo per cui si vuole sospendere i pagamenti.
7. Confermare la sospensione.

Un abbonamento sospeso può essere ripreso in qualsiasi momento prima della fine del periodo per cui sono stati sospesi i pagamenti.

Per riprendere l'abbonamento

1. Aprire l'applicazione **Play Store**.
2. Premere l'icona del proprio profilo Google nell'angolo superiore destro dello schermo.
3. Selezionare **Pagamenti e abbonamenti** > **Abbonamenti**.
4. Selezionare l'applicazione Dr.Web nella lista degli abbonamenti.

5. Sulla schermata **Gestisci abbonamento** selezionare **Riprendi**.
6. Confermare la ripresa dei pagamenti.

Annullamento dell'abbonamento

Se viene rimossa l'applicazione Dr.Web, l'abbonamento non verrà annullato.

Dopo l'annullamento dell'abbonamento la licenza continuerà a essere valida fino al momento della scadenza del periodo di riferimento corrente.

Per annullare l'abbonamento

1. Aprire l'applicazione **Play Store**.
2. Premere l'icona del proprio profilo Google nell'angolo superiore destro dello schermo.
3. Selezionare **Pagamenti e abbonamenti** > **Abbonamenti**.
4. Selezionare l'applicazione Dr.Web nella lista degli abbonamenti.
5. Sulla schermata **Gestisci abbonamento** selezionare **Annulla abbonamento**.
6. Sulla schermata **Preferisci sospendere il tuo abbonamento?** premere **No**.
7. Sulla schermata **Perché vuoi procedere all'annullamento?** selezionare qualsiasi delle opzioni e premere **Avanti**.
8. Sulla schermata **Annullare l'abbonamento?** premere **Annulla abbonamento**.

5.7. Rinnovo della licenza

Per visualizzare informazioni sulla licenza in uso:

- **Su Android**. Sulla schermata principale di Dr.Web (v. Immagine 8) premere **Menu** e selezionare la voce **Licenza**.
- **Su Android TV**. Sulla schermata principale di Dr.Web passare alla sezione **Varie** > **Licenza**.

Nella schermata **Licenza** è possibile visualizzare il numero di serie, il nome del titolare della licenza e le date di inizio e di scadenza della licenza.

Se l'utente è abbonato al servizio "Antivirus Dr.Web", in modalità di protezione centralizzata nella schermata **Licenza** viene inoltre visualizzata la data di scadenza dell'abbonamento.

Rinnovo della licenza

La licenza in abbonamento attraverso Google Play non richiede rinnovo manuale. L'abbonamento viene automaticamente rinnovato e pagato una volta al mese.

Per rinnovare una licenza Dr.Web, non è necessario reinstallare l'applicazione o interromperne il funzionamento.

È possibile rinnovare la licenza in uno dei seguenti modi:

- Se si ha già un nuovo numero di serie, registrarlo.
- Se la licenza corrente è stata acquistata sul sito Doctor Web o su Xiaomi GetApps, è possibile:
  - Acquistare una licenza.
  - Utilizzare il file della chiave.
  - Rinnovare la licenza sulla pagina personale sul sito Doctor Web.

  Per passare a questa pagina, premere **Menu**, selezionare la voce **Dr.Web** e andare sul link **Mio Dr.Web**.
- Se la licenza corrente è stata acquistata in Google Play:
  1. Sulla schermata principale di Dr.Web premere **Menu** e selezionare la voce **Licenza**.
  2. Sulla schermata **Licenza** (v. Immagine 6) premere **Rinnova la licenza da Google Play**.

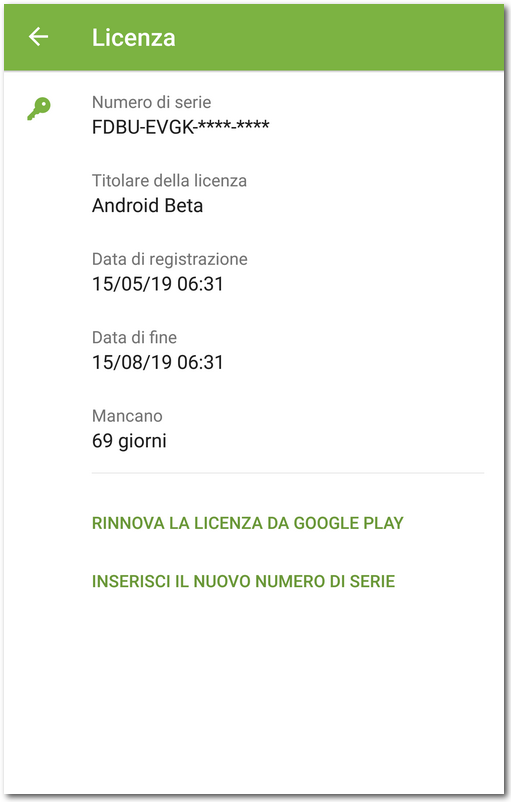

Immagine 6. Rinnovo della licenza

3. Sulla schermata **Rinnovo della licenza** selezionare una delle seguenti varianti:
   - **Licenza di 1 anno**
   - **Licenza di 2 anni**

Quando si sceglie una delle varianti, si apre la schermata di acquisto della licenza. Qualche tempo dopo che il pagamento viene effettuato, la licenza viene attivata automaticamente. Come conferma dell'acquisto, un file della chiave di licenza viene inviato sull'indirizzo email dell'utente. Se a causa di possibili errori tecnici la licenza non viene attivata, contattare il servizio di supporto tecnico: https://support.drweb.com/.

- Se la licenza corrente è stata acquistata in HUAWEI AppGallery:
  1. Sulla schermata principale di Dr.Web premere **Menu** e selezionare la voce **Licenza**.
  2. Sulla schermata **Licenza** premere **Rinnova la licenza da HUAWEI AppGallery**.
  3. Sulla schermata **Rinnovo della licenza** selezionare una delle seguenti varianti:
     - **Licenza di 1 anno**
     - **Licenza di 2 anni**

     Quando si sceglie una delle varianti, si apre la schermata di acquisto della licenza. Qualche tempo dopo che il pagamento viene effettuato, la licenza viene attivata automaticamente. Come conferma dell'acquisto, un file della chiave di licenza viene inviato sull'indirizzo email dell'utente. Se a causa di possibili errori tecnici la licenza non viene attivata, contattare il servizio di supporto tecnico: https://support.drweb.com/.

5.8. Configurazione degli avvisi di scadenza della licenza

Sui dispositivi mobili possono essere attivati gli avvisi di imminente scadenza della licenza (tranne il caso in cui viene utilizzata una licenza in abbonamento da Google Play).

Per attivare gli avvisi

1. Sulla schermata principale di Dr.Web premere **Menu** e selezionare **Impostazioni** (v. Impostazioni).
2. Selezionare la voce **Licenza**.
3. Spuntare il flag **Avvisi**.

6. Per iniziare

Dopo l'installazione di Dr.Web e l'attivazione della licenza è possibile familiarizzare con l'interfaccia e il menu principale dell'applicazione, configurare la barra delle notifiche e impostare un widget di Dr.Web sulla schermata principale del dispositivo.

6.1. Contratto di licenza

Al primo avvio dell'applicazione si aprirà il Contratto di licenza che l'utente deve accettare per continuare a utilizzare l'applicazione.

Sulla stessa schermata viene chiesto di accettare la clausola sull'invio delle statistiche di funzionamento dell'applicazione e di minacce trovate ai server Doctor Web, nonché ai server Google e Yandex.

È possibile rifiutarsi di inviare le statistiche in qualsiasi momento nelle impostazioni dell'applicazione, deselezionando il flag **Invio delle statistiche** nella sezione **Impostazioni generali**.

Se la versione Dr.Web è stata fornita dall'amministratore della rete antivirus aziendale, il Contratto di licenza non verrà aperto.

6.2. Permessi

A partire dalla versione 6.0 nel sistema operativo Android è comparsa la possibilità di consentire o vietare alle applicazioni l'accesso alle funzioni del dispositivo e ai dati personali.

Dopo aver installato Dr.Web e accettato il Contratto di licenza, concedere all'applicazione i permessi necessari. I permessi possono essere richiesti anche al primo clic su uno dei componenti o alla loro attivazione.

- Dr.Web chiede i seguenti permessi al primo avvio dell'applicazione:
  - L'accesso a foto, multimedia e file sul dispositivo.
  - Accesso a tutti i file (sui dispositivi con Android 11.0 e versioni successive).

  Questi permessi sono necessari per il funzionamento dell'applicazione.
  - Il permesso di invio delle notifiche (sui dispositivi con Android 13.0 e versioni successive).

  Il permesso è richiesto affinché Dr.Web possa utilizzare la barra delle notifiche per i messaggi sullo stato di protezione del dispositivo e sul funzionamento dei componenti Dr.Web. Se il permesso non verrà concesso, Dr.Web non potrà informare l'utente sul rilevamento di minacce e sugli eventi dei componenti fino a quando l'applicazione non verrà aperta.

- Filtro chiamate ed SMS chiede i seguenti permessi:
  - Fare e gestire chiamate.
  - Inviare e visualizzare messaggi SMS.
  - L'accesso ai contatti.
  - L'accesso alle notifiche.
  - L'accesso alla lista delle chiamate (sui dispositivi con Android 9.0 e versioni successive).
  - Il permesso di nominare Dr.Web applicazione predefinita per l'identificazione automatica dei numeri e la protezione antispam (sui dispositivi con Android 10.0 e versioni successive).
- Filtro URL chiede l'accesso alle funzioni di accessibilità Android per il funzionamento nei browser supportati.
- Antifurto Dr.Web chiede i seguenti permessi:
  - L'accesso alle chiamate e alla gestione delle stesse.
  - La possibilità di inviare e visualizzare messaggi SMS.
  - L'accesso ai contatti.
  - L'accesso alle notifiche.
  - L'accesso ai dati sulla posizione del dispositivo.
  - L'accesso alle funzioni di accessibilità di Android.
  - Il permesso di nominare Dr.Web amministratore del dispositivo.
- Firewall Dr.Web chiede i seguenti permessi:
  - Connessione alla rete VPN per il monitoraggio del traffico.
  - Sovrapposizione sopra altre finestre.
- Dr.Web su Android TV chiede i seguenti permessi:
  - L'accesso ai contatti.
  - L'accesso a foto, multimedia e file sul dispositivo.
  - Accesso a tutti i file (sui dispositivi con Android 11.0 e versioni successive).

In modalità di protezione centralizzata vengono chiesti i seguenti permessi:

- Autorizzazioni principali (l'accesso a foto, contenuti multimediali e file, contatti ecc.) — per la maggior parte delle funzionalità dell'applicazione.
- Il permesso di invio delle notifiche (sui dispositivi con Android 13.0 e versioni successive) — per la visualizzazione dei messaggi sullo stato di protezione e sul funzionamento dei componenti.
- Accesso a tutti i file (sui dispositivi con Android 11.0 e versioni successive) — per l'esecuzione della scansione del dispositivo.
- Filtro chiamate ed SMS (a seconda della versione di Android, v. sopra) — per il filtraggio delle chiamate e degli SMS in arrivo.
- Amministrazione del dispositivo — per la protezione dell'applicazione da disinstallazioni e la completa operatività di Antifurto.

- Accesso alle funzioni di accessibilità — per il filtraggio delle applicazioni e la completa operatività di Filtro URL, Antifurto e Parental control.
- Sovrapposizione sopra altre finestre — per il filtraggio delle applicazioni e il funzionamento di Firewall.

Se i permessi necessari non vengono concessi, si aprirà la schermata **Sono richieste autorizzazioni** (v. Immagine 7). È possibile concedere tutti i permessi o solo i permessi obbligatori. I permessi obbligatori per il funzionamento dei componenti sono contrassegnati da un'icona gialla. I permessi facoltativi sono contrassegnati da un'icona grigia. Dopo che i permessi vengono concessi, l'icona diventa verde.

Se sono stati concessi tutti i permessi richiesti da un componente, l'utilizzo dell'applicazione continuerà automaticamente. Se solo i permessi obbligatori vengono concessi, sarà possibile continuare a utilizzare l'applicazione facendo clic sul pulsante **Continua**. Sarà possibile concedere i permessi facoltativi al prossimo passaggio a questo componente dalla schermata principale di Dr.Web o sulla schermata delle impostazioni.

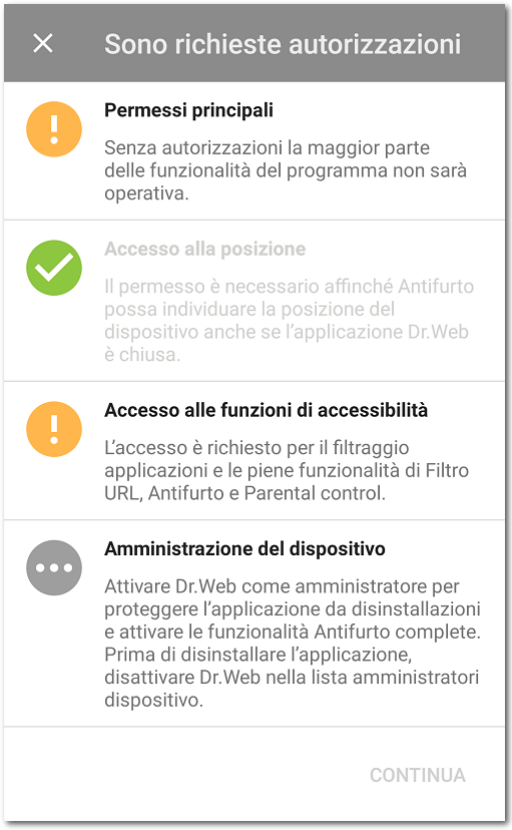

Immagine 7. Sono richieste autorizzazioni

Se vengono rifiutate una o più richieste di concessione dei permessi obbligatori, verrà chiesto di passare alla schermata delle impostazioni:

- Sui dispositivi con Android 9.0 o versioni precedenti:
  1. Premere **Vai su Impostazioni** e selezionare la sezione **Permessi**.

2. Selezionare la voce **Memoria** o **Archiviazione** e concedere il permesso utilizzando l'interruttore.

- Sui dispositivi con Android 10.0:
  1. Premere **Vai su Impostazioni** e selezionare la sezione **Permessi**.
  2. Selezionare la voce **Memoria** o **Archiviazione** nella categoria **Rifiutate** e selezionare l'opzione **Consenti**.
- Sui dispositivi con Android 11.0 o versioni successive:
  1. Premere **Vai su Impostazioni** e selezionare la sezione **Permessi**.
  2. Selezionare la voce **File e contenuti multimediali** o **Archiviazione** nella categoria **Rifiutate** e selezionare l'opzione **Consenti la gestione di tutti i file**. Tramite questa opzione viene concesso l'accesso a foto e contenuti multimediali, nonché l'accesso a tutti i file.

Per aprire la lista di tutti i permessi per Dr.Web

1. Aprire le impostazioni del dispositivo .
2. Premere **Applicazioni** o **Gestione delle applicazioni**.
3. Trovare nella lista delle applicazioni installate Dr.Web e premerlo.
4. Nella schermata **Informazioni applicazione** selezionare la voce **Permessi**.
5. Nel menu locato nell'angolo superiore destro selezionare **Tutti i permessi**.

6.3. Interfaccia

Schermata principale

Sulla schermata principale (vedi Immagine 8) si trova la lista dei componenti principali Dr.Web.

Il **Menu** nell'angolo superiore destro della schermata principale consente di:

- Aprire una schermata con informazioni sulla licenza.
- Aprire le statistiche.
- Aprire l'elenco dei file spostati in quarantena.
- Avviare manualmente l'aggiornamento dei database dei virus.
- Passare alle impostazioni dell'applicazione.
- Aprire la guida.
- Passare alla gestione dell'account.
- Aprire una schermata con informazioni sull'applicazione.

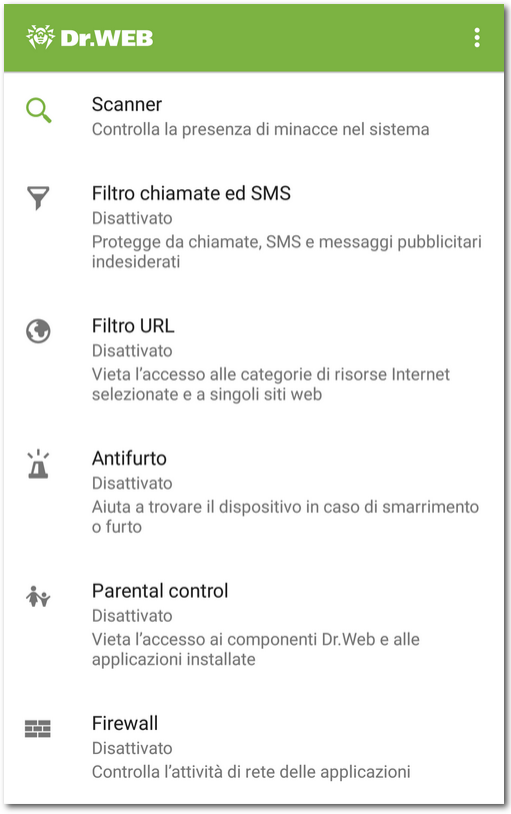

Immagine 8. Schermata principale Dr.Web

Barra di stato

Nella parte superiore della schermata principale di Dr.Web si trova una barra di stato con un indicatore che mostra lo stato corrente della protezione del dispositivo (vedi Immagine 9).

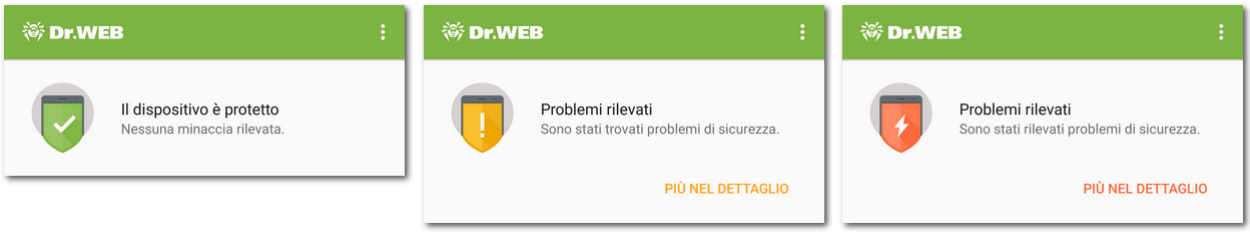

Immagine 9. Barra di stato

- L'indicatore verde significa che il dispositivo è protetto. Non è richiesta alcuna azione aggiuntiva.
- L'indicatore giallo significa che Dr.Web ha rilevato problemi di sicurezza, per esempio, l'assenza della licenza, o una vulnerabilità. Per avere ulteriori informazioni sui problemi trovati e per risolverli, premere **Più nel dettaglio**.
- L'indicatore rosso significa che Dr.Web ha rilevato modifiche sospette nell'area di sistema o minacce. Per aprire i risultati della scansione e neutralizzare le minacce, premere **Più nel dettaglio**.

Se Dr.Web ha rilevato più eventi che richiedono l'attenzione dell'utente, il pulsante **Più nel dettaglio** aprirà la sezione **Eventi** in cui verranno visualizzati tutti i messaggi importanti.

6.4. Avvisi

Sui dispositivi con Android 7.0 o versioni successive tutti gli avvisi Dr.Web vengono raggruppati in un unico avviso a tendina.

Sui dispositivi con Android 8.0 o versioni successive gli avvisi Dr.Web sono suddivisi in categorie, o canali. Nelle impostazioni del dispositivo è possibile gestire separatamente il comportamento di ciascuna categoria di avvisi. Se si disattiva una delle categorie, non si riceverà più avvisi da questa categoria. Di default tutte le categorie sono attivate.

Categorie di avvisi

Categoria	Avvisi
Rilevamento di una minaccia	• Avvisi di minacce rilevate dal componente SpIDer Guard. • Avvisi di minacce rilevate da Scanner Dr.Web.
Applicazioni sicure	Avvisi sull'assenza di minacce nelle applicazioni o negli aggiornamenti appena installati. Sui dispositivi con Android 7.1 o versioni precedenti gli avvisi di questa categoria possono essere attivati o disattivati nelle impostazioni generali Dr.Web.
Stato della protezione antivirus	Se la barra delle notifiche è disattivata, questa categoria contiene i seguenti avvisi: • **Sistema è protetto**. Viene visualizzato se il componente SpIDer Guard è attivato e la scansione di Scanner Dr.Web non è in esecuzione. • Avviso di tipo di scansione di Scanner Dr.Web. Viene visualizzato se è in esecuzione una delle scansioni: rapida, completa o personalizzata. • Avviso di scansione del supporto esterno. Viene visualizzato in caso di scansione della scheda SD e dei supporti rimovibili tramite il componente SpIDer Guard. Se la barra delle notifiche è attivata, su di essa viene visualizzato un messaggio di scansione in corso, se una delle scansioni di Scanner Dr.Web è in esecuzione.
Stato dei componenti addizionali	• **Componenti addizionali sono attivati**. Viene visualizzato se sono attivati Filtro di chiamate ed SMS, Filtro URL, Antifurto Dr.Web o Firewall Dr.Web. • **Agent è attivato**. Viene visualizzato in modalità di protezione centralizzata se sono disattivati Filtro di chiamate ed SMS (sono consentite tutte le chiamate e gli SMS in arrivo), Filtro URL, Antifurto Dr.Web e Firewall Dr.Web. • **Agent e componenti addizionali sono attivati**. Viene visualizzato in modalità di protezione centralizzata se sono attivati Filtro chiamate ed SMS, Filtro URL, Antifurto Dr.Web o Firewall Dr.Web.

Categoria	Avvisi
Avvisi dagli amici	Avvisi ricevuti dagli amici.
Configurazione dei componenti di protezione	**Configurazione dei componenti...** Viene visualizzato all'individuazione della posizione del dispositivo su richiesta di un amico, se è attivato Antifurto Dr.Web nella versione scaricata da Google Play.
Altro	• **Sono richieste autorizzazioni**. Viene visualizzato all'apertura dell'applicazione se la richiesta di accesso a foto, file multimediali e altri è stata precedentemente rifiutata. Nella versione dell'applicazione fornita dall'amministratore della rete antivirus aziendale dell'utente o dal fornitore del servizio "Antivirus Dr.Web", l'avviso viene visualizzato all'apertura dell'applicazione se qualsiasi dei permessi richiesti è stato precedentemente rifiutato. • Avvisi sulla licenza: ▫ **Errore di verifica della licenza**. Viene visualizzato se si è verificato un errore di controllo della licenza. Probabilmente, la licenza non è presente o non è stata confermata dal server. ▫ **Mancano giorni: <numero giorni>**. Viene visualizzato se la licenza sta per scadere e nelle impostazioni dell'applicazione è spuntato il flag Avvisi. ▫ **La licenza è scaduta**. Viene visualizzato se si utilizza il servizio "Antivirus Dr.Web" e la licenza è scaduta. ▫ **Contattare l'amministratore di rete antivirus**. Viene visualizzato se si utilizza il servizio "Antivirus Dr.Web" e la licenza è stata bloccata. • **È disponibile la nuova versione di Dr.Web**. Viene visualizzato nella versione scaricata dal sito Doctor Web se è comparsa una nuova versione e nelle impostazioni dell'applicazione è spuntato il flag Nuova versione. • Avvisi di Antifurto Dr.Web: ▫ **Nessuna SIM card trovata** ▫ **È stata trovata una SIM card nuova**. • Avviso di Filtro chiamate ed SMS: **Sono vietate tutte le chiamate e gli SMS in arrivo**. Viene visualizzato se è attivato il profilo **Blocca tutti**. • Avvisi di Firewall Dr.Web: ▫ **Firewall Dr.Web è disattivato**. Viene visualizzato se la connessione VPN dell'applicazione Dr.Web è stata interrotta. ▫ **È stato superato il limite di traffico mobile**. Viene visualizzato se è stato superato il limite di traffico mobile impostato e nelle impostazioni di Firewall è spuntato il flag Avvisi. • **Nuovo messaggio**. Viene visualizzato se è stato ricevuto un messaggio dall'amministratore della rete antivirus.
Raggruppa avvisi	Questa categoria non contiene avvisi specifici, ma consente di raggruppare tutti gli avvisi Dr.Web in un unico avviso a tendina.

Barra delle notifiche

La barra delle notifiche Dr.Web (vedi Immagine 10) si usa per l'accesso veloce alle funzionalità principali dell'applicazione. Inoltre, visualizza prontamente avvertimenti di modifiche sospette nell'area di sistema e di minacce.

Se Dr.Web rileverà modifiche sospette nell'area di sistema o minacce, sui dispositivi con Android 11.0 e versioni precedenti l'icona dell'applicazione sulla barra delle notifiche cambierà in . Sui dispositivi con Android 12.0 e versioni successive l'icona dell'applicazione cambierà in , mentre l'indicatore dello stato di protezione cambierà colore in rosso .

Immagine 10. Barra delle notifiche su Android 11.0 (a sinistra) e Android 12.0 (a destra)

Su Android TV la barra delle notifiche non è disponibile.

Per attivare la barra delle notifiche Dr.Web

1. Sulla schermata principale di Dr.Web selezionare **Menu** > **Impostazioni**.
2. Selezionare **Impostazioni generali**.
3. Attivare l'opzione **Barra delle notifiche**.

Su Android 5.0 e 5.1, se Dr.Web rileverà modifiche sospette nell'area di sistema o minacce, la barra delle notifiche viene visualizzata sopra tutte le applicazioni fino a quando un'azione non verrà applicata all'oggetto rilevato o l'avviso non verrà cancellato dalla barra delle notifiche.

Se il dispositivo non supporta l'utilizzo delle SIM, invece dell'opzione **Filtro** nella barra delle notifiche viene visualizzata l'opzione **I download** che consente di avviare la scansione degli oggetti scaricati sul dispositivo.

Se Dr.Web funziona in modalità di protezione centralizzata e non si hanno i permessi di modifica delle impostazioni Filtro chiamate ed SMS o Filtro URL, le opzioni corrispondenti **Filtro** e **Filtro URL** non saranno disponibili nella barra delle notifiche.

Tramite la barra delle notifiche è possibile eseguire le seguenti azioni:

- Sui dispositivi con Android 11.0 e versioni precedenti:
  - Aprire l'applicazione. Per questo scopo premere l'icona .
  - Avviare una scansione rapida, completa o personalizzata. Premere **Scanner**.

- Selezionare un filtro per le chiamate e i messaggi in arrivo. Premere **Filtro**.
- Selezionare le categorie di siti a cui si vuole limitare l'accesso. Premere **Filtro URL**.

- Sui dispositivi con Android 12.0 e versioni successive:
  - Aprire l'applicazione (con indicatore di protezione verde). Per questo scopo premere .
  - Concedere i permessi necessari per il funzionamento dell'applicazione (con indicatore giallo). Premere .
  - Aprire i risultati del controllo (con indicatore rosso). Premere .
  - Avviare una scansione rapida, completa o personalizzata. Premere .
  - Selezionare un filtro per le chiamate e i messaggi in arrivo. Premere .
  - Selezionare le categorie di siti a cui si vuole limitare l'accesso. Premere .
  - Visualizzare lo stato di protezione, le azioni correnti e quelle consigliate. Premere .

6.5. Widget

Per comodità di utilizzo di Dr.Web è possibile aggiungere alla schermata principale del dispositivo uno specifico widget che consente di attivare e disattivare la protezione antivirus continua SpIDer Guard.

> Su Android TV il widget non è disponibile.

Per aggiungere il widget Dr.Web

1. Aprire la lista dei widget disponibili sul dispositivo.
2. In questa lista selezionare il widget Dr.Web.

Un widget senza indicatore informa sulla protezione attiva del dispositivo tramite il componente SpIDer Guard. Un widget con un indicatore giallo indica che il componente SpIDer Guard è disattivato (v. Immagine 11). Premere il widget per avviare nuovamente SpIDer Guard.

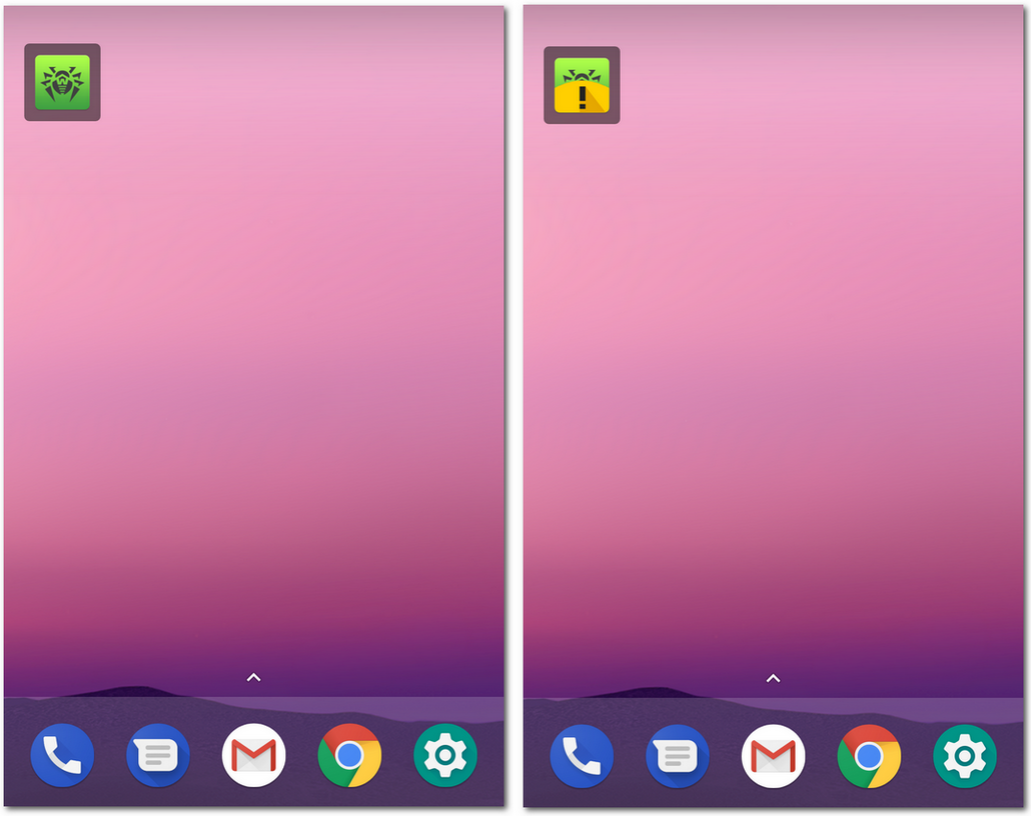

Immagine 11. Widget Dr.Web

6.6. Mio Dr.Web

Il servizio online Mio Dr.Web è la pagina personale dell'utente sul sito Doctor Web. Su questa pagina l'utente può ottenere informazioni sulla licenza (scadenza, numero di serie), rinnovare la licenza, visualizzare la data e l'ora dell'ultimo aggiornamento dei database dei virus e il numero di record nei database, scoprire le notizie e le offerte speciali, fare una domanda al servizio di supporto tecnico ed eseguire altre azioni.

Per aprire il servizio online Mio Dr.Web

1. Sulla schermata principale di Dr.Web premere **Menu** e selezionare la voce **Dr.Web**.
2. Premere **Mio Dr.Web**.

7. Account Dr.Web

L'account Dr.Web consente di proteggere con una password o un'impronta digitale l'accesso ai componenti Dr.Web e alle impostazioni del dispositivo.

Di default la password dell'account o l'impronta digitale sarà richiesta:

- Per accedere ai componenti Dr.Web:
  - Antifurto Dr.Web.
  - Parental control.
- Se è attivato Antifurto Dr.Web, per accedere alle opzioni dell'applicazione:
  - **Reset delle impostazioni**
  - **Copia di backup**
  - **Amministrazione**
- Se è attivato Antifurto Dr.Web, per accedere alle impostazioni sul dispositivo:
  - **Impostazioni** > **Applicazioni** o **Gestione applicazioni** > **Dr.Web Security Space** (su Android 6.0 e versioni successive).
  - **Impostazioni** > **Accessibilità**.
  - **Impostazioni** > **Sicurezza** > **Geolocalizzazione** (su Android 6.0 e versioni successive).
  - **Impostazioni** > **Sicurezza** > **Amministratori dispositivo** > **Dr.Web Security Space**.
  - **Impostazioni** > **Avanzate** > **Reimpostazione** (il nome dell'impostazione e la sua posizione differiscono su dispositivi diversi).

> Sui dispositivi Xiaomi è inoltre protetto l'accesso all'impostazione **Controllo attività**.

Se sul dispositivo è attivato Parental control, l'accesso alle sezioni e impostazioni elencate sopra tramite l'impronta digitale può essere ottenuto se nelle impostazioni di Parental control è attivata l'opzione **Sblocco mediante impronta digitale**.

È inoltre possibile proteggere con la password o l'impronta digitale l'accesso a Filtro chiamate ed SMS, Filtro URL e alle impostazioni dell'applicazione (v. sezione Blocco dell'accesso ad applicazioni e componenti).

Creazione dell'account

1. Sulla schermata principale Dr.Web premere **Menu** nell'angolo superiore destro.
2. Selezionare la voce **Account**.
3. Sulla schermata **Account** premere il pulsante **Crea**.
4. Indicare un indirizzo email.

L'indirizzo potrà essere necessario in seguito, se si dimenticherà la password. Pertanto, specificare un indirizzo a cui si ha accesso.

Notare che dopo la registrazione dell'account non è possibile modificare l'indirizzo email. Per utilizzare un altro indirizzo, sarà necessario eliminare l'account e crearlo nuovamente con un nuovo indirizzo.

Per registrare l'indirizzo email, è necessaria una connessione Internet attiva.

5. Premere il pulsante **Avanti**.
6. Scegliere una password. La password deve contenere almeno 4 caratteri.
7. Ripetere la password e premere **Avanti**.

   Nella schermata successiva si vedrà la conferma di quello che l'account è stato creato con successo.
8. Premere **Finito**.

Gestione dell'account

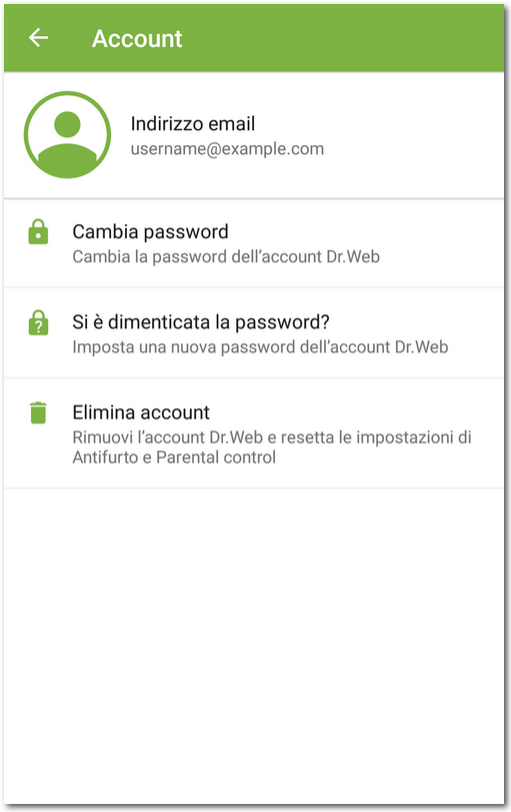

Immagine 12. Account

Sulla schermata **Account** (v. Immagine 12) è possibile eseguire le seguenti azioni:

- Cambiare la password.

- Se dimenticata la password, impostare una nuova password.
- Eliminare l'account.

> ⚠ Nel caso di rimozione dell'account, i componenti Antifurto e Parental control verranno disattivati, le relative impostazioni verranno resettate.

Per modificare la password o rimuovere l'account, inserire la password corrente dell'account o scansionare l'impronta digitale.

8. Componenti Dr.Web

Sulla schermata principale di Dr.Web si trovano la lista dei componenti e il loro stato corrente (attivato o disattivato):

- Scanner verifica il sistema su richiesta dell'utente. Sono possibili 3 tipi di scansione: rapida, completa e personalizzata.
- Filtro chiamate ed SMS blocca chiamate e messaggi SMS indesiderati.
- Filtro URL limita l'accesso dell'utente alle risorse internet.
- Antifurto aiuta a trovare e bloccare il dispositivo in caso di smarrimento o furto.
- Parental control imposta limitazioni all'utilizzo del dispositivo.
- Firewall controlla le connessioni internet e la trasmissione di dati in rete.
- Auditor di sicurezza esegue un'analisi del sistema e rimuove problemi di sicurezza e vulnerabilità rilevati.

Sui dispositivi su cui non è previsto l'uso delle SIM (non c'è il vassoio SIM), **Filtro chiamate ed SMS** e **Antifurto Dr.Web** non sono disponibili.

8.1. Protezione antivirus

- SpIDer Guard controlla il file system in tempo reale.
- Scanner Dr.Web consente di avviare manualmente una scansione per verificare presenza di minacce.
- Sulla schermata Risultati del controllo è possibile selezionare le azioni per neutralizzare le minacce alla sicurezza rilevate.

8.1.1. SpIDer Guard: protezione antivirus continua

SpIDer Guard si attiva automaticamente dopo che viene accettato il Contratto di licenza. Il componente funziona indipendentemente dal fatto che l'applicazione sia in esecuzione o meno. Se SpIDer Guard è attivato, nella barra di stato Android viene visualizzata l'icona Dr.Web .

Su alcuni dispositivi l'icona Dr.Web potrebbe non essere visualizzata quando l'applicazione è in esecuzione in background. Questo avviene perché il firmware del dispositivo ottimizza i processi in background per risparmiare energia o migliorare le prestazioni. Per fissare l'icona Dr.Web nella barra di stato Android, togliere le limitazioni all'applicazione in background: controllare le impostazioni del dispositivo e della gestione applicazioni integrata. Le impostazioni variano in base al modello del dispositivo. Spesso basta premere l'icona con lucchetto per l'applicazione Dr.Web nelle applicazioni recenti.

SpIDer Guard protegge il sistema anche se l'icona Dr.Web non è visualizzata nella barra di stato. Se verrà installata un'applicazione malevola, il componente reagirà e visualizzerà un avviso di minaccia. È possibile controllare il funzionamento di SpIDer Guard tramite il file di test EICAR.

Se SpIDer Guard rileverà una modifica sospetta nell'area di sistema o una minaccia, sullo schermo appariranno:

- Un'icona nella barra di stato di Android nell'angolo superiore sinistro dello schermo:
  - — su Android 4.4,
  - — su Android 5.0–11.0,
  - — su Android 12.0 e versioni successive.
- Un avviso a comparsa sul rilevamento della minaccia (v. Immagine 13).
- Un'icona (su Android 11.0 e versioni precedenti) o (su Android 12.0 e versioni successive) sulla barra delle notifiche.
- Un messaggio con un indicatore rosso sulla barra di stato.

Per aprire i risultati del controllo, premere l'icona ( ) o il messaggio sulla barra di stato.

> SpIDer Guard viene terminato nel caso della completa pulizia della memoria interna del dispositivo tramite il Task manager incorporato. In questo caso, per ripristinare la protezione antivirus continua, sarà necessario aprire nuovamente Dr.Web.

Per disattivare o attivare nuovamente SpIDer Guard

1. Sulla schermata principale di Dr.Web premere **Menu** e selezionare la voce **Impostazioni**.
2. Sulla schermata **Impostazioni** selezionare **SpIDer Guard**.

Impostazioni di SpIDer Guard

> In modalità di protezione centralizzata le impostazioni del componente SpIDer Guard possono essere modificate o bloccate secondo i criteri di sicurezza aziendali o la lista dei servizi pagati.

Per aprire le impostazioni di SpIDer Guard

1. Sulla schermata principale di Dr.Web premere **Menu** e selezionare la voce **Impostazioni**.
2. Sulla schermata **Impostazioni** selezionare **SpIDer Guard**.

File in archivi

Per attivare il controllo di file in archivi compressi, spuntare il flag **File in archivi**.

Di default il controllo di archivi è disattivato. L'attivazione del controllo di archivi può influire sulle prestazioni del sistema e aumentare il consumo della batteria. La disattivazione del controllo di archivi non influisce sul livello di protezione in quanto SpIDer Guard controlla i file APK di installazione indipendentemente dal valore impostato del parametro **File in archivi**.

Scheda SD incorporata e supporti rimovibili

Per attivare la verifica della scheda SD incorporata e dei supporti rimovibili ad ogni collegamento, spuntare il flag **Scheda SD incorporata e supporti rimovibili**. Se questa impostazione è attivata, la verifica viene avviata ogni volta che SpIDer Guard viene attivato. Con questo viene visualizzato l'avviso corrispondente.

Area di sistema

Per tenere traccia di modifiche nell'area di sistema, spuntare il flag **Area di sistema**. Se questa impostazione è attivata, SpIDer Guard tiene traccia di modifiche (aggiunta, modifica e rimozione di file) e informa sulla rimozione di qualsiasi file, nonché sull'aggiunta e la modifica di file eseguibili: `.jar`, `.odex`, `.so`, file di formato APK, ELF ecc.

Controllo ripetuto dell'area di sistema

Per avviare un nuovo controllo dell'area di sistema, premere **Controllo ripetuto dell'area di sistema**. SpIDer Guard ricontrollerà tutte le modifiche nell'area di sistema che precedentemente sono state ignorate.

Avvisi dell'area di sistema

Per attivare gli avvisi sulla modifica a qualsiasi file (non solo a un file eseguibile) nell'area di sistema, spuntare il flag **Avvisi dell'area di sistema**.

Opzioni avanzate

Per attivare il controllo della presenza nel sistema di adware e riskware (compresi gli hacktool e joke), selezionare la voce **Opzioni avanzate** e spuntare i rispettivi flag **Adware** e **Riskware**.

Statistiche

L'applicazione registra gli eventi relativi al funzionamento di SpIDer Guard: attivazione/disattivazione, rilevamento di minacce alla sicurezza e risultati della verifica della memoria del dispositivo e delle applicazioni che vengono installate. Le statistiche di SpIDer Guard vengono visualizzate nella sezione **Eventi** nella scheda **Statistiche** e sono ordinate per data (vedi sezione Statistiche).

Controllo del funzionamento di SpIDer Guard

È possibile controllare il funzionamento di SpIDer Guard tramite il file di test EICAR. Questo file è solitamente usato per:

- Controllare la correttezza dell'installazione dell'antivirus.
- Dimostrare il comportamento dell'antivirus in caso di presenza di una minaccia di virus.
- Controllare il regolamento aziendale al rilevamento di una minaccia.

Il file non è un virus e non contiene frammenti di codice virale, quindi è completamente sicuro per il dispositivo. Il file viene rilevato da Dr.Web come «EICAR Test File (NOT a Virus!)».

È possibile scaricare il file da internet o crearlo in autonomo:

1. In qualsiasi editor di testo creare un nuovo file costituito da una riga:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

2. Salvare il file con l'estensione `.com`.

Non appena il file EICAR verrà salvato sul dispositivo, apparirà un avviso a comparsa da SpIDer Guard (v. Immagine 13).

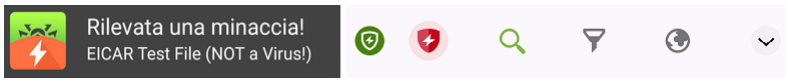

Immagine 13. Rilevamento del file di test EICAR su Android 10.0 (a sinistra) e Android 12.0 (a destra)

8.1.2. Scanner Dr.Web: scansione su richiesta dell'utente

La scansione del sistema su richiesta dell'utente viene eseguita dal 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 scansionare il file system periodicamente, se il componente SpIDer Guard è stato inattivo per qualche tempo. Di solito in questo caso è sufficiente eseguire una scansione rapida del sistema.

In modalità di protezione centralizzata, le impostazioni di Scanner Dr.Web possono essere modificate o bloccate secondo i criteri di sicurezza aziendali o la lista dei servizi pagati. La scansione può essere avviata secondo un calendario impostato sul server di protezione centralizzata.

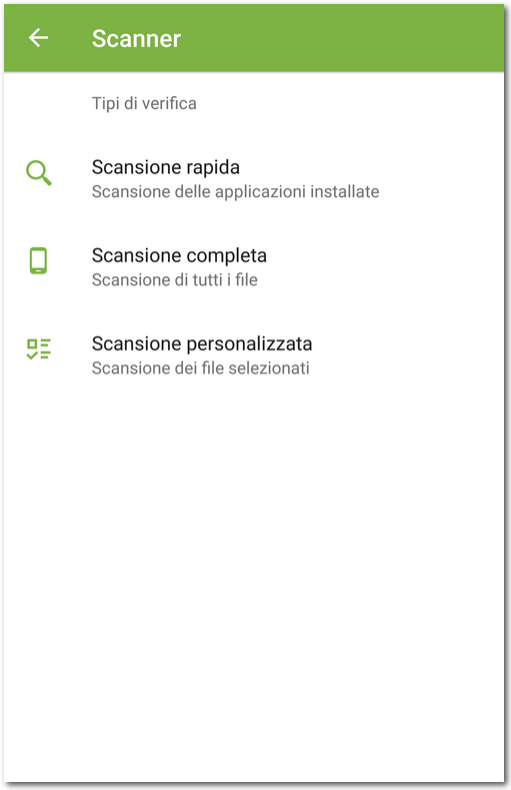

Immagine 14. Scanner Dr.Web

Scansione

Per eseguire una scansione del sistema, sulla schermata principale di Dr.Web selezionare la voce **Scanner**, quindi sulla schermata **Scanner** (vedi Immagine 14) eseguire una delle seguenti azioni:

- Per avviare una scansione delle sole applicazioni installate, selezionare la voce **Scansione rapida**.
- Per avviare una scansione di tutti i file, selezionare la voce **Scansione completa**.
- Per controllare singoli file e cartelle, selezionare la voce **Scansione personalizzata**, quindi selezionare gli oggetti richiesti nella lista comparsa degli oggetti del file system (vedi Immagine 15). Per selezionare tutti gli oggetti, spuntare la casella nell'angolo superiore destro dello schermo. Quindi premere **Controlla**.

Se sul dispositivo sono disponibili i permessi di root, è possibile selezionare per la scansione le cartelle `/sbin` e `/data` locate nella cartella radice.

Sui dispositivi con Android 11.0 e 12.0, per la scansione delle cartelle `/Android/data` e `/Android/obb` è necessario concedere a Dr.Web il permesso di accesso a queste cartelle.

Per consentire l'accesso alla cartella /Android/data o /Android/obb

1. Selezionare la voce **Scansione personalizzata**.

2. Selezionare la cartella `/Android/data` o `/Android/obb` nella lista degli oggetti del file system.
3. Nella finestra di dialogo premere **Consenti**.
4. Premere **Usa questa cartella**.

Sui dispositivi con Android 13.0 e versioni successive, le cartelle `/Android/data` e `/Android/obb` sono protette dal sistema e non sono disponibili per la scansione.

Se durante qualsiasi scansione Scanner Dr.Web rileva minacce, in fondo alla schermata di scansione apparirà l'icona . Premere l'icona per aprire i risultati della scansione (vedi Immagine 16) e neutralizzare le minacce. Se è stata chiusa la schermata di scansione o è stata chiusa l'applicazione, è possibile aprire i risultati della scansione premendo l'icona sulla barra delle notifiche.

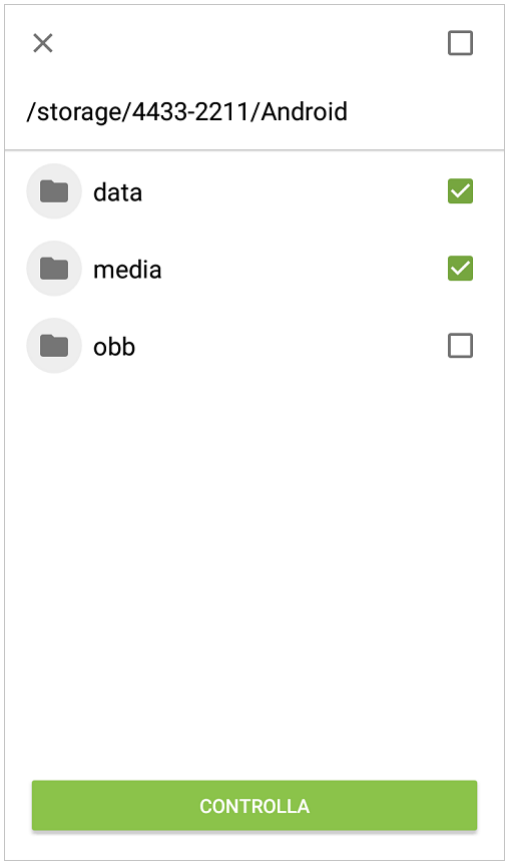

Immagine 15. Scansione personalizzata

Invio di file sospetti al laboratorio antivirus Doctor Web

È possibile inviare al laboratorio antivirus Doctor Web archivi ZIP sospetti (file con l'estensione `.jar`, `.apk`) che presumibilmente contengono virus, file con l'estensione `.odex`, `.dex`, `.so`, o archivi ZIP sicuramente puliti che provocano il cosiddetto falso positivo.

Per inviare un file al laboratorio

1. Premere e tenere premuto un file nella lista degli oggetti del file system (vedi Immagine 15), quindi premere il pulsante **Invia al laboratorio**.
2. Sulla schermata successiva immettere un indirizzo email se si desidera ricevere i risultati dell'analisi del file inviato.
3. Scegliere una delle categorie di richiesta:
   - **Probabile virus**, se si ritiene che il file sia una minaccia.
   - **Falso positivo**, se si ritiene che il file sia erroneamente classificato come minaccia.
4. Premere il pulsante **Invia**.

Al laboratorio antivirus Doctor Web è possibile inviare file di cui le dimensioni non superano 250 MB.

Impostazioni di Scanner Dr.Web

Per accedere alle impostazioni di Scanner Dr.Web, passare alla schermata Impostazioni e selezionare la voce **Scanner**.

- Per attivare il controllo di file in archivi compressi, spuntare il flag **File in archivi**.

Di default il controllo di archivi è disattivato. L'attivazione del controllo di archivi può influire sulle prestazioni del sistema e aumentare il consumo della batteria. La disattivazione del controllo di archivi non influisce sul livello di protezione in quanto Scanner Dr.Web controlla i file APK di installazione indipendentemente dal valore impostato del parametro **File in archivi**.

- Per attivare/disattivare il controllo della presenza nel sistema di adware e riskware (compresi hacktool e joke), selezionare la voce **Opzioni avanzate** e spuntare/deselezionare rispettivamente i flag **Adware** e **Riskware**.

Statistiche

L'applicazione registra gli eventi relativi al funzionamento di Scanner Dr.Web (tipo di scansione, risultati della scansione, rilevamento di minacce alla sicurezza). Le azioni dell'applicazione vengono visualizzate nella sezione **Eventi** nella scheda **Statistiche**, ordinate per data (vedi sezione Statistiche).

8.1.3. Risultati del controllo

Come aprire i risultati del controllo

- Se Scanner Dr.Web rileverà minacce, sulla schermata di scansione apparirà l'icona .

  Per aprire i risultati del controllo, premere questa icona.
- Se SpIDer Guard rileverà una modifica sospetta nell'area di sistema o una minaccia, sullo schermo appariranno:
  - Un'icona nella barra di stato di Android nell'angolo superiore sinistro dello schermo:
    - — su Android 4.4,
    - — su Android 5.0–11.0,
    - — su Android 12.0 e versioni successive.
  - Un avviso a comparsa sul rilevamento della minaccia (v. Immagine 13).
  - Un'icona (su Android 11.0 e versioni precedenti) o (su Android 12.0 e versioni successive) sulla barra delle notifiche.
  - Un messaggio con un indicatore rosso sulla barra di stato.

  Per aprire i risultati del controllo, premere l'icona ( ) o il messaggio sulla barra di stato.

> Su Android 5.0 e versioni successive l'avviso di minaccia compare anche sulla schermata di blocco del dispositivo da cui è possibile passare ai risultati del controllo.

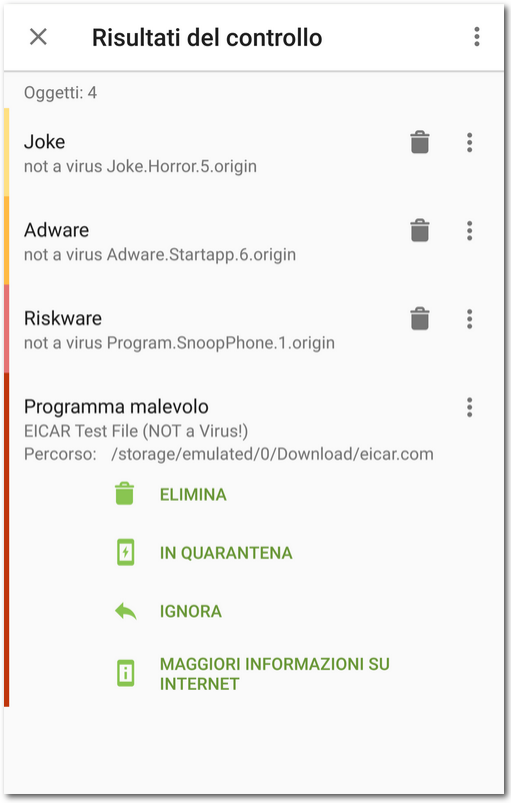

Immagine 16. Risultati del controllo

Neutralizzazione delle minacce

Sulla schermata **Risultati del controllo** è possibile visualizzare la lista delle minacce e modifiche sospette nell'area di sistema. Per ciascun oggetto sono indicati il suo tipo e nome, nonché l'icona dell'opzione che è raccomandata per questo oggetto.

Gli oggetti sono contrassegnati con colori diversi a seconda del grado di pericolo. Tipi di oggetti in ordine di diminuzione del pericolo:

1. Programma malevolo.
2. Riskware.
3. Hacktool.
4. Adware.
5. Modifiche nell'area di sistema:
   - File nuovi nell'area di sistema.
   - Modifica dei file di sistema.
   - Eliminazione dei file di sistema.
6. Joke.

Per visualizzare il percorso di un file, selezionare l'oggetto corrispondente. Nel caso di minacce rilevate in applicazioni è indicato anche il nome del pacchetto dell'applicazione.

Neutralizzazione di tutte le minacce

Per rimuovere tutte le minacce contemporaneamente

- Nell'angolo superiore destro della schermata **Risultati del controllo** selezionare **Menu** > **Elimina tutto**.

Per spostare in quarantena tutte le minacce contemporaneamente

- Nell'angolo superiore destro della schermata **Risultati del controllo** selezionare **Menu** > **Tutto in quarantena**.

Neutralizzazione delle minacce una per una

Per ciascun oggetto è disponibile il proprio set di opzioni. Per espandere una lista delle opzioni, selezionare un oggetto. Le opzioni consigliate sono elencate per prime. Selezionare una delle opzioni:

Cura per curare un'applicazione infetta.

L'opzione è disponibile per alcune minacce nelle applicazioni di sistema, se sul dispositivo sono disponibili i permessi di root.

Elimina per rimuovere completamente una minaccia dalla memoria del dispositivo.

In alcuni casi Dr.Web non può rimuovere applicazioni che utilizzano le funzioni di accessibilità Android. Se Dr.Web non rimuoverà un'applicazione dopo la selezione dell'opzione **Elimina**, passare a modalità provvisoria e rimuovere l'applicazione manualmente. Se a Dr.Web è concesso l'accesso alle funzioni di accessibilità, l'applicazione verrà rimossa automaticamente dopo la selezione dell'opzione **Elimina**.

L'opzione non è disponibile per le minacce nelle applicazioni di sistema nei seguenti casi:

- Se sul dispositivo non sono disponibili i permessi di root.
- Se la rimozione di un'applicazione può compromettere l'operatività del dispositivo.
- Se è stata rilevata una versione di una minaccia. Per determinare se un'applicazione rappresenta davvero una minaccia, segnalare un falso positivo.

In quarantena per spostare la minaccia in una cartella isolata (vedi sezione Quarantena).

Se una minaccia è stata rilevata in un'applicazione installata, non può essere spostata in quarantena. In questo caso l'opzione **In quarantena** non è disponibile.

Ignora per lasciare temporaneamente intatta la modifica nell'area di sistema o la minaccia.

Blocca per disattivare l'accesso dell'applicazione alle connessioni internet.

L'opzione è disponibile per le minacce nelle applicazioni di sistema.

Invia al laboratorio o **Falso positivo** per inviare il file al laboratorio antivirus Doctor Web per l'analisi. L'analisi mostrerà se questa è davvero una minaccia o un falso positivo. Se si è verificato un falso positivo, esso verrà corretto. Per ricevere i risultati dell'analisi, indicare un indirizzo email.

Se il file è stato correttamente inviato al laboratorio, all'oggetto viene automaticamente applicata l'azione **Ignora**.

L'opzione **Invia al laboratorio** è disponibile solo per file eseguibili aggiunti o modificati nell'area di sistema: `.jar`, `.odex`, `.so`, file di formato APK, ELF ecc.

L'opzione **Falso positivo** è disponibile solo per versioni di minacce e per le minacce nell'area di sistema.

Maggiori informazioni su Internet per aprire la pagina con la descrizione dell'oggetto rilevato sul sito Doctor Web.

8.1.3.1. Minacce nelle applicazioni di sistema

Le applicazioni installate nell'area di sistema in alcuni casi possono eseguire funzioni caratteristiche dei programmi malevoli, per cui Dr.Web può identificare tali applicazioni come minacce.

Per le applicazioni di sistema è disponibile l'opzione **Blocca**. Selezionarla affinché Firewall Dr.Web blocchi tutte le connessioni internet per l'applicazione di sistema identificata come minaccia.

Per le applicazioni di sistema, così come per qualsiasi applicazione installata, l'opzione **In quarantena** non è disponibile.

Se un'applicazione di sistema può essere rimossa senza compromettere l'operatività del dispositivo o curata, per essa è disponibile l'opzione corrispondente. Per questo scopo, sul dispositivo devono essere disponibili i permessi di root.

Se un'applicazione di sistema non può essere rimossa senza compromettere l'operatività del dispositivo, l'opzione **Elimina** non è disponibile, ma è possibile utilizzare le seguenti raccomandazioni:

- Arrestare l'applicazione attraverso le impostazioni del dispositivo: nella lista delle applicazioni installate sulla schermata **Impostazioni** > **Applicazioni** selezionare l'applicazione identificata come minaccia, dopodiché sulla schermata con informazioni su di essa premere il pulsante **Interrompi**.

  Sarà necessario eseguire questa azione dopo ogni riavvio del dispositivo.

- Disattivare l'applicazione attraverso le impostazioni del dispositivo: nella lista delle applicazioni installate sulla schermata **Impostazioni** > **Applicazioni** selezionare

l'applicazione identificata come minaccia, dopodiché sulla schermata con informazioni su di essa premere il pulsante **Disattiva**.

- Se sul dispositivo è installato un firmware custom, è possibile ritornare al software ufficiale del produttore del dispositivo in autonomo o contattando un centro assistenza.
- Se si utilizza il software ufficiale del produttore del dispositivo, provare a contattare l'azienda produttrice per ricevere ulteriori informazioni su questa applicazione.
- Se sul dispositivo sono disponibili i permessi di root, è possibile provare a rimuovere tali applicazioni utilizzando utility specifiche.

Per disattivare l'avviso sulle minacce in applicazioni di sistema che non possono essere rimosse senza compromettere l'operatività del dispositivo, spuntare il flag **Applicazioni di sistema** nella sezione **Impostazioni** > **Impostazioni generali** > **Opzioni avanzate**.

Su Android TV spuntare il flag **Applicazioni di sistema** nella sezione **Varie** > **Impostazioni** > **Impostazioni generali** > **Opzioni avanzate**.

8.1.3.2. Modifiche nell'area di sistema

L'area di sistema — area di memoria che viene utilizzata dalle applicazioni di sistema e contiene dati critici per il funzionamento del dispositivo e dati utente sensibili. Se sul dispositivo non sono consentiti i permessi di root, l'area di sistema non è disponibile per l'utente.

Le applicazioni malevole possono ottenere i permessi di root e apportare modifiche all'area di sistema: rimuovere, aggiungere o modificare file o cartelle.

Il componente SpIDer Guard può tenere traccia di modifiche nell'area di sistema. È possibile attivare il controllo dell'area di sistema nelle impostazioni di SpIDer Guard. Se il componente rileverà modifiche sospette, avviserà l'utente.

Modifica	Nome	Tipo
Rimozione di una cartella di file	read-only.area.dir.deleted.threat	Eliminazione dei file di sistema
Rimozione di un file	read-only.area.deleted.threat	Eliminazione dei file di sistema
Aggiunta di una cartella di file	read-only.area.dir.added.threat	File nuovi nell'area di sistema
Aggiunta di un file	read-only.area.added.threat	File nuovi nell'area di sistema
Modifica di un file	read-only.area.changed.threat	Modifica dei file di sistema

Se SpIDer Guard rileverà una delle modifiche sopraelencate, i file o le cartelle stessi non sono necessariamente malevoli, ma la modifica può essere apportata da un'applicazione malevola.

Per le modifiche rilevate sono disponibili le seguenti opzioni:

- Ignora
- Invia al laboratorio — disponibile solo in caso di aggiunta o modifica di file eseguibili: `.jar`, `.odex`, `.so`, file di formato APK, ELF ecc.
- Maggiori informazioni su Internet

SpIDer Guard informa solo sulle modifiche sopraelencate. Per rilevare un'applicazione malevola che poteva apportare modifiche all'area di sistema, eseguire la scansione completa del dispositivo.

8.1.3.3. Minacce che utilizzano la vulnerabilità Stagefright

La vulnerabilità Stagefright consente di hackerare il dispositivo attraverso un file multimediale con codice malevolo.

Le minacce che utilizzano la vulnerabilità Stagefright vengono rilevate e neutralizzate da Firewall Dr.Web. Attivarlo per fornire protezione dagli exploit Stagefright.

Firewall Dr.Web analizza in tempo reale il contenuto dei file multimediali che vengono caricati sul dispositivo. Se Dr.Web rileverà un codice malevolo in un file che viene scaricato sul dispositivo:

- Il download del file viene interrotto.
- Nella parte inferiore dello schermo viene visualizzato un avviso con l'icona  . Il nome della minaccia rilevata avrà il postfisso <*nome.minaccia*>.Stagefright.
- Un record della minaccia rilevata sarà inserito nelle statistiche di funzionamento dell'applicazione.

8.1.4. Applicazioni che bloccano il dispositivo

Dr.Web consente di proteggere il dispositivo mobile dai programmi ransomware. I simili programmi sono molto pericolosi. Possono cifrare file conservati nella memoria incorporata del dispositivo o sui supporti rimovibili (come per esempio, una scheda SD). Questi programmi possono bloccare lo schermo e visualizzare su di esso messaggi di riscatto per la decifratura dei file e lo sblocco del dispositivo.

Le azioni dei programmi ransomware possono colpire le fotografie, i video e documenti dell'utente. Inoltre, questi programmi rubano e trasmettono sui server dei malintenzionati diverse informazioni sul dispositivo infetto (compreso l'identificatore IMEI), informazioni dalla rubrica (nomi dei contatti, numeri di telefono e indirizzi email), monitorano le chiamate in entrata e uscita e sono in grado di bloccarle. Tutte le informazioni raccolte, comprese quelle relative alle chiamate, anche vengono trasmesse sul server di controllo.

I programmi ransomware vengono riconosciuti e rimossi da Dr.Web al tentativo di infiltrazione sul dispositivo protetto. Tuttavia, il numero e la diversità di tali programmi sono in continuo

aumento. Pertanto, un'applicazione di blocco del dispositivo può essere installato sul dispositivo soprattutto se i database dei virus Dr.Web non venivano aggiornati per qualche tempo e non includono informazioni sui nuovi esemplari.

Se il dispositivo mobile è stato bloccato da un programma ransomware e se SplDer Guard è attivato, è possibile sbloccare il dispositivo.

Per sbloccare il dispositivo

1. Entro 5 secondi collegare e scollegare il caricabatterie.
2. Entro i successivi 10 secondi collegare le cuffie.
3. Entro i successivi 5 secondi scollegare le cuffie.
4. Entro i successivi 10 secondi scuotere vigorosamente il dispositivo mobile.
5. Dr.Web termina tutti i processi attivi sul dispositivo, compreso il processo avviato dal programma di blocco del dispositivo, dopodiché viene accesa una breve vibrazione (sui dispositivi che hanno questa funzionalità). Quindi si apre la schermata Dr.Web.

   

   Notare che con la terminazione dei processi attivi i dati delle altre applicazioni che erano attive al momento del blocco del dispositivo potrebbero andare persi.

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 rimuovere l'applicazione malevola.

8.2. Filtro chiamate ed SMS

Filtro chiamate ed SMS blocca chiamate e messaggi SMS indesiderati, inclusi gli invii di SMS pubblicitari, nonché chiamate e messaggi da numeri sconosciuti e nascosti.

È possibile attivare il filtro di divieto o quello di permesso.

- Il filtro di divieto blocca i contatti, le parole chiave o le maschere aggiunti.
- Il filtro di permesso consente chiamate ed SMS solo dai contatti o dalle maschere aggiunti.

Quando si attiva un filtro, l'altro viene disattivato.

Per il filtraggio è possibile selezionare una delle liste standard o creare una lista personalizzata.

Il filtro SMS non è operativo nelle versioni dell'applicazione da Google Play.

Il filtro potrebbe non funzionare correttamente sui dispositivi con due SIM.

Il filtro SMS potrebbe non funzionare correttamente a causa di limitazioni tecniche di Android. I messaggi bloccati possono essere visualizzati nel registro SMS.

In modalità di protezione centralizzata le impostazioni di filtraggio possono essere modificate o bloccate secondo i criteri di sicurezza aziendali o la lista dei servizi pagati.

Permessi

Al primo avvio Filtro chiamate ed SMS può richiedere i seguenti permessi:

- L'accesso ai contatti.
- Fare e gestire chiamate.
- Inviare e visualizzare messaggi SMS.

Premere **Consenti** in ciascuna finestra.

Sui dispositivi con Android 9.0 e versioni successive Filtro chiamate ed SMS chiede anche l'accesso alla lista chiamate.

Sui dispositivi con Android 10.0 e versioni successive Filtro chiamate ed SMS chiede anche il permesso di utilizzare Dr.Web come applicazione predefinita per l'identificazione automatica dei numeri e la protezione antispam.

Senza i permessi necessari il componente non sarà operativo.

Se si utilizza un telefono Xiaomi con l'applicazione installata **Sicurezza**, in questa applicazione concedere a Dr.Web il permesso di gestione degli SMS.

8.2.1. Filtro di divieto

Il filtro di divieto blocca le chiamate e gli SMS dai contatti aggiunti.

Come utilizzare il filtro di divieto

- Attivare l'opzione **Blocca tutti** per bloccare tutte le chiamate e i messaggi SMS in arrivo.
- Aggiungere contatti a **Black list**.
- Creare liste personalizzate.

Per creare una lista

1. Aprire il filtro di divieto.
2. Premere l'icona .
3. Indicare il nome della lista.
4. Aggiungere contatti o parole chiave. Una lista vuota non può essere salvata.

Per aggiungere contatti alla lista

1. Sulla schermata della lista richiesta premere l'icona . Selezionare una delle opzioni:

   Contatti — aggiungi un contatto dai contatti sul dispositivo.

   Registro chiamate — aggiungi un contatto dalle chiamate recenti. È disponibile solo nella versione scaricata dal sito.

   Registro SMS — aggiungi un contatto dai messaggi SMS recenti. È disponibile solo nella versione scaricata dal sito.

   Parola chiave — aggiungi una parola chiave per bloccare messaggi SMS. È disponibile solo nella versione scaricata dal sito.

   Dr.Web cercherà nei messaggi la parola o frase che viene aggiunta. Se si vuole che l'applicazione blocchi i messaggi in cui ci sono più parole che non sono una accanto all'altra, aggiungerle una per una.

   Numero nascosto — blocca le chiamate da qualsiasi numero nascosto. È disponibile solo nella versione da Google Play. Nella versione dal sito e nella versione da HUAWEI AppGallery un numero nascosto può essere aggiunto dal registro chiamate o SMS.

   Nuovo contatto — crea un nuovo contatto o una maschera.

   Importazione dei contatti — importa una lista di contatti salvata in precedenza.
2. Se necessario, per ciascun contatto modificare il nome e il telefono, selezionare quello che si vuole bloccare: **Chiamate** o **SMS**. I numeri nascosti e i numeri aggiunti dai contatti dell'utente non possono essere modificati.

Per salvare sul dispositivo i contatti da una lista

1. Selezionare la lista richiesta.
2. Nell'angolo superiore destro premere l'icona .

8.2.2. Filtro di permesso

Il filtro di permesso consente solo le chiamate e gli SMS dai contatti aggiunti.

Come utilizzare il filtro di permesso

- Attivare l'opzione **Contatti** per accettare solo le chiamate e i messaggi SMS in arrivo dai numeri dei contatti.
- Creare liste personalizzate.

Per creare una lista

1. Aprire il filtro di permesso.
2. Premere l'icona .
3. Indicare il nome della lista.
4. Aggiungere contatti. Una lista vuota non può essere salvata.

Per aggiungere contatti alla lista

1. Sulla schermata della lista richiesta premere l'icona . Selezionare una delle opzioni:

   Contatti — aggiungi un contatto dai contatti sul dispositivo.

   Registro chiamate — aggiungi un contatto dalle chiamate recenti. È disponibile solo nella versione scaricata dal sito.

   Registro SMS — aggiungi un contatto dai messaggi SMS recenti. È disponibile solo nella versione scaricata dal sito.

   Nuovo contatto — crea un nuovo contatto o una maschera.

   Importazione dei contatti — importa una lista di contatti salvata in precedenza.
2. Se necessario, modificare il nome e il telefono per ciascun contatto. Un numero aggiunto dai contatti sul dispositivo non può essere modificato.

Per salvare sul dispositivo i contatti da una lista

1. Selezionare la lista richiesta.
2. Nell'angolo superiore destro premere l'icona .

8.2.3. Maschere

Le maschere consentono di aggiungere numeri simili alle liste dei filtri di divieto e di permesso:

- Numeri che iniziano con una sequenza specifica di cifre (o altri caratteri).
- Numeri che terminano con una sequenza specifica di cifre (o altri caratteri).
- Numeri che contengono una sequenza specifica di cifre (o altri caratteri).

Per aggiungere una maschera

1. Sulla schermata della lista richiesta premere l'icona e selezionare **Nuovo contatto**.

2. Se necessario, modificare il nome.
3. Inserendo il numero, utilizzare l'asterisco * all'inizio, alla fine o su entrambi i lati.

   L'asterisco sostituisce qualsiasi sequenza di caratteri. Non utilizzare l'asterisco nel mezzo del numero o due asterischi di fila: tale maschera non sarà operativa.
4. Se una maschera si aggiunge alla lista del filtro di divieto, selezionare quello che si vuole bloccare: **Chiamate** o **SMS**.

Esempi di maschere

Esempio	Commento
+7*	Tutti i numeri che iniziano con +7
0	Tutti numeri che contengono 0 all'inizio, nel mezzo o alla fine del numero
*0	Tutti i numeri che terminano con 0
* +7*0 *0*0 **0 +7**	Esempi di maschere non valide

8.2.4. Modifica delle liste

Per modificare una lista

1. Premere la lista che si desidera modificare.
2. Apportare modifiche.
3. Premere il pulsante **Salva**.

Per rimuovere una lista

- Far scorrere il dito con il nome della lista verso sinistra.

Se si rimuove accidentalmente una lista sbagliata, premere **Annulla**. Le liste standard non possono essere rimosse.

Per rimuovere più liste

1. Prima premere e tenere premuta una sola lista.
2. Dopo la vibrazione selezionare le altre liste da rimuovere.
3. Premere l'icona nell'angolo superiore destro.

Per rimuovere un contatto da una lista

- Far scorrere il dito verso sinistra.

Per rimuovere più contatti da una lista

1. Prima premere e tenere premuto un solo contatto.
2. Dopo la vibrazione selezionare gli altri contatti che si desidera rimuovere.
3. Premere l'icona nell'angolo superiore destro.
   Per annullare la rimozione accidentale di un contatto, premere **Annulla**.

> Quando si rimuove un contatto da una lista, esso non viene rimosso dai contatti sul dispositivo.

8.2.5. Chiamate ed SMS bloccati

Per aprire la lista delle chiamate e dei messaggi SMS bloccati

1. Sulla schermata principale di Dr.Web selezionare **Filtro chiamate ed SMS**.
2. Premere **Menu** e selezionare **Chiamate bloccate** o **SMS bloccati**.

Se ci sono chiamate o messaggi SMS bloccati, le relative informazioni appariranno sulla barra di stato. Per visualizzare informazioni su una chiamata o un messaggio bloccato, nella barra di stato premere **Più nel dettaglio**.

Per ogni chiamata o messaggio SMS bloccato sono disponibili le seguenti informazioni:

- Data e ora di arrivo della chiamata o del messaggio.
- Numero e nome della persona che ha chiamato o inviato il messaggio.
- Testo del messaggio SMS.

Azioni con le chiamate e gli SMS bloccati

Per chiamare

1. Premere il numero nella lista delle chiamate o dei messaggi bloccati.
2. Premere **Chiama**.

Per inviare un messaggio SMS

1. Premere il numero nella lista delle chiamate o dei messaggi bloccati.
2. Premere **Invia SMS**.

Per rimuovere una chiamata o un messaggio SMS

- Far scorrere il dito verso sinistra.

Per rimuovere tutte le chiamate o i messaggi SMS

1. Premere **Menu** nell'angolo superiore destro dello schermo.
2. Premere **Cancella la lista**.

8.3. Filtro URL

L'accesso a siti viene controllato dal filtro URL. Il filtro URL consente di proteggere l'utente dalle visite a risorse internet indesiderate. Per configurare il filtro URL, si possono selezionare singoli siti o categorie di siti.

Al tentativo di apertura di un sito dalla lista di quelli vietati, si vedrà una pagina di blocco.

Il filtro URL supporta il browser integrato di Android, nonché i browser Google Chrome, Yandex.Browser, Microsoft Edge, Firefox, Firefox Focus, Opera, Adblock Browser, Dolphin Browser, Sputnik, Boat Browser e Atom.

Attivazione del filtro URL

Sulla schermata principale di Dr.Web selezionare l'opzione **Filtro URL** (v. Immagine 17).

Filtro URL può richiedere l'accesso alle funzioni accessibilità di Android. L'accesso è necessario per il corretto funzionamento del filtro URL nei browser installati. Senza l'accesso Filtro URL non sarà operativo.

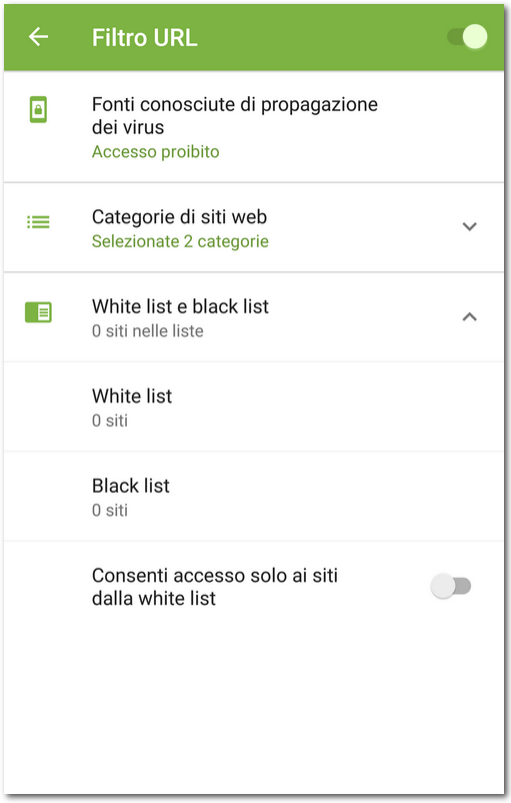

Immagine 17. Filtro URL

Categorie di siti

Dr.Web consente di selezionare determinate categorie di siti per negarne l'accesso. Espandere la lista **Categorie di siti** e selezionare le categorie richieste:

- Siti sconsigliati
- Siti con contenuti per adulti

  Selezionando questa categoria, si attiva il *filtro famiglia* nei motori di ricerca Google, Yandex, Bing, Yahoo e Rambler. Ciò significa che materiali "per adulti" verranno completamente esclusi dai risultati di una ricerca.
- Violenza
- Armi
- Giochi d'azzardo
- Droga
- Linguaggio volgare
- Giochi online
- Terrorismo
- Posta elettronica
- Social network

- Chat
- URL aggiunte su richiesta di un titolare del diritto d'autore
- Anonymizer
- Pool per l'estrazione di criptovalute.

Di default il filtro URL vieta l'accesso ai siti noti come fonti di diffusione dei virus.

White list e black list

È possibile creare liste di siti l'accesso a cui viene consentito o bloccato a prescindere da altre impostazioni del filtro URL. Di default le liste sono vuote.

Per aggiungere un sito alla white list o black list

1. Nella finestra del filtro URL espandere la sezione **White list e black list**.
2. Selezionare la lista a cui si vuole aggiungere un indirizzo.
3. Premere l'icona  nell'angolo inferiore destro.
4. Indicare l'indirizzo di un sito in uno dei formati elencati:
   - example.com
   - http://example.com
   - https://www.example.com
   - www.example.com

È possibile aggiungere solo indirizzi di siti specifici, l'aggiunta di maschere o parole chiave non è supportata.

5. Premere **Aggiungi URL**.

Se si cercherà di aggiungere un indirizzo che è già presente nella lista opposta, si verrà chiesti di spostarlo.

Consenti accesso solo ai siti dalla white list

Attivare questa opzione per visualizzare soltanto i siti che sono stati inseriti nella **White list**. L'accesso a tutti gli altri siti verrà vietato.

In modalità di protezione centralizzata le impostazioni di filtro URL possono essere modificate o bloccate secondo i criteri di sicurezza aziendali o la lista dei servizi pagati.

8.4. Antifurto Dr.Web

Antifurto Dr.Web consente di gestire il dispositivo in caso di smarrimento o furto. Ad esempio, è possibile rimuovere da remoto i dati personali, individuare la posizione del dispositivo o bloccarlo. Per sbloccare il dispositivo, è necessario inserire la password:

- dell'account Dr.Web, se è configurato
- di Antifurto, se l'account non è configurato.

Come gestire il dispositivo tramite Antifurto

- Anticipatamente configurare Antifurto, ad esempio, attivare il blocco del dispositivo dopo il cambio della SIM.
- Inviare ad Antifurto un comando, ad esempio, per individuare la posizione del dispositivo.

8.4.1. Attivazione di Antifurto Dr.Web

1. Sulla schermata principale di Dr.Web selezionare **Antifurto**.
2. Sulla schermata **Antifurto** premere il pulsante **Attiva**.
3. Se Antifurto viene attivato per la prima volta, consentire all'applicazione l'accesso alle accessibilità Android, nonché alle funzioni e ai dati del dispositivo.

   Se si utilizza la versione dell'applicazione dal sito Doctor Web su un telefono Xiaomi con l'applicazione installata **Sicurezza**, in questa applicazione concedere a Dr.Web il permesso di gestione degli SMS.

   Antifurto funziona solo se tutti i permessi sono stati concessi.
4. Se l'account Dr.Web non è stato creato sul dispositivo, crearlo.

   Se l'account è già creato, inserire la password dell'account. Se viene inserita una password errata 10 volte di seguito, il campo di inserimento della password verrà temporaneamente bloccato. Si vedrà quanto tempo manca al tentativo successivo.
5. Se Dr.Web non è amministratore del dispositivo, attivare l'applicazione come amministratore:
   - Per impedire la rimozione indesiderata dell'applicazione.
   - Per consentire ad Antifurto Dr.Web di ripristinare le impostazioni di fabbrica del dispositivo. Ciò proteggerà i dati utente in caso di smarrimento o furto del dispositivo.
6. Per aggiungere amici, premere l'icona  . Gli amici aiuteranno a gestire da remoto il dispositivo in caso di smarrimento o furto, nonché nel caso in cui si dimenticherà la password dell'account Dr.Web. Premere **Avanti**.
7. Modificare un testo che verrà visualizzato sullo schermo del dispositivo in caso di blocco. Qui si può indicare come è possibile contattare l'utente e restituirgli il dispositivo smarrito. Premere **Avanti**.

8. Modificare il testo di un avviso che può essere inviato agli amici se Antifurto bloccherà il dispositivo e si dimenticherà la password. Premere **Avanti**.
9. Attivare le impostazioni necessarie e premere **Finito**.

8.4.2. Configurazione di Antifurto Dr.Web

In modalità di protezione centralizzata le impostazioni di Antifurto Dr.Web possono essere modificate o bloccate in conformità ai criteri di sicurezza aziendali o la lista dei servizi pagati.

Per aprire Antifurto

1. Sulla schermata principale di Dr.Web selezionare **Antifurto**.
2. Se accanto al campo di inserimento della password è presente l'icona , premere l'icona e toccare il lettore di impronte digitali.

   Se l'autenticazione tramite impronta digitale non è disponibile, inserire la password dell'account Dr.Web. Se viene inserita una password errata 10 volte di seguito, il campo di inserimento della password verrà temporaneamente bloccato. Si vedrà quanto tempo manca al tentativo successivo.

Quando si esegue l'aggiornamento dalle versioni precedenti alla versione 12, la password di Antifurto Dr.Web diventa automaticamente la password dell'account Dr.Web.

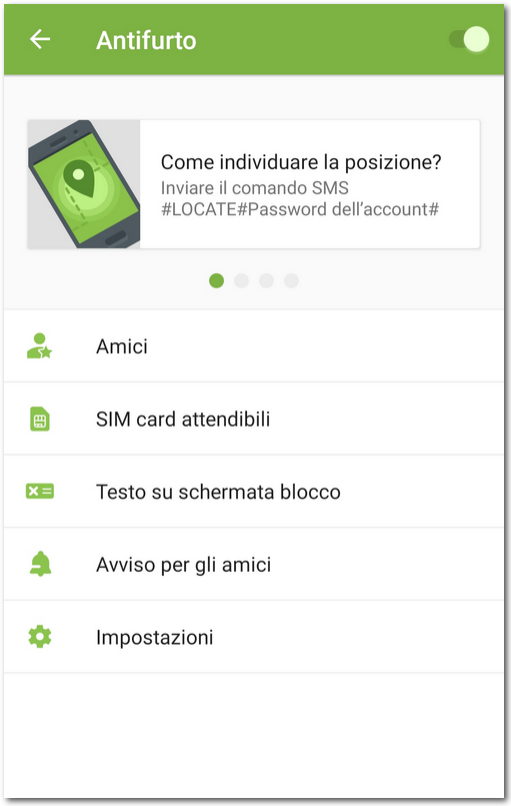

Immagine 18. Antifurto Dr.Web

Schede con i comandi SMS

È disponibile solo nella versione dell'applicazione dal sito Doctor Web.

Le schede con i comandi SMS sono situate nella parte superiore della schermata **Antifurto** (v. Immagine 18).

- Per visualizzare tutti i comandi SMS, scorrere le schede verso destra.
- Per aprire la descrizione completa di un comando SMS o inviare un comando SMS, premere la scheda con questo comando.

Amici

Amici — contatti ai quali l'utente si affida per la gestione del dispositivo tramite comandi, o i quali si affidano all'utente. Nell'applicazione gli amici sono suddivisi in due schede: Mi fido di e Si fidano di me.

Mi fido di

In questa scheda è situata la lista degli amici cui l'utente si affida per la gestione del dispositivo tramite comandi. L'utente ha aggiunto agli amici questi contatti indicando i loro numeri di telefono o indirizzi email.

Icona	Versione dell'applicazione	Commento
	Solo la versione dal sito Doctor Web	L'utente ha aggiunto un numero di telefono. L'amico può inviare i comandi SMS senza password sul dispositivo dell'utente.
	Qualsiasi	L'utente ha aggiunto un indirizzo email. L'amico non ha ancora confermato la richiesta di amicizia e non può inviare i comandi push ad Antifurto. Per confermare la richiesta, sul dispositivo dell'amico aggiunto devono essere installate l'applicazione Dr.Web Security Space o la versione gratuita Dr.Web Light. La richiesta potrebbe essere stata saltata. Se necessario, inviare una seconda richiesta.
	Qualsiasi	L'utente ha aggiunto un indirizzo email. L'amico ha confermato la richiesta di amicizia e può inviare i comandi push ad Antifurto. • Se sul dispositivo dell'amico è installata l'applicazione Dr.Web Security Space, l'amico può inviare qualsiasi comando. • Se sul dispositivo dell'amico è installata l'applicazione Dr.Web Light, l'amico può aiutare a sbloccare il dispositivo se è stato bloccato da Antifurto e l'utente non si ricorda più la password.
	Qualsiasi	L'utente ha aggiunto un indirizzo email, ma l'amico ha rifiutato la richiesta di amicizia. L'amico non può inviare i comandi push ad Antifurto. In tale caso il contatto può essere rimosso dalla lista degli amici.

Per aggiungere un amico

- Nella scheda **Mi fido di** premere l'icona  .
  - **Per la versione dell'applicazione dal sito Doctor Web**. Aggiungere un numero di telefono. Sarà possibile inviare da questo numero sul dispositivo i comandi SMS senza password. Per questo scopo, selezionare una delle opzioni:
    -  **Contatti** — seleziona un telefono dai contatti sul dispositivo.
    -  **Registro chiamate** — seleziona un telefono dalle chiamate recenti.
    -  **Registro SMS** — seleziona un telefono dai messaggi SMS recenti.
    -  **Nuovo contatto** — inserisci un nuovo numero di telefono.
  - **Per qualsiasi versione dell'applicazione**. Aggiungere un indirizzo email. Sull'indirizzo indicato verrà inviata un'email con la richiesta di amicizia. La richiesta può essere confermata nell'applicazione Dr.Web Security Space o nella versione gratuita Dr.Web Light. Dopo aver confermato la richiesta, l'amico potrà inviare i comandi ad Antifurto tramite

notifiche. Da Dr.Web Light sarà possibile inviare il comando di sblocco del dispositivo e reset della password se il dispositivo verrà bloccato. Da Dr.Web Security Space sarà possibile inviare qualsiasi comando.

In totale è possibile aggiungere fino a cinque indirizzi email (e fino a cinque numeri di telefono — nella versione dell'applicazione dal sito Doctor Web).

Per modificare il contatto di un amico

1. Nella scheda **Mi fido di** selezionare il contatto richiesto.
2. Premere l'icona .
3. Apportare modifiche.
4. Premere l'icona per salvare le modifiche.

> Il record non può essere modificato se questo contatto ha rifiutato la richiesta di amicizia.

Per rimuovere un amico

- Far scorrere il dito con il contatto corrispondente verso sinistra.

  Se si rimuove accidentalmente un contatto sbagliato dalla lista degli amici, è possibile annullare la rimozione premendo **Annulla**.

Si fidano di me

Nella scheda **Si fidano di me** si trova la lista degli amici che si affidano all'utente per la gestione del loro dispositivo. Hanno aggiunto l'utente agli amici in Antifurto Dr.Web indicandone l'indirizzo email. Per poter gestire da remoto il dispositivo di un amico, è necessario confermare la richiesta di amicizia.

Stati delle richieste di amicizia

Icona	Commento
	La richiesta di amicizia non è ancora stata confermata dall'utente. Per poter inviare i comandi push sul dispositivo dell'amico, confermare la richiesta di amicizia.
	La richiesta di amicizia è stata confermata dall'utente, è possibile gestire da remoto il dispositivo dell'amico tramite i comandi push.
	L'utente è stato rimosso dalla lista amici. Affinché l'utente possa inviare i comandi push, l'amico deve inviare una seconda richiesta.

Per confermare una richiesta di amicizia

Eseguire una delle seguenti azioni:

- Premere l'avviso di richiesta che si è ricevuto dopo che si è stati aggiunti agli amici e premere **Conferma**.
- Selezionare il contatto richiesto sulla scheda **Si fidano di me** e premere **Conferma**.

Per rifiutare una richiesta di amicizia

Eseguire una delle seguenti azioni:

- Premere l'avviso di richiesta che si riceve dopo che si è stati aggiunti agli amici e premere **Rifiuta**.
- Selezionare il contatto richiesto sulla scheda **Si fidano di me** e premere **Rifiuta**.
- Rimuovere il contatto dalla lista amici.

Per modificare il contatto di un amico

1. Nella scheda **Si fidano di me** selezionare il contatto richiesto.
2. Premere l'icona .
3. Apportare modifiche al record.
4. Premere l'icona per salvare le modifiche.

> Il record non può essere modificato se questo contatto ha cancellato l'utente dagli amici.

Per rimuovere un amico

- Far scorrere il dito con il contatto corrispondente verso sinistra.

  Se si rimuove accidentalmente il contatto di un amico di cui non è stata ancora confermata la richiesta di amicizia, è possibile annullare la rimozione premendo **Annulla**.

Per sbloccare il dispositivo di un amico

1. Premere l'avviso che si è ricevuto dall'amico.
2. Contattare in autonomo l'amico per scoprire il codice di conferma. Non fidarsi di messaggi ricevuti che contengono un codice di conferma, potrebbero essere stati inviati dai malintenzionati.
3. Inserire il codice di conferma.
4. Premere **Sblocca**.

SIM card affidabili

SIM affidabili — lista delle SIM utilizzate nel dispositivo mobile. Di default Antifurto blocca il dispositivo se rileva in esso una SIM non presente sulla lista di quelle affidabili. In questo caso, se il dispositivo verrà rubato e verrà sostituita la SIM, il dispositivo non potrà essere utilizzato. Se una SIM affidabile viene sostituita con un'altra da questa lista, Antifurto non blocca il dispositivo.

Se si utilizzano due SIM alla volta su un dispositivo con Android 5.1 o versioni successive, entrambe le SIM vengono aggiunte in maniera automatica alla lista delle SIM affidabili. Su un dispositivo con Android 5.0 o versioni precedenti è possibile rendere affidabile una sola SIM (non è possibile aggiungere contemporaneamente entrambe le SIM).

Per ciascuna SIM nella lista sono indicati il nome, nonché il suo identificatore (su dispositivi con Android 5.0 o versioni precedenti) o l'operatore di telefonia mobile (su dispositivi con Android 5.1 o versioni successive).

Nuove SIM possono essere aggiunte alla lista delle SIM affidabili al riavvio del dispositivo o all'avvio di Dr.Web.

Premere **SIM card affidabili** per aprire o modificare la lista:

- Per visualizzare informazioni più dettagliate su una SIM, premerla nella lista. A seconda della versione del sistema operativo, possono essere disponibili i seguenti campi: nome, operatore, identificatore.
- Per rinominare una SIM, premerla nella lista. Nella schermata che si è aperta indicare un nuovo nome nel campo **Nome** e premere **Salva**.
- Per cancellare una SIM dalla lista delle SIM affidabili, scorrere il dito verso sinistra.

> La SIM attualmente in uso non può essere cancellata dalla lista delle SIM affidabili.

Testo su schermata blocco

Qui si può modificare un testo che verrà visualizzato sullo schermo del dispositivo bloccato in caso di smarrimento o furto. Per esempio si può indicare un secondo numero di telefono o un indirizzo email per il contatto.

Per modificare il testo sulla schermata di blocco

- Premere **Testo su schermata blocco**, digitare un nuovo testo e premere **Salva**.

Avviso per gli amici

Avviso per gli amici — questo è un avviso che può essere inviato agli amici se Antifurto bloccherà il dispositivo e si dimenticherà la password. Dopo aver ricevuto l'avviso, gli amici devono chiedere all'utente il codice di conferma per resettare la password dell'utente e affinché l'utente possa impostarne una nuova.

Per modificare il testo dell'avviso

- Premere **Avviso per gli amici**, digitare un nuovo testo e premere **Salva**.

Impostazioni

Blocca dopo il riavvio

Di default l'opzione è disattivata.

Se questa opzione è attivata, Antifurto Dr.Web bloccherà il dispositivo dopo ogni riavvio. Per sbloccare il dispositivo, è necessario inserire la password dell'account Dr.Web. Senza la password il dispositivo non può essere sbloccato.

Blocca dopo il cambio della SIM card

Di default l'opzione è attivata.

Se rilevata sul dispositivo una SIM non presente sulla lista delle SIM affidabili, Antifurto Dr.Web bloccherà il dispositivo. Per sbloccare il dispositivo, è necessario inserire la password dell'account Dr.Web. Senza la password il dispositivo non può essere sbloccato.

Invia agli amici un SMS circa la sostituzione della SIM

È disponibile solo nella versione dell'applicazione dal sito Doctor Web.

Di default l'opzione è disattivata.

Se questa opzione è attivata, Antifurto Dr.Web invierà messaggi SMS a tutti i contatti dalla lista degli amici non appena rileverà sul dispositivo una SIM non presente sulla lista di quelle affidabili. Inoltre, Antifurto Dr.Web individuerà il numero associato a questa SIM.

Quando il dispositivo con SIM sostituita viene riavviato, Antifurto invierà nuovamente messaggi SMS ai contatti dalla lista degli amici. Antifurto può inviare un massimo di cinque tali invii SMS al giorno.

Elimina i dati

Di default l'opzione è disattivata.

Se il dispositivo è stato rubato ed è bloccato, un estraneo può provare a sbloccarlo cercando la password a forza bruta. Affinché nessuno possa ottenere l'accesso ai dati, attivare l'opzione **Elimina i dati**.

Dopo che la password verrà inserita 10 volte in modo errato sul dispositivo bloccato:

- Se Dr.Web è attivato come amministratore del dispositivo, le impostazioni del dispositivo verranno ripristinate alle impostazioni di fabbrica (verranno rimosse tutte le applicazioni installate, i dati personali, le fotografie, i messaggi SMS, i contatti, tutte le informazioni dalla scheda di memoria). Notare che il ripristino alle impostazioni di fabbrica rimuoverà anche Dr.Web.
- Se Dr.Web non è attivato come amministratore del dispositivo, verranno rimossi i dati personali (eccetto SMS in quanto Dr.Web non è l'applicazione per la ricezione e l'invio di SMS di default). Dr.Web non verrà rimosso e continuerà a bloccare il dispositivo.

Modalità di funzionamento senza SIM

La modalità di funzionamento senza SIM viene attivata sia quando la SIM è fisicamente assente e sia se il dispositivo impedisce alle applicazioni installate di accedere alle informazioni della SIM. Questo riguarda i dispositivi per cui è previsto l'uso delle SIM.

Non appena Antifurto Dr.Web rileverà che non ha accesso alla SIM, si aprirà una schermata in cui viene chiesto di inserire la password dell'account Dr.Web. Inoltre, nella barra delle notifiche apparirà un messaggio di SIM non trovata. Immettere la password per rendere affidabile la modalità senza SIM. L'invio dei comandi SMS non sarà disponibile, però si potranno utilizzare le altre funzionalità di Antifurto Dr.Web.

8.4.3. Comandi di Antifurto Dr.Web

Utilizzare i comandi di Antifurto Dr.Web per gestire il dispositivo da remoto.

- I comandi push vengono inviati tramite le notifiche push e non vengono visualizzati sul dispositivo del destinatario.
- I comandi SMS vengono inviati tramite i messaggi SMS e vengono visualizzati sul dispositivo del destinatario.

Requisiti per l'utilizzo dei comandi di Antifurto

Dispositivo	Comandi push	Comandi SMS
Mittente	Dispositivo con qualsiasi versione dell'applicazione. Antifurto è attivato, in Antifurto è confermata la richiesta di amicizia del destinatario.	L'installazione dell'applicazione Dr.Web non è richiesta. • Qualsiasi dispositivo se la password è specificata nel comando SMS. • Dispositivo con il numero di telefono aggiunto alla lista amici del destinatario se la password non è specificata nel comando SMS.
Destinatario	Dispositivo con qualsiasi versione dell'applicazione. Antifurto è attivato.	Dispositivo con la versione dell'applicazione dal sito o da HUAWEI AppGallery. Antifurto è attivato.

Un'impostazione di sistema presente su alcuni dispositivi **Schermata di blocco** può ostacolare l'inserimento della password dell'account Dr.Web su un dispositivo bloccato dal comando. Di default, l'impostazione è disattivata. Se veniva attivata, nelle impostazioni del dispositivo aprire **App** > **Dr.Web** > **Altre autorizzazioni** e disattivare l'impostazione **Schermata di blocco**.

8.4.3.1. Comandi push

Cosa sono i comandi push

I comandi push — comandi per la gestione di Antifurto Dr.Web per inviare i quali vengono utilizzate le notifiche push Android. Le notifiche push che contengono comandi push non vengono visualizzate sul dispositivo del destinatario, ma vengono elaborate dall'applicazione.

Non è garantito il corretto funzionamento delle notifiche push in una versione da HUAWEI AppGallery installata su dispositivi diversi da Huawei, in quanto per l'invio possono essere utilizzati servizi mobili non aggiornati alla versione corrente.

Cosa è necessario per utilizzare un comando push

1. Per l'invio e la ricezione dei comandi push i dispositivi devono essere connessi a internet.
2. Sul dispositivo del destinatario deve essere installata l'applicazione Dr.Web Security Space. Sul dispositivo del mittente — Dr.Web Security Space o Dr.Web Light.
3. Sul dispositivo del destinatario deve essere attivato Antifurto.
4. Un comando push può essere inviato solo da un dispositivo su cui è stata precedentemente confermata la richiesta di amicizia del destinatario.

- Dall'applicazione Dr.Web Security Space l'amico può inviare qualsiasi comando push.
- Dall'applicazione Dr.Web Light l'amico può sbloccare il dispositivo del destinatario utilizzando il componente Aiuto all'amico.

Per inviare un comando push

1. Sulla schermata **Antifurto** premere **Amici**.
2. Selezionare la scheda **Si fidano di me**.
3. Selezionare l'amico sul cui dispositivo si deve inviare il comando.
4. Selezionare il comando.

La consegna dei comandi push può richiedere fino a 15 minuti.

Comandi

Un'impostazione di sistema presente su alcuni dispositivi **Schermata di blocco** può ostacolare lo sblocco di un dispositivo bloccato dal comando. Assicurarsi in anticipo che l'impostazione sia disattivata.

Comando	Azione
Individua la posizione	Ricevere le coordinate del dispositivo mobile. In risposta al comando si riceverà un link con le coordinate della posizione del dispositivo sulla mappa. Per indicare la posizione del dispositivo, viene utilizzato Dr.Web Anti-theft Locator — servizio specifico di Doctor Web che visualizza nella finestra del browser una mappa dell'area e la posizione del dispositivo sulla mappa. 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 di trasmissione GSM base più vicine. Dunque, a seconda dei dati ottenuti, le coordinate verranno determinate esattamente (una posizione sulla mappa) o approssimativamente (un cerchio di un determinato raggio). Nella parte superiore della schermata con la mappa è possibile selezionare il servizio di mappe più adatto.
Blocca il dispositivo	Bloccare il dispositivo. Per sbloccare il dispositivo, è necessario inserire la password, dell'account Dr.Web.
Blocca il dispositivo e accendi il segnale acustico	Bloccare il dispositivo e attivare un segnale acustico che suonerà anche dopo il riavvio del dispositivo. Per sbloccare il dispositivo, è necessario inserire la password dell'account Dr.Web.

Comando	Azione
Elimina i dati	Eliminare tutti i dati dal dispositivo. Se Dr.Web è attivato come amministratore sul dispositivo dell'amico, questo comando ripristinerà le impostazioni di fabbrica del dispositivo. Questo comando verrà inoltre eseguito se il dispositivo è bloccato e nelle impostazioni di Antifurto Dr.Web è attivata l'opzione **Elimina i dati**.
Resetta password	Sbloccare il dispositivo e resettare la password dell'account Dr.Web. Per inviare il comando, è richiesto il codice di conferma. Il codice è visualizzato sul dispositivo dell'amico.

8.4.3.2. Comandi SMS

I comandi SMS possono essere inviati solo sui dispositivi su cui è installata la versione dell'applicazione dal sito Doctor Web.

Affinché i comandi SMS funzionino su un telefono Xiaomi con l'applicazione installata **Sicurezza**, in questa applicazione deve essere concesso a Dr.Web il permesso di gestione degli SMS.

I comandi SMS sono comandi per la gestione remota di Antifurto Dr.Web inviati tramite messaggi SMS. Utilizzando i comandi SMS, è possibile scoprire dove si trova il dispositivo mobile, nonché bloccarne le funzioni e rimuovere le proprie informazioni personali.

È possibile inviare un comando SMS nel seguente modo:

- Indicando la password — da qualsiasi dispositivo.
- Senza indicare la password — dal dispositivo di un amico.

Non è consigliabile inviare i comandi SMS con la password su un dispositivo smarrito o rubato: i malintenzionati potrebbero vedere l'SMS con la password ricevuto e sbloccare il dispositivo. In modo da poter inviare un comando SMS senza password, anticipatamente aggiungere i numeri di telefono alla lista degli amici.

Comandi SMS

Un'impostazione di sistema presente su alcuni dispositivi **Schermata di blocco** può ostacolare lo sblocco di un dispositivo bloccato dal comando. Assicurarsi in anticipo che l'impostazione sia disattivata.

Comando	Azione
#LOCK#*Password*#	Bloccare il dispositivo.

Comando	Azione
	In risposta al comando si riceverà un messaggio SMS: "Antifurto Dr.Web - Dispositivo <*nome dispositivo*> è bloccato".
#SIGNAL#*Password*#	Bloccare il dispositivo e attivare un segnale acustico che suonerà anche dopo il riavvio del dispositivo. In risposta al comando si riceverà un messaggio SMS: "Antifurto Dr.Web - Dispositivo <*nome dispositivo*> è bloccato".
#LOCATE#*Password*#	Ricevere le coordinate del dispositivo mobile in un messaggio SMS. In risposta al comando si riceverà un link con le coordinate della posizione del dispositivo sulla mappa. Per indicare la posizione del dispositivo, viene utilizzato Dr.Web Anti-theft Locator — servizio specifico di Doctor Web che visualizza nella finestra del browser una mappa dell'area e la posizione del dispositivo sulla mappa. 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 di trasmissione GSM base più vicine. Dunque, a seconda dei dati ottenuti, le coordinate verranno determinate esattamente (una posizione sulla mappa) o approssimativamente (un cerchio di un determinato raggio). Nella parte superiore della schermata con la mappa è possibile selezionare il servizio di mappe più adatto.
#UNLOCK#*Password*#	Sbloccare il dispositivo senza resettare la password dell'account Dr.Web.
#WIPE#*Password*#	Ripristinare le impostazioni di fabbrica del dispositivo mobile e rimuovere tutti i dati dalla memoria interna del dispositivo. In risposta al comando si riceverà un messaggio SMS: "Antifurto Dr.Web - Eliminazione dei dati sul dispositivo <*nome dispositivo*>". Questo comando verrà inoltre eseguito se il dispositivo è bloccato e nelle impostazioni di Antifurto Dr.Web è attivata l'opzione **Elimina i dati**.
#RESETPASSWORD#	Sbloccare il dispositivo e impostare una nuova password. Questo comando può essere eseguito solo se viene inviato da un numero di telefono indicato nella lista degli amici.

I comandi SMS non fanno distinzione tra maiuscole e minuscole. Per esempio, per bloccare il dispositivo mobile, è possibile inviare il comando **#LOCK#***Password*# nella forma **#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 l'uso di reti wireless per la localizzazione.

Invio di comandi SMS tramite Antifurto Dr.Web

Tramite Antifurto Dr.Web è possibile inviare comandi SMS ai dispositivi su cui anche è attivato Antifurto Dr.Web.

Per inviare un comando SMS

1. Sulla schermata **Antifurto** (v. Immagine 18) premere qualsiasi scheda con un comando SMS.
2. Premere **Invia comando SMS**.
3. Sulla schermata **Invio del comando SMS**:
   1. Nella lista **Comando** selezionare il comando richiesto:
      - **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#.
      - **Sblocca e imposta una nuova password** — corrisponde al comando #RESETPASSWORD#.
   2. Nel campo **A chi** indicare il numero di telefono del destinatario.
   3. Nel campo **Password del destinatario** indicare la password dell'account del destinatario.

      Se il proprio numero è incluso nella lista degli amici del destinatario, si può lasciare vuoto questo campo.
   4. Nella lista **Da chi** selezionare la SIM da cui verrà inviato il comando.

      Questa opzione è disponibile su dispositivi con due SIM con Android 5.1 o versioni successive.
   5. Premere il pulsante **Invia**.

8.4.4. Disattivazione di Antifurto Dr.Web

Per disattivare Antifurto Dr.Web

1. Sulla schermata principale di Dr.Web selezionare **Antifurto**.
2. Inserire la password dell'account Dr.Web o di Antifurto.
3. Sulla schermata **Antifurto** (vedi Immagine 18) disattivare Antifurto utilizzando l'interruttore nell'angolo superiore destro dello schermo.
4. Nella finestra apparsa premere **OK**.

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

8.5. Parental control

Tramite Parental control il proprietario dell'account Dr.Web può vietare l'accesso a qualsiasi applicazione o gruppo di applicazioni installate, nonché alle impostazioni dei componenti Dr.Web.

Come funziona Parental control

Sul dispositivo al cui utente si vuole bloccare l'accesso alle applicazioni e alle impostazioni dei componenti Dr.Web deve essere installata l'applicazione Dr.Web. Si attiva il componente Parental control sul dispositivo dell'utente e si indicano i parametri del proprio account Dr.Web. Dopo aver attivato il componente, si impostano le limitazioni all'accesso dell'utente del dispositivo alle applicazioni, ai gruppi di applicazioni o alle impostazioni dei componenti Dr.Web. Al tentativo di avviare un'applicazione bloccata o aprire le impostazioni di un componente l'utente del dispositivo vede una schermata di blocco o la schermata di inserimento della password. L'accesso a un'applicazione o un componente bloccato è possibile solo dopo l'inserimento della password dell'account Dr.Web o il riconoscimento dell'impronta digitale impostata.

Funzioni principali di Parental control

Parental control consente di:

- vietare completamente l'accesso a un'applicazione o un gruppo di applicazioni;
- vietare completamente l'accesso alle impostazioni dei componenti Dr.Web;
- creare le limitazioni all'accesso a un'applicazione o un gruppo di applicazioni in un intervallo di tempo impostato;
- creare gruppi personalizzati di applicazioni bloccate;
- tenere traccia degli eventi relativi alle applicazioni e ai componenti bloccati.

Attivazione di Parental control

Per attivare Parental control

1. Sulla schermata principale di Dr.Web selezionare **Parental control**.
2. Se sul dispositivo non è stato creato l'account Dr.Web, crearlo.

Se l'account è stato creato, inserire la password dell'account. Se viene inserita una password errata 10 volte di seguito, il campo di inserimento della password verrà temporaneamente bloccato. Si vedrà quanto tempo manca al tentativo successivo.

3. Sulla schermata **Parental control** premere il pulsante **Attiva**.
4. Se Dr.Web non è amministratore del dispositivo, attivare l'applicazione come amministratore. Questo aiuterà a prevenire la rimozione indesiderata dell'applicazione. Inoltre, in caso di smarrimento o furto del dispositivo, si potranno proteggere i propri dati riportando il dispositivo alle impostazioni di fabbrica tramite Antifurto Dr.Web.

Disattivazione di Parental control

Per disattivare Parental control

1. Sulla schermata principale di Dr.Web selezionare **Parental control**.
2. Inserire la password dell'account Dr.Web.
3. Disattivare Parental control utilizzando l'interruttore nell'angolo superiore destro dello schermo e premere **OK**.

Modalità tutorial

Nella parte superiore della schermata principale del componente Parental control (v. Immagine 19) sono disponibili mini-slide che consentono di passare alla modalità tutorial. La modalità tutorial aiuta a familiarizzare velocemente con le funzioni principali di Parental control.

La modalità tutorial è composta da quattro sezioni:

- Applicazioni: divieto dell'accesso ad applicazioni e gruppi di applicazioni.
- Accesso per orario: limitazione dell'accesso ad applicazioni e gruppi di applicazioni in base a un orario.
- Componenti: divieto dell'accesso alle impostazioni dei componenti Dr.Web.
- Impostazioni: le impostazioni e il log di Parental control.

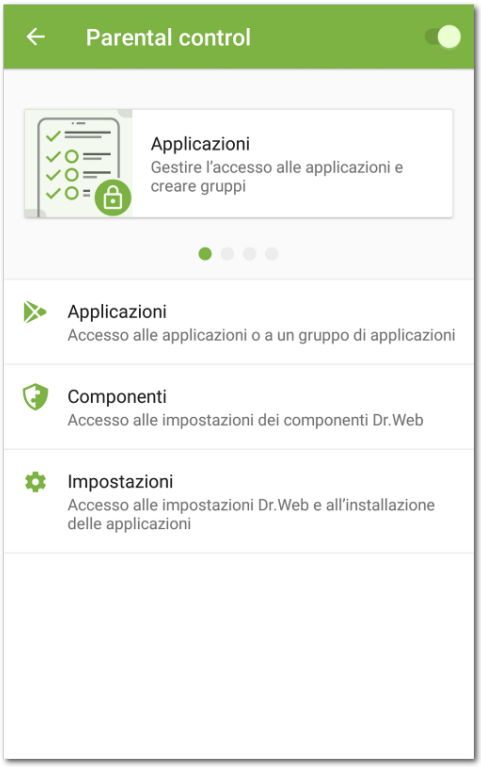

Immagine 19. Parental control

Le mini-slide consentono di aprire una delle sezioni della modalità tutorial. Far scorrere il dito con una mini-slide verso sinistra o destra per passare alla mini-slide successiva o precedente. Premere una mini-slide per aprire la sezione corrispondente della modalità tutorial.

In modalità tutorial sono disponibili slide a schermo intero che mostrano come utilizzare le funzioni principali di Parental control (v. Immagine 20). Far scorrere la slide corrente verso sinistra per passare a quella successiva.

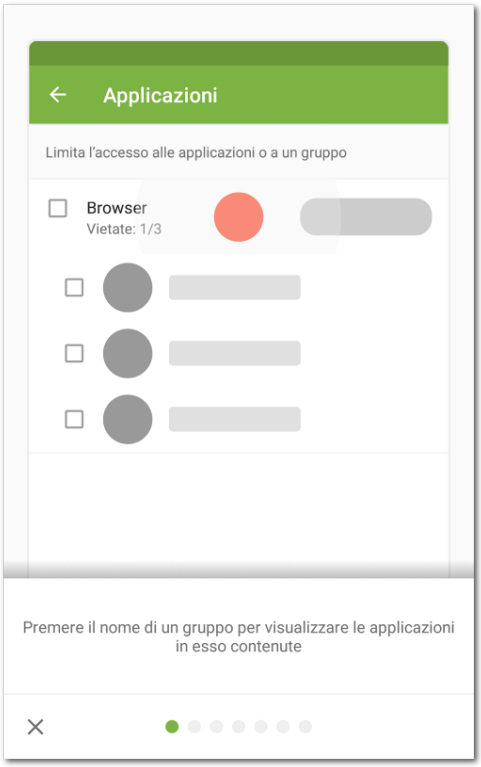

Immagine 20. Slide della modalità tutorial

Per uscire dalla modalità tutorial, premere ✕ nell'angolo inferiore sinistro dello schermo.

8.5.1. Blocco dell'accesso ad applicazioni e componenti

Applicazioni

La sezione **Applicazioni** contiene la lista di tutte le applicazioni installate sul dispositivo.

Divieto dell'accesso ad applicazioni e gruppi di applicazioni

Il componente Parental control consente di bloccare l'accesso a singole applicazioni o interi gruppi di applicazioni. Al tentativo di apertura di un'applicazione l'accesso a cui è vietato o limitato compare una schermata di blocco applicazione che chiude l'accesso all'applicazione stessa. L'accesso all'applicazione può essere ottenuto tramite la password dell'account Dr.Web o l'impronta digitale impostata.

Per vietare l'accesso a un'applicazione o a tutte le applicazioni di un gruppo, spuntare il flag di fronte al nome dell'applicazione o del gruppo. Per consentire nuovamente l'accesso, togliere il flag.

Gruppi di applicazioni

Di default le applicazioni sono divise in gruppi di sistema per categoria. Per visualizzare le applicazioni in un gruppo, premere il nome del gruppo.

> Sui dispositivi con Android 8.0 e versioni precedenti tutte le applicazioni rientrano nel gruppo di sistema **Altre**.

È anche possibile creare gruppi di applicazioni personalizzati.

Per creare un gruppo personalizzato

1. Premere l'icona nell'angolo inferiore destro dello schermo.
2. Nel menu che si è aperto selezionare **Nuovo gruppo**.
3. Inserire un nome per il nuovo gruppo.
4. Premere di fronte alle applicazioni che si vogliono aggiungere al nuovo gruppo.
5. Premere per salvare il nuovo gruppo.

I gruppi personalizzati vengono visualizzati in cima alla lista dei gruppi di applicazioni.

Per modificare un gruppo personalizzato

1. Far scorrere il dito con il nome del gruppo verso sinistra.
2. Premere l'icona .
3. Apportare le modifiche richieste.
4. Premere l'icona nell'angolo superiore destro dello schermo.

Per rimuovere un gruppo personalizzato

1. Far scorrere il dito con il nome del gruppo verso sinistra.
2. Premere l'icona .

Per rimuovere più gruppi personalizzati

1. Premere e tenere premuto il nome di uno dei gruppi da rimuovere.
2. Selezionare gli altri gruppi da rimuovere.
3. Rimuovere i gruppi premendo l'icona nell'angolo superiore destro dello schermo.

> I gruppi di sistema non possono essere modificati o rimossi.

Se nelle impostazioni di Parental control è attivata l'opzione **Vieta i browser senza filtro URL** o **Vieta l'avvio di nuove applicazioni**, nella lista delle applicazioni compare rispettivamente il gruppo di sistema **Browser senza Filtro URL** o **Nuove applicazioni**. Per consentire l'accesso alle applicazioni da questi gruppi, disattivare l'opzione corrispondente nelle impostazioni di Parental control.

Ricerca nella lista delle applicazioni

Per comodità di navigazione nella lista delle applicazioni è possibile utilizzare la ricerca.

Per eseguire la ricerca per nome di un'applicazione o un gruppo

1. Premere l'icona nell'angolo inferiore destro dello schermo.
2. Nel menu che si è aperto selezionare **Ricerca**.
3. Inserire la richiesta nel campo di ricerca nella parte inferiore dello schermo.

Limitazione dell'accesso per orario

È possibile bloccare l'accesso a gruppi di applicazioni su base continuativa e in periodi di tempo impostati.

Il tipo di blocco viene visualizzato a destra del nome del gruppo. Sono possibili due tipi di blocco:

- **Sempre** — l'accesso al gruppo è bloccato in modo permanente.
- **Intervallo** — l'accesso al gruppo è bloccato in un determinato periodo di tempo.

Di default quando un gruppo di applicazioni viene bloccato, l'accesso viene sempre bloccato.

Per impostare un periodo di blocco

1. Premere il tipo di blocco a destra del gruppo di applicazioni.
2. Premere nell'angolo inferiore destro dello schermo.
3. Selezionare i giorni della settimana in cui sarà attiva la limitazione.
4. Premere **Inizio** e impostare l'ora di inizio della limitazione.
5. Premere **OK** per confermare l'ora di inizio selezionata.
6. Premere **Fine** e impostare l'ora di fine della limitazione.
7. Premere **OK** per confermare l'ora di fine selezionata.
8. Premere nell'angolo superiore destro dello schermo per salvare la limitazione.

Per una singola limitazione può essere impostato un solo intervallo di tempo. Per bloccare il gruppo di applicazioni in altri giorni della settimana e orari, creare ulteriori limitazioni.

Le limitazioni possono essere modificate e rimosse.

Per modificare una limitazione

1. Premere il tipo di blocco a destra del gruppo di applicazioni.
2. Far scorrere il dito con la limitazione verso sinistra.
3. Premere l'icona .
4. Apportare le modifiche richieste.
5. Salvare le modifiche premendo l'icona nell'angolo superiore destro dello schermo.

Per rimuovere una limitazione

1. Premere il tipo di blocco a destra del gruppo di applicazioni.
2. Far scorrere il dito con la limitazione verso sinistra.
3. Premere l'icona .

Componenti

Oltre a vietare l'accesso ad applicazioni o gruppi di applicazioni, è anche possibile vietare l'accesso alle impostazioni di componenti Dr.Web: Filtro chiamate ed SMS, Filtro URL, Firewall, nonché alle impostazioni dell'applicazione Dr.Web.

Per vietare l'accesso alle impostazioni dei componenti

1. Sulla schermata principale di Parental control selezionare la sezione **Componenti**.
2. Spuntare i flag di fronte ai componenti Dr.Web l'accesso a cui si vuole vietare:

- Filtro chiamate ed SMS. Consente al proprietario dell'account di creare liste di numeri da cui l'utente del dispositivo può ricevere chiamate e messaggi. Per esempio, è possibile consentire le chiamate e i messaggi SMS in arrivo solo da determinati numeri o dai numeri dalla lista dei contatti. L'utente del dispositivo non potrà modificare la lista dei numeri consentiti o vietati.
- Filtro URL. Consente al proprietario dell'account di limitare l'accesso dell'utente del dispositivo a determinati siti, pagine web, nonché categorie di siti (per esempio "Droga", "Armi", "Terrorismo", "Siti per adulti" ecc.). L'utente del dispositivo non potrà modificare la lista dei siti e delle categorie di siti a cui ha accesso.
- Firewall Consente al proprietario dell'account di limitare l'utilizzo del traffico mobile, controllare il trasferimento dei dati e gestire le connessioni internet delle applicazioni sul dispositivo dell'utente. L'utente non potrà modificare le regole e limitazioni impostate.
- Impostazioni Dr.Web. Consente al proprietario dell'account di vietare all'utente del dispositivo di accedere alle impostazioni Dr.Web e modificarle. Per esempio, l'utente non potrà resettare le impostazioni.

Per i componenti Dr.Web non è possibile impostare una limitazione di accesso per orario. L'accesso sarà sempre vietato.

Per accedere a un componente bloccato, è richiesto inserire la password dell'account Dr.Web o scansionare l'impronta digitale (se è attiva l'impostazione corrispondente).

Schermata di blocco

Al tentativo di avvio di un'applicazione bloccata compare una schermata di blocco (v. Immagine 21). Per accedere all'applicazione è necessario inserire la password dell'account e premere il pulsante **Sblocca**. È anche possibile ottenere l'accesso all'applicazione tramite l'impronta digitale se nelle impostazioni di Parental control è attivata l'opzione **Sblocco mediante impronta digitale**.

Immagine 21. Schermata di blocco applicazione

Nuove applicazioni

Se nelle impostazioni di Parental control è attivata l'opzione **Vieta l'avvio di nuove applicazioni**, tutte le applicazioni installate dopo l'attivazione dell'opzione ricadono in un gruppo di sistema bloccato **Nuove applicazioni**. All'avvio di un'applicazione dal gruppo **Nuove applicazioni** sulla schermata di blocco è disponibile un'opzione attraverso cui è possibile consentire l'accesso all'applicazione su base continuativa.

Per consentire l'accesso a una nuova applicazione

1. Avviare l'applicazione richiesta.
2. Sulla schermata di blocco inserire la password dell'account Dr.Web.
3. Spuntare il flag di fronte all'opzione **Escludi dal gruppo "Nuove applicazioni"**.
4. Premere il pulsante **Sblocca**.

8.5.2. Impostazioni di Parental control

Alla sezione **Impostazioni** (v. Immagine 22) è possibile passare dalla schermata principale del componente. La sezione consente di gestire le impostazioni di Parental control, nonché passare al log di Parental control.

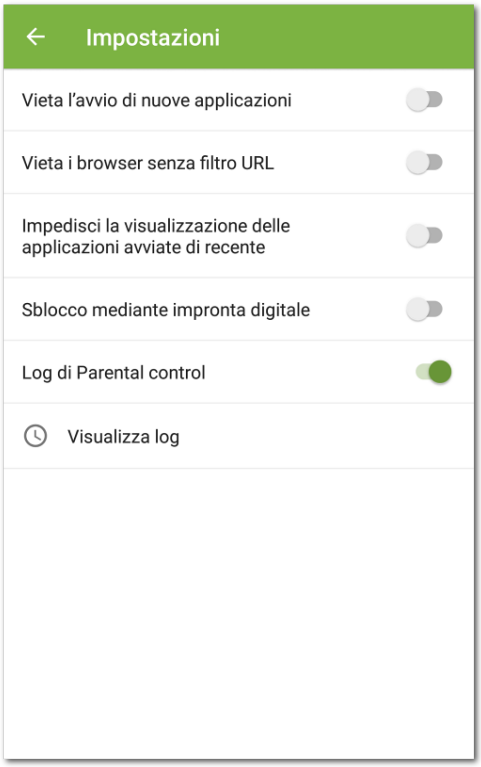

Immagine 22. Impostazioni di Parental control

Nella sezione **Impostazioni** sono disponibili le seguenti opzioni:

- **Vieta l'avvio di nuove applicazioni**. Consente di vietare l'accesso alle applicazioni che vengono installate sul dispositivo dopo l'attivazione dell'opzione. Le nuove applicazioni vengono incluse in un gruppo di sistema **Nuove applicazioni**. L'accesso alle applicazioni del gruppo è sempre vietato.

  L'accesso a un'applicazione specifica può essere consentito tramite l'opzione **Escludi dal gruppo "Nuove applicazioni"** sulla schermata di blocco di questa applicazione.

- **Vieta i browser senza filtro URL**. Consente di vietare l'accesso ai browser non supportati da Filtro URL. I browser vengono inclusi in un gruppo di sistema **Browser senza Filtro URL**. L'accesso alle applicazioni di questo gruppo è sempre vietato.

  

  Per l'attivazione dell'opzione è necessario che sul dispositivo sia attivato Filtro URL.

- **Impedisci la visualizzazione delle applicazioni avviate di recente**. Consente di vietare l'invocazione della schermata delle applicazioni avviate di recente sul dispositivo. Al tentativo di invocare la schermata delle applicazioni avviate di recente comparirà una schermata di blocco.

  

  In caso di utilizzo di shell di sistema di terze parti l'opzione potrebbe non funzionare correttamente.

- **Sblocco mediante impronta digitale**. Consente di utilizzare l'impronta digitale invece della password dell'account Dr.Web per lo sblocco delle applicazioni e dei componenti.

  

  Prima di attivare l'opzione, assicurarsi che sul dispositivo sia registrata solo l'impronta digitale del proprietario dell'account Dr.Web.

  Il lettore di impronte digitali verrà disattivato dopo ripetuti errori di riconoscimento dell'impronta. Per la riattivazione del lettore è necessario sbloccare il dispositivo in un altro modo impostato (sequenza di sblocco, codice PIN o password).

- **Log di Parental control**. Attiva la registrazione del log di Parental control. Dopo l'attivazione dell'opzione è disponibile l'opzione **Visualizza log**.

8.5.3. Log di Parental control

Nel log di Parental control vengono registrati gli eventi relativi ad applicazioni e componenti l'accesso a cui è vietato o limitato.

Di default gli eventi del log di Parental control sono presentati sotto forma di lista di eventi raggruppati per data. Vengono registrati nel log i seguenti eventi:

- Eventi delle applicazioni:
  - tentativo di avvio
  - sblocco.
- Eventi dei componenti e di Parental control:
  - attivazione
  - disattivazione.

Per ciascun evento è indicato il tempo.

Visualizzazione degli eventi nel log

Per comodità di lettura è possibile gestire la visualizzazione degli eventi nel log di Parental control: ordinare, filtrare o raggruppare gli eventi. Inoltre, è disponibile la ricerca per evento.

Filtro eventi

Per ordinare o filtrare gli eventi in base a un parametro impostato, premere l'icona nell'angolo inferiore destro dello schermo e selezionare **Filtro**.

Sono disponibili le seguenti opzioni di ordinamento:

- prima i meno recenti,
- prima i più recenti,
- in ordine alfabetico A-Z,
- in ordine alfabetico dalla Z alla A.

È anche possibile impostare un filtro per tipo di evento: sblocco, tentativo di avvio delle applicazioni; attivazione, disattivazione dei componenti.

Per ordinare o filtrare la lista degli eventi, selezionare i valori richiesti e tornare alla lista degli eventi.

È possibile ripristinare la visualizzazione di eventi di default premendo nell'angolo superiore destro della schermata **Filtro eventi**.

Ricerca

Per cercare nel log degli eventi di Parental control

1. Premere l'icona nell'angolo inferiore destro dello schermo.
2. Nel menu che si è aperto selezionare **Ricerca**.
3. Inserire la richiesta nel campo di ricerca nella parte inferiore dello schermo.

Raggruppamento

È possibile raggruppare gli eventi per applicazione o componente. Con questo tipo di raggruppamento il log di Parental control costituisce una lista di applicazioni e componenti i cui eventi sono stati registrati nel log (v. Immagine 23).

Per raggruppare gli eventi del log di Parental control, sulla schermata del log premere **Menu** nell'angolo superiore destro e spuntare il flag **Raggruppa**. Premere il nome di un'applicazione

o di un componente per espandere la lista degli eventi relativi a tale applicazione o componente.

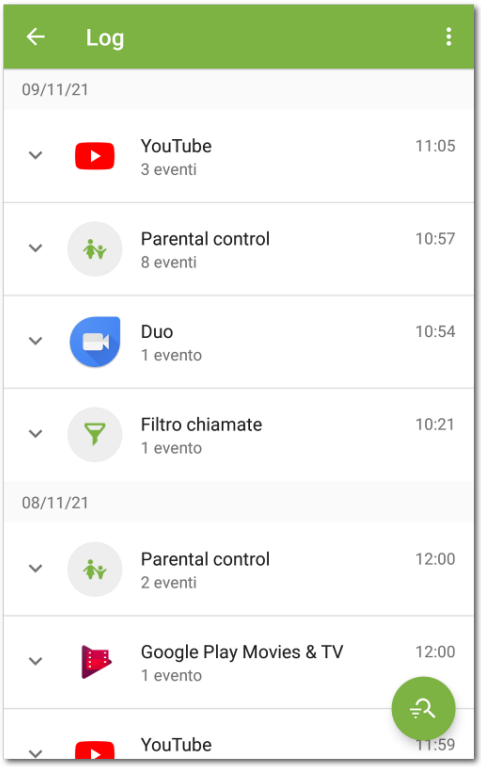

Immagine 23. Raggruppamento di eventi

Filtro gruppi

Se desiderato, è possibile ordinare i gruppi di eventi in base a un determinato parametro.

Per ordinare gli eventi raggruppati

1. Premere l'icona nell'angolo inferiore destro dello schermo.
2. Selezionare l'opzione **Filtro**.
3. Sulla schermata **Filtro gruppi** selezionare il tipo di ordinamento.
4. Tornare alla lista degli eventi.

È possibile ripristinare la visualizzazione di eventi di default premendo nell'angolo superiore destro della schermata **Filtro gruppi**.

Salvataggio del log

Per salvare il log degli eventi in file, sulla schermata del log premere **Menu** nell'angolo superiore destro e selezionare **Salva il log**.

Il log viene salvato nel file `DrWeb_Parental_Log.txt` situato nella cartella `Android/data/com.drweb/files` nella memoria interna del dispositivo.

Sui dispositivi con Android 11.0 o versioni successive il log viene salvato nella cartella `Download/DrWeb`.

Pulizia del log

Per rimuovere tutti gli eventi dal log di Parental control, sulla schermata del log premere **Menu** e selezionare la voce **Cancella il log**.

8.6. Firewall Dr.Web

Firewall Dr.Web protegge il dispositivo mobile da accessi non autorizzati dall'esterno e previene fughe di dati importanti attraverso la rete. Consente di controllare le connessioni e il trasferimento di dati attraverso la rete e di bloccare connessioni sospette.

Caratteristiche dell'utilizzo

Firewall Dr.Web è realizzato sulla base della tecnologia di VPN per Android, il che gli permette di funzionare senza l'ottenimento dei permessi di superutente (root) sul dispositivo. La realizzazione della tecnologia di VPN su Android è associata con alcune limitazioni:

- In ciascun momento solo un'applicazione alla volta sul dispositivo può utilizzare la VPN. Di conseguenza, quando un'applicazione abilita la VPN sul dispositivo, si apre una finestra con la richiesta del permesso di utilizzare la VPN per questa applicazione. Se l'utente concede tale permesso, l'applicazione inizia a utilizzare la VPN; mentre un'altra applicazione che utilizzava la VPN fino a quel momento perde questa possibilità. Tale richiesta compare alla prima attivazione di Firewall Dr.Web. Inoltre, può comparire al riavvio del dispositivo e quando la VPN viene richiesta da altre applicazioni. La VPN deve essere condivisa nel tempo tra le applicazioni, e Firewall è in grado di funzionare solo quando possiede completamente i permessi di utilizzo della VPN.
- L'abilitazione di Firewall Dr.Web può portare all'impossibilità di connettere il dispositivo su cui è in esecuzione ad altri dispositivi direttamente attraverso Wi-Fi o una rete locale. Questo dipende dal modello del dispositivo e dalle applicazioni utilizzate per la connessione.
- Con Firewall Dr.Web attivato non è possibile utilizzare il dispositivo come un punto di accesso Wi-Fi.

La tecnologia VPN per Android viene utilizzata solo per l'implementazione delle funzioni di Firewall, tuttavia, non viene creato alcun tunnel VPN e il traffico internet non viene cifrato.

Per attivare Firewall Dr.Web

1. Sulla schermata principale di Dr.Web selezionare l'opzione **Firewall**.
2. Premere il pulsante **Attiva** o utilizzare l'interruttore nell'angolo superiore destro dello schermo.

   Dr.Web chiede il permesso di connettersi alla VPN. Affinché il firewall possa funzionare, è necessario concedere questo permesso.

Per attivare Firewall dopo un avvio del dispositivo, aprire l'applicazione Dr.Web.

Sui dispositivi con Android 7.0 o versioni successive è possibile configurare l'attivazione automatica di Firewall Dr.Web dopo il riavvio del dispositivo. A tal fine:

1. Nelle impostazioni del dispositivo selezionare **VPN**.
2. Aprire le impostazioni di rete di **Dr.Web**.
3. Sulla schermata **Dr.Web** attivare l'impostazione **VPN permanente**.

Sui dispositivi con Android 8.0 o versioni successive è possibile bloccare l'accesso a internet dopo l'avvio del dispositivo fino a quando non comparirà la connessione alla VPN. A tal fine abilitare l'impostazione **Connettiti solo tramite VPN**.

Se i permessi di utilizzo di VPN passano a un'altra applicazione, Firewall Dr.Web viene disattivato, di cui sarà visualizzato un avviso corrispondente nella sezione delle notifiche. Per attivare nuovamente Firewall Dr.Web, basta premere questo avviso.

Se si utilizza il dispositivo in modalità di accesso limitato (profilo ospite), le impostazioni di Firewall Dr.Web non saranno disponibili.

Schermata iniziale

Sulla schermata iniziale di Firewall sono situate schede con informazioni dalle sue sezioni:

- Limitazione di traffico (se è presente una limitazione attiva): visualizza informazioni sulla limitazione di traffico corrente.
- Applicazioni attive: visualizza un diagramma della quantità di traffico in entrata e in uscita utilizzato dalle connessioni di rete attive delle applicazioni.
- Tutte le applicazioni: visualizza la quantità complessiva di traffico in entrata e in uscita utilizzato dalle applicazioni installate sul dispositivo.

Premere **Più nel dettaglio** sulle schede del traffico delle applicazioni e della limitazione di traffico per passare alla sezione corrispondente.

Il menu nell'angolo superiore destro della schermata iniziale consente di:

- passare alla configurazione della limitazione di traffico mobile;

- aprire il log di Firewall.

8.6.1. Gestione dell'attività di rete delle applicazioni

Firewall Dr.Web consente di controllare l'utilizzo del traffico sul dispositivo e configurare le impostazioni generali di accesso internet delle applicazioni. Le possibilità di gestione generale includono:

- monitoraggio in tempo reale del traffico attivo delle applicazioni;
- visualizzazione della lista delle applicazioni che utilizzavano il traffico internet e della quantità di traffico da esse consumato;
- gestione dell'accesso delle applicazioni al trasferimento dati via Wi-Fi, internet mobile e in roaming;
- limitazione del consumo di traffico complessivo durante un periodo di tempo impostato.

8.6.1.1. Applicazioni attive

Nella sezione **Applicazioni attive** viene visualizzata in tempo reale la lista delle connessioni attive avviate dalle applicazioni installate sul dispositivo. La sezione fornisce un rapido accesso alla gestione del traffico internet corrente delle applicazioni.

Sulla scheda della sezione sulla schermata iniziale di Firewall vengono visualizzate le applicazioni con il maggior traffico attivo. Premere **Più nel dettaglio** per aprire la lista completa delle applicazioni con connessioni attive.

Per ciascuna applicazione sulla schermata **Applicazioni attive** (v. Immagine 24) sono visualizzate le seguenti informazioni:

- Quantità complessiva di traffico in entrata e in uscita sulle connessioni stabilite.
- Accesso al trasferimento dati via Wi-Fi, internet mobile e in roaming.
- Presenza di impostazioni utente. Le applicazioni con accesso a trasferimento dati modificato sono contrassegnate dal badge .
- Presenza di minacce di sistema con connessione internet bloccata. Le applicazioni di sistema con accesso a trasferimento dati bloccato sono contrassegnate dal badge .

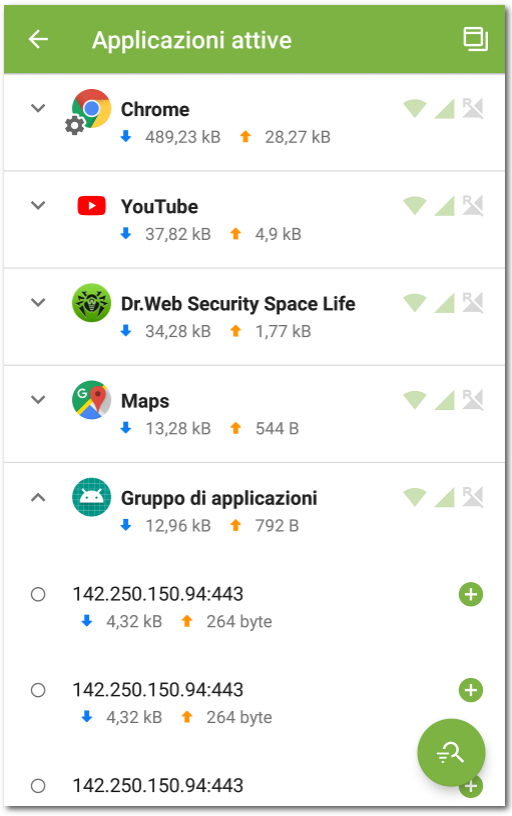

Immagine 24. Applicazioni attive

Connessioni delle applicazioni

Premere l'icona ⌄ a sinistra del nome di un'applicazione sulla schermata **Applicazioni attive** per vedere informazioni dettagliate sulle connessioni stabilite dall'applicazione:

- lista delle connessioni stabilite;
- quantità di traffico in entrata e in uscita su ciascuna delle connessioni stabilite;
- presenza per la connessione di una regola:
  - 🟢 di permesso,
  - 🔴 di divieto,
  - 🟠 di reindirizzamento,
  - ○ nessuna regola impostata.

Per copiare l'indirizzo di una connessione, premere e tenere premuta la riga con l'indirizzo della connessione. L'indirizzo verrà copiato negli appunti.

Premere la riga di una connessione per passare alla schermata Connessione.

Regole delle connessioni

È possibile gestire le connessioni che vengono stabilite dalle applicazioni tramite le regole di permesso, di divieto e di reindirizzamento (v. sezione Regole delle connessioni). Per creare o modificare una regola, premere l'icona o a destra di una connessione.

Ordinamento delle applicazioni

Per ordinare la lista delle applicazioni, premere l'icona nell'angolo inferiore destro dello schermo, quindi premere **Filtro** e selezionare i parametri di ordinamento richiesti:

- traffico decrescente — le applicazioni con il maggior traffico in cima alla lista;
- traffico crescente — le applicazioni con il minor traffico in cima alla lista;
- in ordine alfabetico dalla A alla Z;
- in ordine alfabetico dalla Z alla A.

Di default le applicazioni sono ordinate per traffico decrescente (le applicazioni con il maggior traffico si trovano in cima alla lista). Per ripristinare l'ordinamento di default, premere l'icona sulla schermata **Filtro**.

Ricerca

Per passare rapidamente a un'applicazione richiesta, utilizzare la ricerca per nome di applicazione. Per fare ciò, premere l'icona nell'angolo inferiore destro dello schermo, quindi premere **Ricerca** e inserire la richiesta nel campo di ricerca nella parte inferiore dello schermo.

Finestra mobile

Per avere la possibilità di vedere sempre le connessioni internet attive e controllare la quantità di traffico in entrata e uscita, è possibile attivare una finestra mobile che verrà visualizzata sopra tutte le applicazioni (v. Immagine 25).

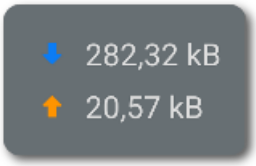

Immagine 25. Finestra mobile

Per attivare la finestra mobile

1. Aprire la schermata **Applicazioni attive** e premere l'icona nell'angolo superiore destro dello schermo (v. Immagine 24).
2. Consentire all'applicazione di visualizzare la finestra mobile sopra le altre finestre.

   Se il permesso di visualizzazione della finestra mobile sopra altre finestre è revocato, la finestra mobile non viene più visualizzata. Per attivarla nuovamente, premere l'icona nell'angolo superiore destro dello schermo e concedere il permesso richiesto.

   La quantità totale di traffico utilizzato viene calcolata dal momento dell'attivazione della finestra.

- Per aprire la lista delle applicazioni che usano la connessione internet (v. Immagine 26), premere la finestra mobile.
- Per chiudere la lista delle applicazioni, premere .

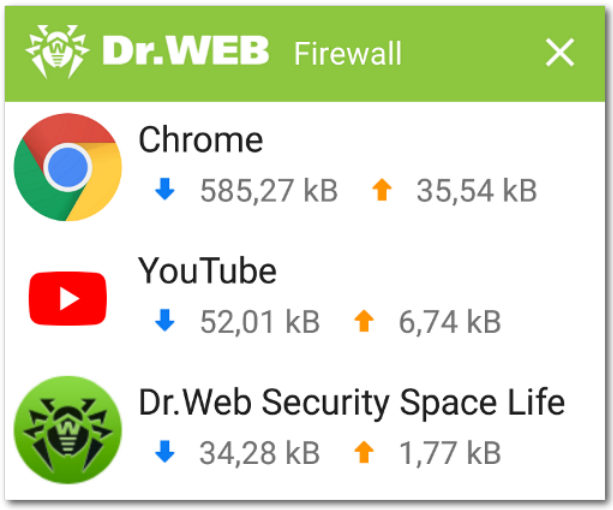

Immagine 26. Lista delle applicazioni che usano la connessione internet

Per disattivare la finestra mobile

- Aprire la schermata **Applicazioni attive** e premere l'icona nell'angolo superiore destro dello schermo.

8.6.1.2. Tutte le applicazioni

Nella sezione **Tutte le applicazioni** è disponibile la lista di tutte le connessioni che sono state avviate dalle applicazioni installate sul dispositivo dal momento dell'attivazione di Firewall Dr.Web (comprese le applicazioni rimosse dal dispositivo, in caso di impostazione corrispondente). La sezione consente di gestire l'accesso di qualsiasi applicazione al traffico internet.

Sulla scheda della sezione sulla schermata iniziale di Firewall viene visualizzato il traffico delle applicazioni in entrata e in uscita complessivo dal momento dell'attivazione di Firewall. Premere **Più nel dettaglio** per aprire la lista completa delle applicazioni.

Per ciascuna applicazione sulla schermata **Tutte le applicazioni** vengono visualizzate le seguenti informazioni:

- quantità complessiva di traffico in entrata e in uscita sulle connessioni stabilite;
- accesso al trasferimento dati via Wi-Fi, internet mobile e in roaming.

Premere il nome di un'applicazione per passare alla schermata Applicazione e visualizzare le statistiche, le impostazioni e le regole per l'applicazione.

Accesso al trasferimento dei dati

Sulla schermata **Tutte le applicazioni** è possibile configurare l'accesso al trasferimento dati via Wi-Fi, internet mobile o in roaming per tutte o alcune applicazioni nella lista utilizzando la barra **Accesso al trasferimento dei dati** (per maggiori informazioni vedi sezione Accesso al trasferimento dei dati).

Filtraggio e ordinamento delle applicazioni

Per filtrare od ordinare la lista delle applicazioni, premere l'icona nell'angolo inferiore destro dello schermo, quindi premere **Filtro** e selezionare i parametri di filtraggio od ordinamento richiesti:

- Visualizzare le applicazioni:
  - con traffico zero.
- Ordinare:
  - traffico decrescente — le applicazioni con il maggior traffico in cima alla lista;
  - traffico crescente — le applicazioni con il minor traffico in cima alla lista;
  - in ordine alfabetico dalla A alla Z;
  - in ordine alfabetico dalla Z alla A.

Di default le applicazioni sono ordinate per traffico decrescente (le applicazioni con il maggior traffico si trovano in cima alla lista), le applicazioni con traffico zero sono visualizzate. Per ripristinare la vista della lista applicazioni di default, premere l'icona sulla schermata **Filtro**.

Ricerca

Per passare rapidamente a un'applicazione richiesta, utilizzare la ricerca nella lista delle applicazioni. Per fare ciò, premere l'icona nell'angolo inferiore destro della schermata

Tutte le applicazioni, quindi premere **Ricerca** e inserire la richiesta nel campo di ricerca nella parte inferiore dello schermo.

Impostazioni di tutte le applicazioni

Per configurare le impostazioni per tutte le applicazioni, sulla schermata **Tutte le applicazioni** premere **Menu** e selezionare l'opzione **Impostazioni**.

Sono disponibili le seguenti impostazioni:

- **Utilizza protocollo IPv6**. Consente di attivare o disattivare l'utilizzo del protocollo IPv6 in parallelo a IPv4.
- **Consenti protocollo DNS sopra TCP**. Consente di attivare o disattivare l'utilizzo del protocollo DNS sopra TCP per il reindirizzamento di richieste DNS e l'occultamento di nomi a dominio.

  L'utilizzo del protocollo DNS sopra TCP può ostacolare la visualizzazione di nomi a dominio sulle schermate Firewall.

  L'impostazione funziona su dispositivi che supportano questo tipo di protocollo. Di default l'impostazione è disattivata.

- **Vieta connessioni per nuove applicazioni**. Consente di vietare l'accesso alla rete per le applicazioni che vengono installate dopo l'attivazione dell'impostazione. È possibile vietare le connessioni tramite Wi-Fi e internet mobile spuntando i flag corrispondenti sotto l'impostazione.
- **Conserva regole e statistiche dopo la rimozione di applicazioni**. Consente di conservare i dati di un'applicazione rimossa dal dispositivo per il periodo di tempo selezionato: una settimana, un mese o un anno.

Tutte le regole

La schermata **Tutte le regole** contiene la lista di tutte le regole delle connessioni di tutte le applicazioni (gruppi di applicazioni).

Per aprire la lista di tutte le regole, sulla schermata **Tutte le applicazioni** premere **Menu** e selezionare l'opzione **Tutte le regole**.

Le regole sono raggruppate per nome dell'applicazione o del gruppo di applicazioni che ha stabilito la connessione. Le applicazioni sono ordinate alfabeticamente. Per espandere la lista delle regole per un'applicazione, premere l'icona a sinistra del nome dell'applicazione o del gruppo di applicazioni. Le regole per un'applicazione sono presentate nell'ordine in cui sono applicate.

Per modificare l'ordine di applicazione delle regole

- Premere e tenere premuta l'icona = di fronte alla regola che si vuole spostare, e trascinare la regola nella posizione desiderata nella lista.

Per eseguire una ricerca nella lista di tutte le regole

- Premere l'icona nell'angolo inferiore destro della schermata **Tutte le regole** e inserire la richiesta nel campo di ricerca nella parte inferiore dello schermo.

Le regole delle applicazioni possono essere conservate sul dispositivo per un periodo indicato dopo la rimozione di un'applicazione, in caso di impostazione corrispondente.

Pulizia dei dati delle applicazioni

Per rimuovere le impostazioni, le regole e le statistiche di tutte le applicazioni

1. Sulla schermata **Tutte le applicazioni** premere **Menu** e selezionare l'opzione **Cancella**.
2. Spuntare i flag di fronte ai dati che si vogliono rimuovere.
3. Premere **Cancella**.

8.6.1.3. Accesso al trasferimento dei dati

È possibile gestire sia per tutte le applicazioni sul dispositivo che per le applicazioni individuali l'accesso al trasferimento dei dati:

- via Wi-Fi ,
- via internet mobile ,
- via internet mobile in roaming .

I tipi di accesso consentiti sono contrassegnati in verde, quelli vietati in grigio.

> Di default per tutte le applicazioni il trasferimento dati tramite Wi-Fi e via internet mobile è consentito, il trasferimento dati via internet mobile in roaming è vietato.

Per modificare l'accesso al trasferimento dati per tutte le applicazioni

- Sulla schermata **Tutte le applicazioni** premere **Wi-Fi**, **Internet mobile** o **Roaming** nella parte superiore dello schermo.

Per modificare l'accesso al trasferimento dati per più applicazioni

1. Sulla schermata **Tutte le applicazioni** premere e tenere premuta una delle applicazioni.

2. Selezionare le altre applicazioni per cui si vuole modificare l'accesso al trasferimento dati.
3. Utilizzare le icone nell'angolo superiore destro dello schermo per consentire/vietare il trasferimento dei dati in modo corrispondente per tutte le applicazioni selezionate.

   Per uscire dalla modalità di modifica dell'accesso, premere ✕ nell'angolo superiore sinistro.

Per modificare l'accesso al trasferimento dati per una singola applicazione

- Sulla schermata Applicazione passare alla scheda **Impostazioni** e fare clic sull'icona , o .

Le applicazioni con accesso a trasferimento dati modificato sono contrassegnate dal badge .

8.6.1.4. Limitazione dell'utilizzo del traffico mobile

Tramite Firewall Dr.Web è possibile impostare un limite di utilizzo del traffico mobile in un periodo di tempo indicato.

> La funzione non è disponibile sui dispositivi su cui non è previsto l'utilizzo delle SIM (è assente lo slot SIM).

Per impostare una limitazione di traffico

1. Sulla schermata iniziale di Firewall Dr.Web premere **Menu** e selezionare l'opzione **Limitazione di traffico**.
2. Premere **Limite**.
3. Impostare un limite di traffico (in megabyte o gigabyte).
4. Se necessario, indicare la quantità di traffico consumato dall'inizio del periodo di limitazione selezionato (il tempo viene conteggiato dalle 00:00 del giorno corrente).
5. Premere **Salva**.
6. Selezionare il periodo di limitazione: un giorno, una settimana o un mese. Se viene selezionato il periodo **Settimana** o **Mese**, indicare il giorno della settimana o il giorno del mese in cui la limitazione verrà aggiornata nei limiti del periodo selezionato.
7. Se desiderato, spuntare il flag **Avvisa se viene raggiunto il limite di traffico mobile** per ricevere avvisi sul raggiungimento del limite impostato.
8. Premere l'icona nell'angolo superiore destro dello schermo.

Immagine 27. Limitazione di traffico

Con la limitazione dell'utilizzo traffico mobile attivata, sulla schermata iniziale di Firewall Dr.Web sulla scheda **Limitazione di traffico** viene visualizzato un diagramma che mostra la quantità di traffico mobile rimanente. Accanto al diagramma viene visualizzato il limite impostato e il conto alla rovescia del tempo mancante all'aggiornamento del periodo di limitazione (v. Immagine 27).

> Con la limitazione attivata, il limite di traffico mobile impostato può essere superato di una piccola quantità non superiore a 4 KB.

Premere **Più nel dettaglio** sulla scheda di limitazione per passare alla schermata **Limitazione di traffico**.

Per modificare la limitazione di traffico corrente

1. Aprire la schermata **Limitazione di traffico**.
2. Apportare le modifiche richieste.
3. Premere l'icona nell'angolo superiore destro dello schermo per salvare le modifiche.

Per disattivare la limitazione di traffico

- Sulla schermata **Limitazione di traffico** premere il pulsante **Disattiva** e confermare l'azione.

8.6.2. Traffico di applicazioni individuali

Firewall Dr.Web consente di configurare e monitorare l'elaborazione del traffico internet a livello di applicazioni individuali e di connessioni da esse stabilite. In questo modo è possibile controllare l'accesso di programmi e processi a risorse di rete.

Sulla schermata **Applicazione** per ciascuna applicazione (in singoli casi, per un gruppo di applicazioni) è possibile visualizzare statistiche di utilizzo del traffico, configurare le regole e impostazioni di utilizzo traffico e di stabilimento connessioni individuali, nonché visualizzare tutti gli eventi di Firewall relativi all'applicazione.

Per aprire la schermata **Applicazione** (vedi Immagine 28), eseguire una delle seguenti azioni:

- Sulla schermata **Applicazioni attive** o **Tutte le applicazioni** premere il nome di un'applicazione nella lista.
- Sulla schermata Connessione premere l'icona ↗ a destra del nome dell'applicazione.

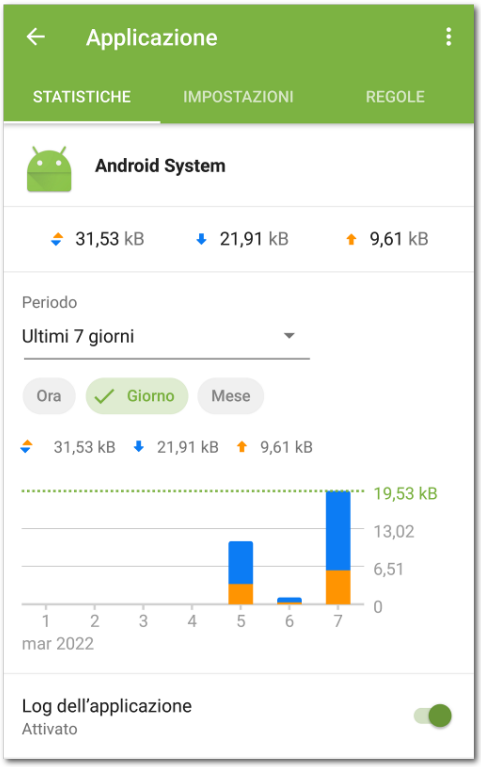

Immagine 28. Schermata Applicazione

Sulla schermata **Applicazione** sono disponibili tre schede: **Statistiche**, **Impostazioni** e **Regole**.

8.6.2.1. Statistiche di utilizzo del traffico internet

Le statistiche sull'utilizzo del traffico internet da qualsiasi applicazione installata sono visualizzate sotto forma di un diagramma (v. Immagine 29).

Per visualizzare le statistiche di utilizzo del traffico, sulla schermata **Applicazioni attive** o **Tutte le applicazioni** premere il nome di un'applicazione nella lista.

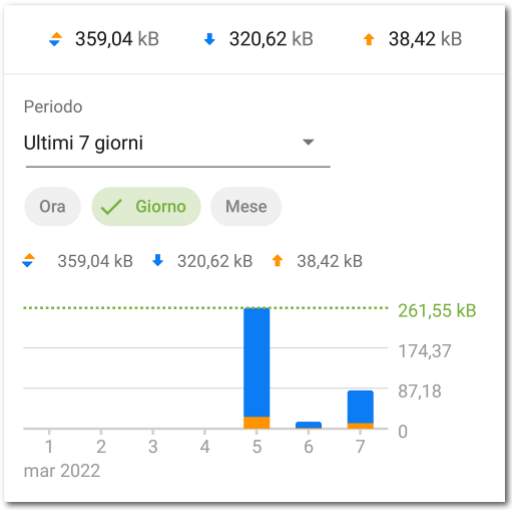

Immagine 29. Statistiche sull'uso del traffico internet di un'applicazione

Sulla scheda **Statistiche** sotto il nome dell'applicazione è indicata la quantità di traffico consumato dall'applicazione dal momento dell'attivazione di Firewall.

Sul diagramma il traffico in uscita è contrassegnato in arancione e quello in entrata in blu. Sopra il diagramma sono riportati i valori numerici del traffico (totale, in uscita e in entrata) consumato nel periodo di tempo indicato.

Visualizzando le statistiche di utilizzo del traffico internet, è possibile eseguire le seguenti azioni:

- Selezionare un periodo di tempo per la visualizzazione delle statistiche. È possibile visualizzare le statistiche per il giorno corrente, gli ultimi 7 giorni, il mese corrente, il mese precedente o impostare in autonomo un periodo di tempo indicando le date di inizio e di fine. Selezionare il periodo di tempo richiesto nella lista a cascata **Periodo** sopra il diagramma.
- Configurare nei limiti del periodo selezionato la visualizzazione delle statistiche per ora, giorno o mese. Selezionare l'opzione di visualizzazione corrispondente sopra il diagramma.

È possibile far scorrere il dito con il diagramma verso sinistra o destra fino a un valore richiesto, se il grafico non è visualizzato per intero.

Rimozione delle statistiche

- Rimozione delle statistiche per una singola applicazione:
  1. Sulla schermata **Applicazioni attive** o **Tutte le applicazioni** premere il nome dell'applicazione di cui si vogliono cancellare le statistiche.
  2. Sulla schermata **Applicazione** premere **Menu** nell'angolo superiore destro e selezionare l'opzione **Cancella**.
  3. Nella finestra che si è aperta spuntare il flag **Statistiche dell'applicazione** e premere **Cancella**.

- Rimozione delle statistiche per tutte le applicazioni:
  1. Sulla schermata **Tutte le applicazioni** premere **Menu** e selezionare l'opzione **Cancella**.
  2. Nella finestra che si è aperta spuntare il flag **Statistiche delle applicazioni** e premere **Cancella**.

> Dopo la rimozione di un'applicazione dal dispositivo, le statistiche dell'applicazione verranno rimosse automaticamente entro 5 minuti.

Log dell'applicazione

Gli eventi relativi all'attività di rete delle applicazioni installate sul dispositivo vengono registrati nei log delle applicazioni. Utilizzare l'interruttore per iniziare o riprendere la registrazione del log dell'applicazione. Per passare al log, premere **Visualizza log**.

8.6.2.2. Impostazioni di un'applicazione

Accesso al trasferimento dei dati

È possibile consentire o vietare a un'applicazione di trasferire dati via Wi-Fi, internet mobile e internet mobile in roaming facendo clic sull'icona corrispondente (v. sezione Accesso al trasferimento dei dati).

Blocca tutte le connessioni eccetto quelle consentite dalle regole

Per vietare di default tutte le connessioni per un'applicazione, spuntare il flag **Blocca tutte le connessioni eccetto quelle consentite dalle regole**. Se non verranno impostate regole di permesso per l'applicazione, l'applicazione non potrà stabilire alcuna connessione.

Con l'attivazione dell'impostazione **Blocca tutte le connessioni eccetto quelle consentite dalle regole** per l'applicazione verrà automaticamente aggiunta una regola di permesso per la porta 53. La presenza della regola (per i protocolli DNS, UDP o ALL) è obbligatoria per il funzionamento delle regole di permesso con nomi a dominio.

> Per il corretto funzionamento dell'impostazione in presenza delle regole di permesso con nomi a dominio, è inoltre necessario disattivare l'utilizzo del server DNS privato nelle impostazioni del dispositivo.

Non controllare l'applicazione

> L'impostazione è disponibile sui dispositivi con Android 5.0 o versioni successive.
>
> L'impostazione non è disponibile per alcune applicazioni di sistema.

Firewall Dr.Web è implementato sulla base di VPN per Android. La VPN ostacola il funzionamento delle applicazioni che utilizzano una tecnologia incompatibile con VPN, per esempio, Wi-Fi Direct. Ciò può portare all'impossibilità di connessione del dispositivo ad altri dispositivi. In questo caso, è possibile disattivare il controllo di Firewall Dr.Web per l'applicazione (gruppo di applicazioni) richiesta spuntando il flag **Non controllare l'applicazione**.

Si consiglia di disattivare il controllo di Firewall Dr.Web solo per le applicazioni di cui ci si fida.

Se questa opzione è attivata, Firewall Dr.Web non controlla le connessioni di rete di questa applicazione, anche se nelle impostazioni di Firewall Dr.Web sono impostate limitazioni. Il traffico dell'applicazione non viene calcolato.

8.6.2.3. Regole delle connessioni

Il traffico delle applicazioni viene gestito a livello di connessioni che vengono stabilite dalle applicazioni. È possibile impostare le regole di permesso, di divieto e di reindirizzamento per le connessioni a indirizzi IP e porte specifici per ciascuna applicazione installata sul dispositivo.

Le regole delle connessioni sono disponibili sulla scheda Regole della schermata **Applicazione**, nonché sulla schermata Tutte le regole.

Connessioni

Le informazioni generali su ciascuna connessione sono presentate sulla schermata **Connessione** (v. Immagine 30). Per passare a questa schermata, eseguire una delle seguenti azioni:

- Sulla schermata Applicazioni attive premere l'icona ⌄ a sinistra del nome di un'applicazione e quindi premere la riga di una connessione.
- Nel log di Firewall:
  - In modalità di raggruppamento per data: premere la riga di una connessione.
  - In modalità di raggruppamento per nome di applicazione: espandere la lista delle connessioni di un'applicazione tramite l'icona ⌄ a sinistra del nome dell'applicazione e quindi premere la riga di una connessione.
- Nel log di un'applicazione espandere la lista delle connessioni tramite l'icona ⌄ a destra della data di un evento e quindi premere la riga di una connessione.

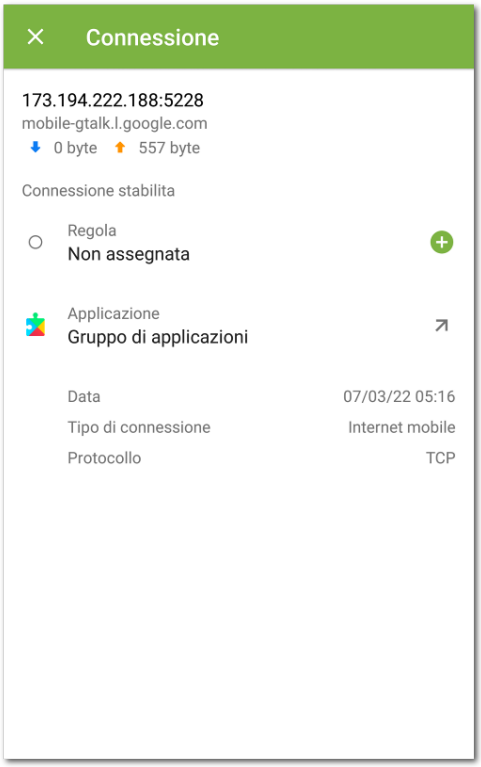

Immagine 30. Schermata Connessione

Sulla schermata **Connessione** sono disponibili le seguenti informazioni:

- indirizzo e porta della connessione;
- nome dell'host (se disponibile);
- quantità di traffico in entrata e in uscita ricevuto o trasmesso dalla connessione;
- stato della connessione;
- regola della connessione;
- applicazione che ha stabilito la connessione;
- data e ora;
- tipo di connessione;
- protocollo.

Per copiare l'indirizzo di una connessione

1. Premere e tenere premuta la riga con l'indirizzo. Si passa alla modalità di copiatura. L'indirizzo sarà evidenziato in grigio.
2. Premere l'icona nell'angolo superiore destro dello schermo. L'indirizzo verrà copiato negli appunti.

Per uscire dalla modalità di copiatura, premere l'icona ✕ nell'angolo superiore sinistro.

Regole delle connessioni

Creazione delle regole

Per creare una nuova regola per una connessione

1. Per una connessione senza regole:
   - Sulla schermata **Connessione** premere l'icona a destra della voce **Regola**.
   - Sulla schermata **Applicazioni attive** espandere la lista delle connessioni stabilite e premere l'icona a destra dell'indirizzo di una connessione.

   Per qualsiasi connessione:

   - Sulla schermata **Applicazione** sulla scheda **Regole** premere l'icona nella parte inferiore destra dello schermo.
2. Nella finestra che si è aperta selezionare il tipo di regola:
   - di permesso,
   - di divieto,
   - di reindirizzamento.
3. Verificare la correttezza dell'indirizzo IP/nome host. Se nessun indirizzo è indicato, indicare un indirizzo IP valido (in formato a.b.c.d per indirizzi IPv4 o [a:b:c:d:e:f:g:h] per indirizzi IPv6), un intervallo di indirizzi IP (in formato a1.b1.c1.d1-a2.b2.c2.d2 o [a1:b1:c1:d1:e1:f1:g1:h1]-[a2:b2:c2:d2:e2:f2:g2:h2]) o una rete intera (in formato a.b.c.0/n, dove n è un numero compreso tra 1 e 32). Se viene creata una regola di reindirizzamento, indicare l'indirizzo di reindirizzamento nel campo sottostante. Invece di un indirizzo, è possibile indicare un nome host.
4. Premere **Altri parametri** per configurare l'impostazione aggiuntiva **Protocollo** — protocollo di rete per la connessione.
5. Premere l'icona per salvare le modifiche.

Le applicazioni con regole delle connessioni impostate sono contrassegnate dal badge .

Visualizzazione delle regole

Per vedere le regole delle connessioni

- Per un'applicazione individuale:
  - Aprire la schermata **Applicazione** e passare alla scheda **Regole**.

  La scheda contiene la lista di tutte le regole impostate per tale applicazione nell'ordine in cui sono applicate.
- Per tutte le applicazioni:

1. Sulla schermata iniziale di Firewall sulla scheda della sezione **Tutte le applicazioni** premere **Più nel dettaglio**.
2. Sulla schermata **Tutte le applicazioni** premere **Menu** e selezionare l'opzione **Tutte le regole**.

La schermata **Tutte le regole** contiene la lista di tutte le regole delle connessioni raggruppate per nome dell'applicazione o del gruppo di applicazioni che ha stabilito la connessione. Le applicazioni sono ordinate alfabeticamente. Per espandere la lista delle regole per un'applicazione, premere l'icona a sinistra del nome dell'applicazione o del gruppo di applicazioni. Le regole per un'applicazione sono presentate nell'ordine in cui sono applicate.

Per modificare l'ordine di applicazione delle regole

- Premere e tenere premuta l'icona di fronte alla regola che si vuole spostare, e trascinare la regola nella posizione desiderata nella lista.

Per eseguire una ricerca nella lista di tutte le regole

- Premere l'icona nell'angolo inferiore destro della schermata **Tutte le regole** e inserire la richiesta nel campo di ricerca nella parte inferiore dello schermo.

Le regole delle applicazioni possono essere conservate sul dispositivo per un periodo indicato dopo la rimozione di un'applicazione, in caso di impostazione corrispondente.

Modifica delle regole

Per modificare una regola esistente

1. Eseguire una delle seguenti azioni:
   - Sulla schermata **Connessione** premere l'icona a destra della regola.
   - Sulla schermata **Applicazioni attive** premere l'icona a sinistra del nome di un'applicazione e quindi premere l'icona di fronte alla connessione la cui regola verrà modificata.
   - Sulla schermata **Applicazione** sulla scheda **Regole** premere la riga di una regola.
   - Sulla schermata **Tutte le regole** premere l'icona a sinistra del nome di un'applicazione e quindi premere la riga di una regola.
2. Apportare le modifiche richieste.
3. Premere l'icona per salvare le modifiche.

Rimozione delle regole

Per rimuovere una regola

- Sulla schermata di modifica della regola:
  1. Premere **Rimuovi regola**.
  2. Nella finestra che si è aperta premere **Elimina**.
- Sulla scheda **Regole** o sulla schermata **Tutte le regole**:
  1. Far scorrere il dito con la regola verso sinistra e premere l'icona .
  2. Nella finestra che si è aperta premere **Elimina**.

Per rimuovere tutte le regole per una determinata applicazione

1. Sulla schermata **Applicazione** premere **Menu** nell'angolo superiore destro e selezionare l'opzione **Cancella**.
2. Nella finestra che si è aperta spuntare il flag **Regole per l'applicazione**. Premere **Cancella**.

Per rimuovere tutte le regole per tutte le applicazioni

1. Sulla schermata **Tutte le regole** premere **Menu** e selezionare l'opzione **Cancella**.
2. Premere **Cancella**.

Importazione ed esportazione delle regole

Le liste di regole create possono essere esportate in un file nella memoria interna del dispositivo. Se necessario (per esempio se Dr.Web verrà reinstallato o utilizzato su un altro dispositivo), le regole potranno essere importate da questo file.

Per esportare le regole in un file

- Regole di un'applicazione individuale:
  1. Sulla schermata **Applicazione** sulla scheda **Regole** premere **Menu** nell'angolo superiore destro e selezionare l'opzione **Esportazione delle regole**.
  2. Premere **OK**.
- Regole per tutte le applicazioni:
  1. Sulla schermata **Tutte le regole** premere **Menu** nell'angolo superiore destro e selezionare l'opzione **Esportazione delle regole**.
  2. Premere **OK**.

Le regole vengono esportate nel file `DrWeb_Firewall_Rules_<nome_applicazione>.hsts`, se queste sono regole per

un'applicazione, o nel file `DrWeb_Firewall_Rules_ALL.hsts`, se queste sono regole per tutte le applicazioni. Il file con le regole viene salvato nella cartella `Internal storage/Android/data/com.drweb/files/`.

> Sui dispositivi con Android 11.0 o versioni successive il file con le regole viene salvato nella cartella `Download/DrWeb`.

Per importare le regole da un file

- Regole di un'applicazione individuale:
  1. Sulla schermata **Applicazione** sulla scheda **Regole** premere **Menu** nell'angolo superiore destro e selezionare l'opzione **Importazione delle regole**.
  2. Nell'albero dei file trovare il file con le regole e premerlo.
- Regole per tutte le applicazioni:
  1. Sulla schermata **Tutte le regole** premere **Menu** nell'angolo superiore destro e selezionare l'opzione **Importazione delle regole**.
  2. Nell'albero dei file trovare il file con le regole e premerlo.

Blocca tutte le connessioni eccetto quelle consentite dalle regole

È possibile vietare tutte le connessioni di un'applicazione, eccetto quelle consentite dalle regole, spuntando il flag corrispondente sulla schermata delle impostazioni dell'applicazione.

8.6.2.4. Log di un'applicazione

Gli eventi delle connessioni di rete vengono registrate nei log delle applicazioni.

Per attivare la registrazione del log di un'applicazione

- Sulla schermata **Applicazione** sulla scheda **Statistiche** utilizzare l'interruttore **Log dell'applicazione**.

Per aprire il log di un'applicazione

- Sulla schermata **Applicazione** sulla scheda **Statistiche** selezionare la voce **Visualizza log**.

Tutte le connessioni di questa applicazione sono riunite per data. Per aprire la lista delle connessioni per una determinata data, premere l'icona a destra della data. Per ciascuna connessione nel log sono disponibili le seguenti informazioni:

- indirizzo e porta della connessione;
- traffico consumato;
- ora di stabilimento della connessione;

- presenza per la connessione di una regola:
  - 🟢 di permesso,
  - 🔴 di divieto,
  - 🟠 di reindirizzamento,
  - ○ nessuna regola impostata.

Premere la riga di una connessione per passare alla schermata Connessione e configurare regole per essa.

Per copiare l'indirizzo di una connessione

- Premere e tenere premuta la riga con l'indirizzo della connessione. L'indirizzo verrà copiato negli appunti.

Per ripulire il log di un'applicazione

1. Sulla schermata del log dell'applicazione premere l'icona nell'angolo superiore destro dello schermo.
2. Nella finestra che si è aperta premere il pulsante **Cancella**.

Per disattivare la registrazione del log di un'applicazione

- Sulla schermata **Applicazione** sulla scheda **Statistiche** utilizzare l'interruttore **Log dell'applicazione**.

8.6.3. Log di Firewall Dr.Web

Gli eventi relativi al funzionamento di Firewall vengono registrati nel log di Firewall Dr.Web.

Per aprire la lista di tutti gli eventi relativi al funzionamento di Firewall Dr.Web, sulla schermata iniziale del componente Firewall premere **Menu** e selezionare l'opzione **Log**.

Nel log di Firewall vengono visualizzate le seguenti informazioni sull'evento:

- nome dell'applicazione;
- indirizzo e porta della connessione (nonché indirizzo di reindirizzamento, se è impostata la regola corrispondente);
- traffico consumato;
- data e ora dell'evento;
- presenza di una regola per la connessione.

Tramite il clic su un evento si apre la schermata Connessione.

Per filtrare od ordinare gli eventi nel log di Firewall

1. Premere l'icona  nell'angolo inferiore destro della schermata **Log**, quindi premere **Filtro**.
2. Selezionare i parametri di filtraggio od ordinamento richiesti:
   - Ordinare:
     - prima più recenti — gli ultimi eventi in cima al log;
     - prima meno recenti — gli ultimi eventi in fondo al log;
     - in ordine alfabetico dalla A alla Z;
     - in ordine alfabetico dalla Z alla A.
   - Visualizzare le connessioni:
     - stabilite,
     - resettate,
     - reindirizzate,
     - con errore.

Di default gli eventi sono ordinati per data (gli ultimi eventi si trovano in cima al log), tutti i tipi di connessioni sono visualizzati. Per ripristinare la vista del log di default, premere l'icona  sulla schermata **Filtro**.

Per comodità di visualizzazione del log è anche possibile raggruppare gli eventi per applicazione.

Per raggruppare gli eventi per applicazione

- Sulla schermata **Log** premere **Menu**  nell'angolo superiore destro e spuntare il flag **Raggruppa**.

Per eseguire una ricerca nel log di Firewall

1. Premere l'icona  nell'angolo inferiore destro della schermata **Log**, quindi premere **Ricerca**.
2. Inserire la richiesta nel campo di ricerca nella parte inferiore dello schermo.

Per copiare l'indirizzo di una connessione

- Premere e tenere premuta la riga con l'indirizzo della connessione. L'indirizzo verrà copiato negli appunti.

Per ripulire il log di Firewall

1. Premere **Menu** e selezionare l'opzione **Cancella**.
2. Confermare l'azione premendo il pulsante **Cancella**.

Dimensione del log

Di default per il file di log è impostata una dimensione pari a 5 MB.

Per modificare la dimensione massima consentita del file di log

1. Sulla schermata del log di Firewall premere **Menu** e selezionare l'opzione **Dimensione del log**.
2. Nella finestra che si è aperta modificare il valore e premere **OK**.

> La dimensione massima del log deve essere maggiore di 0 MB e minore o pari a 99 MB.

8.7. Auditor di sicurezza

Dr.Web analizza la sicurezza del dispositivo e suggerisce come risolvere i problemi e le vulnerabilità individuati attraverso un componente specifico — Auditor di sicurezza. Il componente inizia a funzionare automaticamente dopo il primo avvio dell'applicazione e la registrazione della licenza.

Possibili problemi e modi per risolverli

Dr.Web rileva i seguenti problemi di sicurezza:

- Vulnerabilità
- Impostazioni di sistema, che influiscono sulla sicurezza del dispositivo
- Software in conflitto
- Amministratori del dispositivo nascosti
- Applicazioni che sfruttano la vulnerabilità Fake ID.
- Impostazioni di ottimizzazione.

Per aprire la lista dei problemi di sicurezza rilevati (vedi Immagine 31), sulla schermata principale di Dr.Web selezionare **Auditor di sicurezza**.

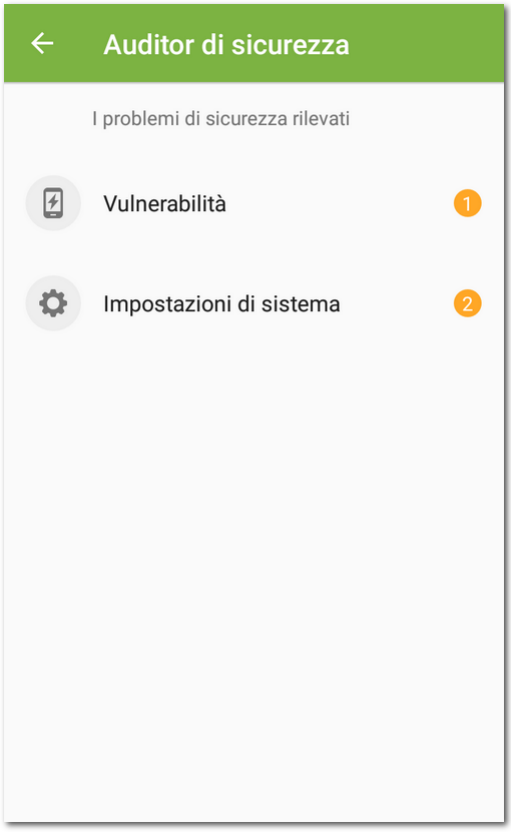

Immagine 31. Auditor di sicurezza

8.7.1. Vulnerabilità

Una *vulnerabilità* è un difetto nel codice software che può essere sfruttato dai malintenzionati per disturbare il funzionamento del sistema.

Auditor di sicurezza rileva nel sistema del dispositivo le seguenti vulnerabilità: BlueBorne, EvilParcel, Extra Field, Fake ID, Janus, ObjectInputStream Serialization, OpenSSLX509Certificate, PendingIntent, SIM Toolkit, Stagefright e Stagefright 2.0.

Utilizzando le vulnerabilità, i malintenzionati possono aggiungere un codice software alle applicazioni le quali di conseguenza possono iniziare a svolgere funzioni che rappresentano una minaccia per la sicurezza del dispositivo.

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 le falle potrebbero essere riparate. Se gli aggiornamenti non sono disponibili, è consigliabile installare applicazioni solo da fonti affidabili.

Permessi di root

Il dispositivo può diventare vulnerabile a diversi tipi di minacce se su di esso sono disponibili i permessi di root, cioè sono state apportate le modifiche volte ad ottenere i permessi di

superutente (root). Questo permette di modificare e rimuovere i file di sistema, il che può portare all'inoperatività del dispositivo. Se queste modifiche sono state apportate 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 svolgere qualche attività, è consigliabile essere particolarmente attenti, installando applicazioni da fonti sconosciute.

8.7.2. Impostazioni di sistema

Auditor di sicurezza rileva le seguenti impostazioni di sistema che influiscono sulla sicurezza del dispositivo:

- **Debugging permesso**. Il debug tramite USB è progettato per sviluppatori e consente di copiare dati da un computer su un dispositivo con Android e viceversa, installare applicazioni sul dispositivo, visualizzare dati dei log delle applicazioni installate e inoltre rimuoverli in alcuni casi. Se non si è sviluppatori e non si usa la modalità di debug, è consigliabile disattivarla. Per passare alla sezione corrispondente delle impostazioni di sistema, premere il pulsante **Impostazioni** sulla schermata con informazioni dettagliate su questo problema.
- **Installazione da sorgenti sconosciute permessa**. L'installazione di applicazioni da fonti sconosciute è la principale causa di diffusione di minacce sui dispositivi con Android 7.1 e versioni precedenti.

  Le applicazioni scaricate da una fonte diversa dalla directory delle applicazioni ufficiale con un'elevata probabilità possono rivelarsi pericolose e arrecare danno al dispositivo. Per ridurre il rischio di installazione di applicazioni non sicure, è consigliabile vietare l'installazione di applicazioni da fonti sconosciute. Per andare alla sezione corrispondente delle impostazioni di sistema, premere il pulsante **Impostazioni** sulla schermata con informazioni dettagliate su questo problema.

  Si consiglia di verificare la presenza di minacce in tutte le applicazioni che vengono installate. Prima di eseguire una verifica, è necessario assicurarsi che i database dei virus Dr.Web siano aggiornati.
- **Avvisi Dr.Web bloccati**. In questo caso Dr.Web non può informare prontamente di minacce rilevate. Questo riduce la sicurezza del dispositivo e può portare all'infezione. Pertanto, è consigliabile passare alle impostazioni del dispositivo e attivare gli avvisi Dr.Web.
- **Installato un certificato radice personalizzato**. Se sul dispositivo sono stati rilevati certificati personalizzati, le relative informazioni verranno visualizzate in Auditor di sicurezza. A causa di certificati personalizzati installati, terze parti possono visualizzare le attività di rete dell'utente. Se non si conosce lo scopo dei certificati rilevati, è consigliato rimuoverli dal dispositivo.

8.7.3. Software in conflitto

L'utilizzo di software in conflitto, in particolare di browser non supportati dal filtro URL riduce la sicurezza del dispositivo. Utilizzando tali browser, l'utente non è protetto da risorse internet indesiderate e malevole. Pertanto, si consiglia di utilizzare, anche come browser predefinito, il

browser incorporato di Android, Google Chrome, Yandex.Browser, Microsoft Edge, Firefox, Firefox Focus, Opera, Adblock Browser, Dolphin Browser, Sputnik, Boat Browser e Atom.

8.7.4. Amministratori del dispositivo nascosti

Le applicazioni che sono attivate come amministratori del dispositivo, ma sono assenti dalla lista amministratori nella sezione corrispondente delle impostazioni del dispositivo non possono essere rimosse con strumenti standard del sistema operativo. Con grande probabilità tali applicazioni non sono sicure.

Se non si sa perché un'applicazione nasconde la sua presenza nella lista degli amministratori del dispositivo, è consigliato rimuoverla. Per rimuovere un'applicazione, premere il pulsante **Elimina** sulla schermata con informazioni dettagliate sul problema relativo a questa applicazione.

8.7.5. Applicazioni che sfruttano la vulnerabilità Fake ID

Se sul dispositivo vengono rilevate applicazioni che utilizzano la vulnerabilità Fake ID, esse vengono visualizzate in una categoria separata di Auditor di sicurezza. Queste applicazioni possono essere malevole, quindi è consigliabile rimuoverle. Per rimuovere un'applicazione, premere il pulsante **Elimina** sulla schermata con informazioni dettagliate sul problema relativo a questa applicazione o utilizzare gli strumenti del sistema operativo.

8.7.6. Impostazioni di ottimizzazione

Il sistema operativo del dispositivo può terminare i processi delle applicazioni che attualmente non vengono utilizzate attivamente. Tale ottimizzazione dei processi in background aiuta a risparmiare batteria e migliorare le prestazioni, ma può influenzare il funzionamento delle applicazioni.

L'applicazione Dr.Web deve funzionare ininterrottamente per fornire la protezione antivirus continua e l'efficacia dei componenti addizionali: Filtro chiamate ed SMS, Filtro URL, Antifurto, Parental control e Firewall.

Affinché l'applicazione funzioni correttamente, togliere le limitazioni all'applicazione in modalità background. Per fare ciò, controllare le impostazioni del dispositivo e della gestione applicazioni integrata.

Il set di impostazioni dipende dal modello del dispositivo:

- Asus
- Huawei
- Meizu
- Nokia

- OnePlus
- Oppo
- Samsung
- Sony
- Xiaomi

Le istruzioni fornite nelle sezioni citate potrebbero parzialmente non corrispondere a singoli dispositivi in quanto le impostazioni possono differire su diversi modelli di dispositivo e versioni del sistema operativo. In caso di discordanza, controllare la procedura nel manuale utente del modello di dispositivo in uso. Se questo non aiuterà a risolvere il problema, contattare il servizio di supporto tecnico.

Revoca delle autorizzazioni

L'avviso viene visualizzato se all'applicazione Dr.Web non è concesso l'accesso alle funzioni di accessibilità.

A partire dalla versione 6.0 il sistema operativo Android revoca i permessi concessi dall'utente se un'applicazione non veniva utilizzata durante alcuni mesi. Il sistema operativo Android 12.0 e versioni successive anche vieta la visualizzazione di notifiche e cancella la cache dell'applicazione. In questo modo il sistema risparmia risorse di memoria del dispositivo e protegge i dati utente. Tuttavia, Dr.Web non sarà in grado di fornire protezione continua del dispositivo se i permessi necessari per le sue funzioni principali e il funzionamento dei componenti saranno revocati. Per il funzionamento stabile dell'applicazione si consiglia di disattivare la revoca di permessi automatica nelle impostazioni del dispositivo. Per passare alla sezione corrispondente delle impostazioni di sistema, premere il pulsante **Impostazioni** sulla schermata con informazioni dettagliate su questo problema.

Accesso alle impostazioni

Sui dispositivi con Android 13.0 e versioni successive il sistema di default chiude per le applicazioni l'accesso a determinate impostazioni. Questo viene fatto per proteggere i dati riservati dall'uso illecito da parte di applicazioni malevole. Tuttavia, per i componenti Dr.Web è richiesto l'accesso a impostazioni come le funzioni di accessibilità del dispositivo e la lettura di notifiche per proteggere i dati dell'utente e bloccare i contenuti indesiderati. Per passare all'impostazione di sistema che consente l'accesso alle impostazioni necessarie per il funzionamento Dr.Web, seguire le istruzioni sulla schermata con informazioni dettagliate su questo problema.

Il parametro **Scorciatoia** nel menu delle funzioni di accessibilità attiva un pulsante che consente di attivare/disattivare l'accesso di Dr.Web alle funzioni di accessibilità da qualsiasi punto sul dispositivo con un solo clic. Si consiglia di disattivare **Scorciatoia** per evitare clic accidentali.

8.7.6.1. Asus

Affinché l'applicazione Dr.Web funzioni correttamente in background sui dispositivi Asus, eseguire le seguenti azioni:

- Consentire l'avvio automatico

  L'avvio automatico consente di avviare i processi dell'applicazione subito dopo che il dispositivo viene acceso. È necessario per la protezione antivirus continua del dispositivo e per il buon funzionamento dei componenti addizionali: Filtro chiamate ed SMS, Filtro URL, Antifurto, Parental control e Firewall.

- Consentire il funzionamento in background

  Il funzionamento in background consente all'applicazione di continuare a rimanere in esecuzione anche se non è attiva. È necessario per la protezione antivirus continua del dispositivo e per il buon funzionamento dei componenti addizionali: Filtro chiamate ed SMS, Filtro URL, Antifurto, Parental control e Firewall.

> Le impostazioni e la loro posizione possono variare in base ai diversi modelli del dispositivo e le versioni del sistema operativo. Se queste istruzioni non risolvono il problema, contattare il servizio di supporto tecnico.

Per consentire l'avvio automatico

1. Nelle impostazioni del dispositivo aprire **Gestione avvio automatico**.
2. Consentire l'avvio automatico per l'applicazione Dr.Web.

Per consentire il funzionamento in background

1. Nell'applicazione **Gestione mobile** aprire **Impostazioni**.
2. Disattivare le impostazioni **Pulisci in sospensione.**

8.7.6.2. Huawei

Dispositivi che supportano la gestione manuale

Sui dispositivi Huawei che supportano la gestione automatica e manuale dell'avvio applicazioni, consentire la gestione avvio manuale per l'applicazione Dr.Web.

La gestione manuale consente all'applicazione di continuare a rimanere in esecuzione anche se non è attiva, e avviare i processi subito dopo che il dispositivo viene acceso. È necessario per la protezione antivirus continua del dispositivo e per il buon funzionamento dei componenti addizionali: Filtro chiamate ed SMS, Filtro URL, Antifurto, Parental control e Firewall.

Per attivare la gestione manuale

- Sui dispositivi con Android:
  1. Nelle impostazioni del dispositivo aprire **Batteria** > **Avvio app**.
  2. Selezionare **Gestione manuale**.
- Sui dispositivi con Harmony OS:
  1. Nelle impostazioni del dispositivo aprire la sezione delle impostazioni di avvio applicazioni.
  2. Trovare Dr.Web nella lista e utilizzare l'interruttore a destra per attivare la gestione manuale.
  3. Nella finestra che si è aperta attivare tutte le impostazioni di gestione aggiuntive e premere **OK**.

Altri dispositivi Huawei

Affinché l'applicazione Dr.Web funzioni correttamente in background su altri dispositivi Huawei, modificare le seguenti impostazioni:

- Consentire il funzionamento in background

  Il funzionamento in background consente all'applicazione di continuare a rimanere in esecuzione anche se non è attiva. È necessario per la protezione antivirus continua del dispositivo e per il buon funzionamento dei componenti addizionali: Filtro chiamate ed SMS, Filtro URL, Antifurto, Parental control e Firewall.
- Disattivare l'ottimizzazione della batteria

  > Se Dr.Web è un amministratore del dispositivo, questa impostazione di ottimizzazione non è disponibile.

  Per ottimizzare l'utilizzo della batteria, il sistema operativo può chiudere l'applicazione Dr.Web. Ciò interromperà la protezione antivirus continua del dispositivo e il funzionamento dei componenti addizionali attivati: Filtro chiamate ed SMS, Filtro URL, Antifurto, Parental control e Firewall.
- Consentire il funzionamento con schermo spento

  Il funzionamento con schermo spento è necessario per la protezione antivirus continua del dispositivo e per il funzionamento dei componenti addizionali: Filtro chiamate ed SMS, Antifurto e Firewall.
- Consentire le finestre a comparsa, se è attivato Antifurto o Parental control

  In modalità background Antifurto e Parental control utilizzano le finestre a comparsa per limitare l'accesso a una singola applicazione o all'intero dispositivo.

Le impostazioni e la loro posizione possono variare in base ai diversi modelli del dispositivo e le versioni del sistema operativo. Se queste istruzioni non risolvono il problema, contattare il servizio di supporto tecnico.

Per consentire il funzionamento in background

1. Aprire le applicazioni recenti.
2. Premere l'icona con lucchetto accanto all'applicazione Dr.Web.

Per disattivare l'ottimizzazione della batteria

1. Nelle impostazioni del dispositivo aprire **Impostazioni avanzate** > **Gestione batteria** > **App protette**.
2. Selezionare **Protetto** per l'applicazione Dr.Web.

Per consentire il funzionamento con schermo spento

1. Nelle impostazioni del dispositivo selezionare **Applicazioni** > **Dr.Web** > **Batteria**.
2. Attivare l'opzione **Funzionamento con schermo spento**.

Per consentire le finestre a comparsa

1. Nelle impostazioni del dispositivo selezionare **Applicazioni**.
2. Nella lista delle applicazioni selezionare Dr.Web.
3. Nella lista dei permessi attivare la visualizzazione in background delle finestre a comparsa.

8.7.6.3. Meizu

Affinché l'applicazione Dr.Web funzioni correttamente in background sui dispositivi Meizu, modificare le seguenti impostazioni:

- Disattivare l'ottimizzazione della batteria

  Se Dr.Web è un amministratore del dispositivo, questa impostazione di ottimizzazione non è disponibile.

  Per ottimizzare l'utilizzo della batteria, il sistema operativo può chiudere l'applicazione Dr.Web. Ciò interromperà la protezione antivirus continua del dispositivo e il funzionamento dei componenti addizionali attivati: Filtro chiamate ed SMS, Filtro URL, Antifurto, Parental control e Firewall.

- Fissare Dr.Web in modalità background

  Il funzionamento in background consente all'applicazione di continuare a rimanere in esecuzione anche se non è attiva. È necessario per la protezione antivirus continua del dispositivo e per il buon funzionamento dei componenti addizionali: Filtro chiamate ed SMS,

Filtro URL, Antifurto, Parental control e Firewall.

- Consentire il funzionamento con schermo spento

  Il funzionamento con schermo spento è necessario per la protezione antivirus continua del dispositivo e per il funzionamento dei componenti addizionali: Filtro chiamate ed SMS, Antifurto e Firewall.

  > Le impostazioni e la loro posizione possono variare in base ai diversi modelli del dispositivo e le versioni del sistema operativo. Se queste istruzioni non risolvono il problema, contattare il servizio di supporto tecnico.

Per disattivare l'ottimizzazione della batteria

1. Nelle impostazioni del dispositivo aprire **Impostazioni avanzate** > **Gestione batteria** > **App protette**.
2. Selezionare **Protetto** per l'applicazione Dr.Web.

Per fissare Dr.Web in modalità background

1. Aprire le applicazioni recenti.
2. Premere l'icona con lucchetto accanto all'applicazione Dr.Web.

Per consentire il funzionamento con schermo spento

1. Nelle impostazioni del dispositivo selezionare **Applicazioni** > **Dr.Web** > **Batteria**.
2. Attivare l'opzione **Funzionamento con schermo spento**.

8.7.6.4. Nokia

Affinché l'applicazione Dr.Web funzioni correttamente in background sui dispositivi Nokia, arrestare l'applicazione Power saver.

> Se Dr.Web è un amministratore del dispositivo, questa impostazione di ottimizzazione non è disponibile.

L'applicazione Power saver ottimizza l'utilizzo della batteria, il che può portare alla chiusura dell'applicazione Dr.Web. Ciò interromperà la protezione antivirus continua del dispositivo e il funzionamento dei componenti addizionali attivati: Filtro chiamate ed SMS, Filtro URL, Antifurto, Parental control e Firewall.

> Le impostazioni e la loro posizione possono variare in base ai diversi modelli del dispositivo e le versioni del sistema operativo. Se queste istruzioni non risolvono il problema, contattare il servizio di supporto tecnico.

Per arrestare Power saver

1. Nelle impostazioni del dispositivo aprire **Applicazioni** > **Tutte le applicazioni**.
2. Premere il menu nell'angolo superiore destro dello schermo e selezionare **Mostra quelle di sistema**.
3. Selezionare **Risparmio energetico** e premere **Interrompi**.

   L'applicazione sarà arrestata fino al successivo riavvio del dispositivo.

8.7.6.5. OnePlus

Affinché l'applicazione Dr.Web funzioni correttamente in background sui dispositivi OnePlus, modificare le seguenti impostazioni:

- Disattivare l'ottimizzazione della batteria

  Se Dr.Web è un amministratore del dispositivo, questa impostazione di ottimizzazione non è disponibile.

  Per ottimizzare l'utilizzo della batteria, il sistema operativo può chiudere l'applicazione Dr.Web. Ciò interromperà la protezione antivirus continua del dispositivo e il funzionamento dei componenti addizionali attivati: Filtro chiamate ed SMS, Filtro URL, Antifurto, Parental control e Firewall.
- Fissare Dr.Web in modalità background

  Il funzionamento in background consente all'applicazione di continuare a rimanere in esecuzione anche se non è attiva. È necessario per la protezione antivirus continua del dispositivo e per il buon funzionamento dei componenti addizionali: Filtro chiamate ed SMS, Filtro URL, Antifurto, Parental control e Firewall.

Inoltre, su alcuni dispositivi è necessario disattivare l'ottimizzazione profonda e l'avvio automatico.

Dopo un'installazione di aggiornamenti del sistema operativo, le impostazioni di ottimizzazione possono essere resettate. In questo caso sarà necessario modificarle di nuovo.

Le impostazioni e la loro posizione possono variare in base ai diversi modelli del dispositivo e le versioni del sistema operativo. Se queste istruzioni non risolvono il problema, contattare il servizio di supporto tecnico.

Per disattivare l'ottimizzazione della batteria

1. Nelle impostazioni del dispositivo aprire **Batteria** > **Ottimizzazione batteria**.
2. Selezionare l'applicazione Dr.Web.
3. Selezionare l'opzione **Non ottimizzare** e premere **Finito**.

Per fissare Dr.Web in modalità background

1. Aprire le applicazioni recenti.
2. Premere l'icona con lucchetto accanto all'applicazione Dr.Web.

Per disattivare l'ottimizzazione profonda

1. Nelle impostazioni del dispositivo aprire **Batteria** > **Ottimizzazione batteria**.
2. Premere l'icona delle impostazioni nell'angolo superiore destro.
3. Disattivare l'ottimizzazione profonda.

Per disattivare l'avvio automatico

1. Nelle impostazioni del dispositivo aprire **Applicazioni**.
2. Premere l'icona delle impostazioni nell'angolo superiore destro.
3. Selezionare **Avvio automatico**.
4. Disattivare l'avvio automatico per l'applicazione Dr.Web.

8.7.6.6. Oppo

Affinché l'applicazione Dr.Web funzioni correttamente in background sui dispositivi Oppo, modificare le seguenti impostazioni:

- Consentire l'avvio automatico

  L'avvio automatico consente di avviare i processi dell'applicazione subito dopo che il dispositivo viene acceso. È necessario per la protezione antivirus continua del dispositivo e per il buon funzionamento dei componenti addizionali: Filtro chiamate ed SMS, Filtro URL, Antifurto, Parental control e Firewall.
- Fissare Dr.Web in modalità background

  Il funzionamento in background consente all'applicazione di continuare a rimanere in esecuzione anche se non è attiva. È necessario per la protezione antivirus continua del dispositivo e per il buon funzionamento dei componenti addizionali: Filtro chiamate ed SMS, Filtro URL, Antifurto, Parental control e Firewall.
- Consentire il funzionamento in background, se sul dispositivo c'è l'applicazione Centro sicurezza

> Le impostazioni e la loro posizione possono variare in base ai diversi modelli del dispositivo e le versioni del sistema operativo. Se queste istruzioni non risolvono il problema, contattare il servizio di supporto tecnico.

Per consentire l'avvio automatico

1. Nelle impostazioni del dispositivo aprire **Gestione app**.

2. Selezionare l'applicazione Dr.Web.
3. Consentire l'avvio automatico.

Per fissare Dr.Web in modalità background

1. Aprire le applicazioni recenti.
2. Impostare l'icona con lucchetto per l'applicazione Dr.Web.

Per consentire il funzionamento in background

1. Aprire **Centro sicurezza**.
2. Selezionare **Autorizzazioni privacy** > **Gestione avvio**.
3. Concedere a Dr.Web il permesso di funzionamento in background.

8.7.6.7. Samsung

Affinché l'applicazione Dr.Web funzioni correttamente in background sui dispositivi Samsung, modificare le seguenti impostazioni:

- Fissare Dr.Web in modalità background

Il funzionamento in background consente all'applicazione di continuare a rimanere in esecuzione anche se non è attiva. È necessario per la protezione antivirus continua del dispositivo e per il buon funzionamento dei componenti addizionali: Filtro chiamate ed SMS, Filtro URL, Antifurto, Parental control e Firewall.

Le impostazioni e la loro posizione possono variare in base ai diversi modelli del dispositivo e le versioni del sistema operativo. Se queste istruzioni non risolvono il problema, contattare il servizio di supporto tecnico.

Per fissare Dr.Web in modalità background

1. Aprire le applicazioni recenti.
2. Premere l'icona Dr.Web. Dal menu a discesa selezionare **Mantieni aperta** o **Aggiungi applicazione**.

   Per l'applicazione fissata comparirà l'icona del lucchetto.

8.7.6.8. Sony

Affinché l'applicazione Dr.Web funzioni correttamente in background sui dispositivi Sony, disattivare l'ottimizzazione della batteria per Dr.Web.

Se Dr.Web è un amministratore del dispositivo, questa impostazione di ottimizzazione non è disponibile.

Per ottimizzare l'utilizzo della batteria, il sistema operativo può arrestare l'applicazione Dr.Web. Ciò interromperà la protezione antivirus continua del dispositivo e il funzionamento dei componenti addizionali attivati: Filtro chiamate ed SMS, Filtro URL, Antifurto, Parental control e Firewall.

> ⚠ Le impostazioni e la loro posizione possono variare in base ai diversi modelli del dispositivo e le versioni del sistema operativo. Se queste istruzioni non risolvono il problema, contattare il servizio di supporto tecnico.

Per disattivare l'ottimizzazione della batteria

1. Sulla schermata principale del dispositivo premere .
2. Selezionare **Impostazioni** > **Batteria**.
3. Premere e selezionare **Ottimizzazione batteria**.
4. Premere **Applicazioni**. Verrà visualizzata una lista di applicazioni che risparmiano batteria.
5. Spuntare il flag accanto a Dr.Web. L'applicazione verrà visualizzata nella scheda **Non ottimizzate**.

> ⚠ In modalità Ultra STAMINA applicazioni non possono essere escluse dall'ottimizzazione.

8.7.6.9. Xiaomi

Affinché l'applicazione Dr.Web funzioni correttamente in background sui dispositivi Xiaomi, modificare le seguenti impostazioni:

- Consentire l'avvio automatico

  L'avvio automatico consente di avviare i processi dell'applicazione subito dopo che il dispositivo viene acceso. È necessario per la protezione antivirus continua del dispositivo e per il buon funzionamento dei componenti addizionali: Filtro chiamate ed SMS, Filtro URL, Antifurto, Parental control e Firewall.
- Consentire il funzionamento in background

  Il funzionamento in background consente all'applicazione di continuare a rimanere in esecuzione anche se non è attiva. È necessario per la protezione antivirus continua del dispositivo e per il buon funzionamento dei componenti addizionali: Filtro chiamate ed SMS, Filtro URL, Antifurto, Parental control e Firewall.
- Fissare Dr.Web in modalità background

  Il funzionamento in background consente all'applicazione di continuare a rimanere in esecuzione anche se non è attiva. È necessario per la protezione antivirus continua del dispositivo e per il buon funzionamento dei componenti addizionali: Filtro chiamate ed SMS, Filtro URL, Antifurto, Parental control e Firewall.
- Consentire le finestre a comparsa, se è attivato Antifurto o Parental control

In modalità background Antifurto e Parental control utilizzano le finestre a comparsa per limitare l'accesso a una singola applicazione o all'intero dispositivo.

Le impostazioni e la loro posizione possono variare in base ai diversi modelli del dispositivo e le versioni del sistema operativo. Se queste istruzioni non risolvono il problema, contattare il servizio di supporto tecnico.

Per consentire l'avvio automatico

1. Nelle impostazioni del dispositivo selezionare **Applicazioni**.
2. Nella lista delle applicazioni selezionare Dr.Web.
3. Consentire l'avvio automatico.

Per consentire il funzionamento in background

1. Nelle impostazioni del dispositivo selezionare **Applicazioni**.
2. Nella lista delle applicazioni selezionare Dr.Web.
3. Selezionare l'impostazione **Controllo attività**.
4. Selezionare l'opzione **Nessuna limitazione**.

Per fissare Dr.Web in modalità background

1. Aprire le applicazioni recenti.
2. Premere l'icona con lucchetto accanto all'applicazione Dr.Web.

Alcune versioni del sistema operativo consentono anche di fissare applicazioni in modalità background attraverso l'applicazione incorporata **Sicurezza**:

1. Nell'applicazione **Sicurezza** aprire la sezione **Incremento velocità**.
2. Premere l'icona delle impostazioni nell'angolo superiore destro dello schermo.
3. Selezionare la voce **Blocco app**.
4. Nella lista delle applicazioni trovare Dr.Web.
5. Utilizzare l'interruttore a destra di Dr.Web per fissare l'applicazione in modalità background.

Per consentire le finestre a comparsa

1. Nelle impostazioni del dispositivo selezionare **Applicazioni**.
2. Nella lista delle applicazioni selezionare Dr.Web.
3. Selezionare **Altre autorizzazioni**.
4. Nella lista dei permessi attivare la visualizzazione in background delle finestre a comparsa.

8.8. Statistiche

Dr.Web registra le statistiche delle minacce rilevate e delle azioni dell'applicazione.

Per visualizzare le statistiche di funzionamento dell'applicazione, sulla schermata principale di Dr.Web premere **Menu** e selezionare la voce **Statistiche**.

Visualizzazione delle statistiche

Nella scheda **Statistiche** sono disponibili due sezioni di informazioni (vedi Immagine 32):

- **Totale**. Contiene informazioni sul numero totale di file controllati e di minacce rilevate e neutralizzate.
- **Eventi**. Contiene informazioni sui risultati delle scansioni tramite Scanner Dr.Web, sull'attivazione/la disattivazione del componente SpIDer Guard, sullo stato di aggiornamento dei database dei virus, sulle minacce rilevate e le azioni eseguite per neutralizzarle.

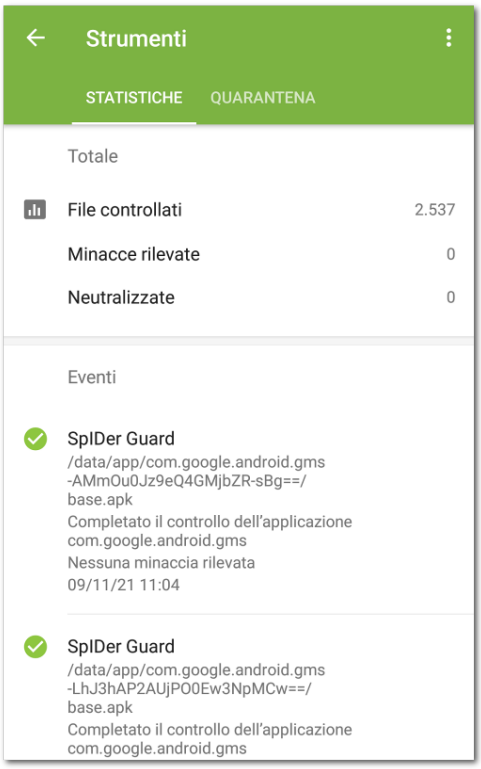

Immagine 32. Statistiche

Pulizia delle statistiche

Per rimuovere tutte le statistiche di funzionamento dell'applicazione raccolte, nella scheda **Statistiche** premere **Menu** e selezionare la voce **Cancella le statistiche**.

Salvataggio del log degli eventi

È possibile salvare il log degli eventi dell'applicazione per il successivo invio al servizio di supporto tecnico Doctor Web in caso di problemi durante l'utilizzo dell'applicazione.

1. Nella scheda **Statistiche** premere **Menu** e selezionare **Salva il log**.
2. Il log viene salvato nei file `DrWeb_Log.txt` e `DrWeb_Err.txt` situati nella cartella `Android/data/com.drweb/files` nella memoria interna del dispositivo.

> Sui dispositivi con Android 11.0 o versioni successive i log vengono salvati nella cartella `Download/DrWeb`.

8.9. Quarantena

Per le minacce rilevate è disponibile l'opzione di spostamento in quarantena — una cartella specifica progettata per il loro isolamento e l'archiviazione sicura (vedi Immagine 33).

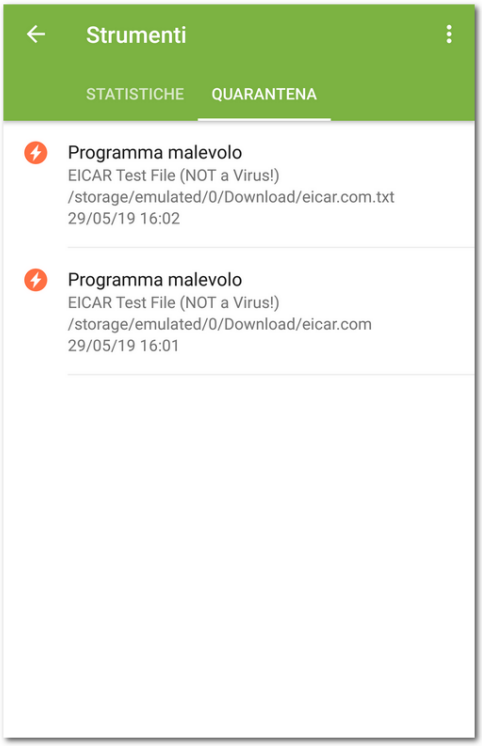

Immagine 33. Quarantena

Visualizzazione della lista degli oggetti in quarantena

Per visualizzare la lista delle minacce spostate in quarantena:

1. Sulla schermata principale di Dr.Web premere **Menu**.

> Su Android TV sulla schermata principale di Dr.Web selezionare la voce **Varie**.

2. Selezionare la voce **Quarantena**.

Si aprirà la lista di tutte le minacce che si trovano in quarantena.

Visualizzazione delle informazioni sulle minacce

Per visualizzare informazioni su una minaccia, premere il suo nome nella lista.

Per ciascuna minaccia è possibile visualizzare le seguenti informazioni:

- nome del file;
- percorso del file;
- data e ora di trasferimento in quarantena.

Opzioni disponibili

Per ciascuna minaccia sono disponibili le seguenti opzioni:

- **Maggiori informazioni su Internet** — per visualizzare la descrizione della minaccia sul sito Doctor Web.
- **Ripristina** — per far tornare il file nella cartella in cui si trovava prima dello spostamento in quarantena (utilizzare questa funzione solo se si è sicuri che il file è innocuo).
- **Elimina** — per rimuovere il file da quarantena e dal sistema.
- **Falso positivo** — per inviare il file al laboratorio antivirus Doctor Web per l'analisi. L'analisi mostrerà se il file rappresenta veramente una minaccia o questo è un falso positivo. Se si è verificato un falso positivo, esso verrà corretto. Per ricevere i risultati dell'analisi, indicare il proprio indirizzo email.

> L'opzione **Falso positivo** è disponibile solo per varianti di minacce.

Rimozione di tutti gli oggetti da quarantena

Per rimuovere tutti gli oggetti spostati in quarantena:

1. Aprire la sezione **Quarantena**.
2. Sulla schermata **Quarantena** premere **Menu** e selezionare la voce **Elimina tutto**.
3. Premere **OK** per confermare l'azione.

   Premere **Annulla** per annullare la rimozione e tornare alla sezione **Quarantena**.

Dimensione quarantena

Per visualizzare informazioni sulla quantità di memoria occupata dalla quarantena e sullo spazio libero nella memoria interna del dispositivo:

1. Aprire la sezione **Quarantena**.
2. Sulla schermata **Quarantena** premere **Menu** e selezionare la voce **Dimensione quarantena**.
3. Premere **OK** per tornare alla sezione **Quarantena**.

9. Impostazioni

Per passare alle impostazioni dell'applicazione (v. Immagine 34), sulla schermata principale di Dr.Web premere **Menu** e selezionare la voce **Impostazioni**.

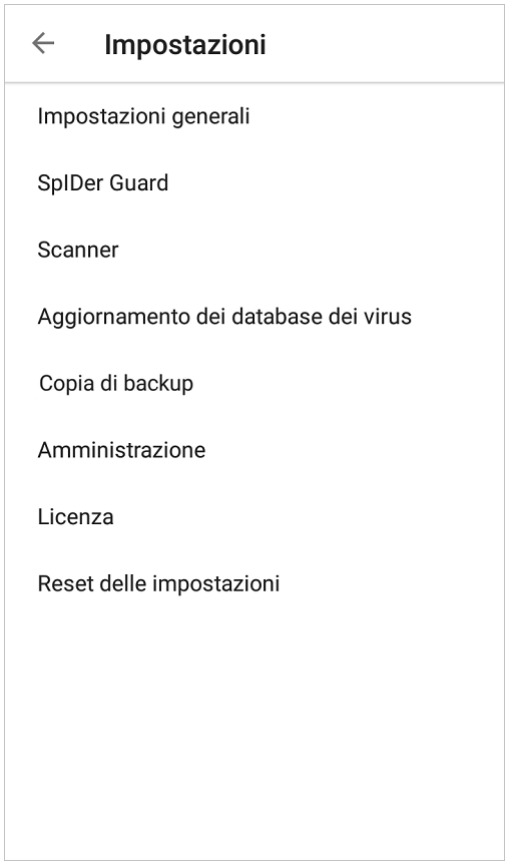

Immagine 34. Impostazioni

Se si è impostata una password di accesso alle impostazioni dell'applicazione, sarà necessario immettere la password dell'account.

Sulla schermata **Impostazioni** sono disponibili le seguenti opzioni:

- **Impostazioni generali**. Permette di configurare la barra delle notifiche, attivare e disattivare gli avvisi acustici e modificare i parametri di invio delle statistiche (vedi sezione Impostazioni generali).
- **SpIDer Guard**. Permette di configurare le impostazioni del componente SpIDer Guard che verifica costantemente l'eventuale presenza di minacce alla sicurezza nel file system e tiene traccia di modifiche nell'area di sistema (vedi sezione Impostazioni di SpIDer Guard).
- **Scanner**. Permette di configurare il componente Scanner che esegue una verifica a richiesta dell'utente (vedi sezione Impostazioni di Scanner Dr.Web).
- **Aggiornamento dei database dei virus**. Permette di vietare l'uso di internet mobile per l'aggiornamento dei database dei virus (vedi sezione Aggiornamento dei database dei virus).

- **Copia di backup**. Permette di importare ed esportare le impostazioni dell'applicazione (vedi sezione Copia di backup).
- **Amministrazione**. Permette di passare a modalità di protezione centralizzata (l'opzione è disponibile per la versione dell'applicazione installata dal sito Doctor Web).
- **Licenza**. Permette di attivare o disattivare l'uso degli avvisi di imminente scadenza della licenza (vedi sezione Configurazione degli avvisi di scadenza della licenza).
- **Reset delle impostazioni**. Permette di resettare le impostazioni personalizzate e tornare alle impostazioni predefinite (vedi sezione Reset delle impostazioni).

Se sul dispositivo è attivato il componente Antifurto Dr.Web, quando vengono modificate alcune impostazioni dell'applicazione (**Reset delle impostazioni**, **Copia di backup** e **Amministrazione**), sarà necessario immettere la password dell'account Dr.Web.

9.1. Impostazioni generali

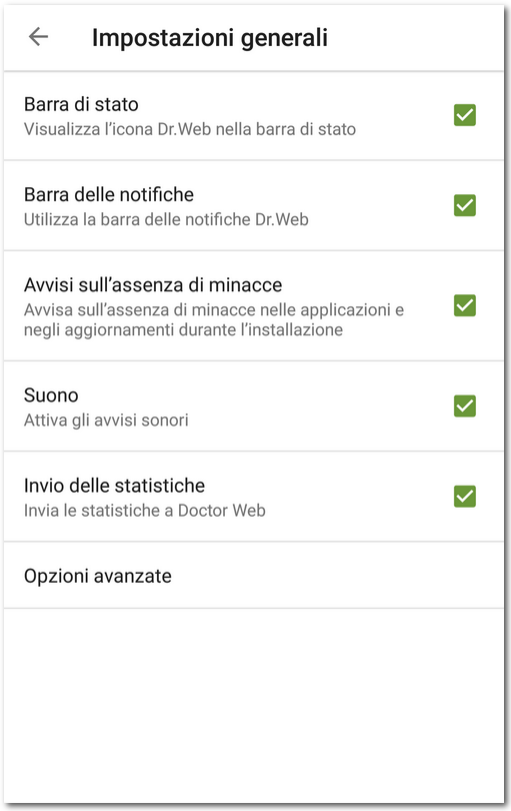

Immagine 35. Impostazioni generali

Sulla schermata **Impostazioni generali** (vedi Immagine 35) sono disponibili le seguenti opzioni:

- **Barra di stato**. Permette di configurare la visualizzazione dell'icona dell'applicazione nella barra di stato. Questa opzione permette inoltre di disattivare la visualizzazione del pannello Dr.Web nell'area delle notifiche (vedi sezione Barra delle notifiche).

L'impostazione non è disponibile sui dispositivi con Android 8.0 o versioni successive.

- **Barra delle notifiche**. Permette di determinare l'aspetto del pannello Dr.Web nell'area delle notifiche. Se l'opzione è attivata, viene utilizzato il pannello Dr.Web. Se l'opzione è disattivata, il pannello ha l'aspetto di un pannello di notifica Android standard.
- **Avvisi sull'assenza di minacce**. Permette di attivare o disattivare gli avvisi su quello che non sono state rilevate minacce nelle applicazioni o negli aggiornamenti appena installati.

L'impostazione non è disponibile sui dispositivi con Android 8.0 o versioni successive. In questo caso gli avvisi di categoria **Applicazioni sicure** possono essere attivati o disattivati nelle impostazioni del dispositivo.

- **Suono**. Permette di configurare gli avvisi sonori per segnalare che una minaccia è stata rilevata, rimossa o messa in quarantena. Di default gli avvisi sonori sono attivati.
- **Invio delle statistiche**. Permette di attivare o disattivare l'invio di statistiche all'azienda Doctor Web.
- **Opzioni avanzate**. Contiene le impostazioni aggiuntive:
  - **Applicazioni di sistema**. Permette di attivare o disattivare l'avviso sulle minacce nelle applicazioni di sistema che non possono essere rimosse senza compromettere l'operatività del dispositivo. Di default questa opzione è disattivata.

9.2. Aggiornamento dei database dei virus

Per rilevare le minacce alla sicurezza, Dr.Web utilizza database dei virus speciali che contengono informazioni su tutte le minacce informatiche per dispositivi con sistema operativo Android, conosciute dagli specialisti Doctor Web. I database dei virus richiedono un aggiornamento periodico in quanto nuovi programmi malevoli compaiono regolarmente. A tale scopo nell'applicazione è implementata la possibilità di aggiornamento dei database dei virus via internet.

In modalità di protezione centralizzata viene bloccata la possibilità di aggiornare manualmente i database dei virus. Gli aggiornamenti vengono scaricati automaticamente dal server di protezione centralizzata. Se sul server di protezione centralizzata è consentito l'avvio dell'applicazione in modalità mobile, quando la connessione al server di protezione centralizzata è interrotta, l'aggiornamento dei database dei virus può essere avviato manualmente.

Aggiornamento

I database dei virus vengono aggiornati automaticamente attraverso internet diverse volte al giorno. Se i database dei virus non vengono aggiornati da più di 24 ore (per esempio, in assenza di connessione internet), è necessario avviare l'aggiornamento manualmente.

Per scoprire se è necessario aggiornare manualmente i database dei virus

1. Sulla schermata principale di Dr.Web premere **Menu** e selezionare **Database dei virus**.
2. Nella finestra che si è aperta si vedono lo stato dei database dei virus e la data dell'ultimo aggiornamento. Se l'ultimo aggiornamento è stato più di 24 ore fa, è necessario eseguire l'aggiornamento manualmente.

Per avviare l'aggiornamento

1. Sulla schermata principale di Dr.Web premere **Menu** e selezionare **Database dei virus**.
2. Nella finestra che si è aperta premere **Aggiorna**.

Subito dopo aver installato l'applicazione, è consigliabile aggiornare i database dei virus in modo che Dr.Web possa utilizzare le più recenti informazioni sulle minacce conosciute. Le firme antivirali dei virus, le informazioni sulle loro caratteristiche e sui loro modelli di comportamento vengono aggiornate non appena gli specialisti del laboratorio antivirus Doctor Web rilevano nuove minacce, talvolta fino a diverse volte all'ora.

Impostazioni di aggiornamento

Di default, gli aggiornamenti vengono scaricati automaticamente diverse volte al giorno.

Per consentire o vietare l'uso della rete mobile per il download degli aggiornamenti

1. Sulla schermata principale di Dr.Web premere **Menu** e selezionare **Impostazioni** (vedi Immagine 34).
2. Selezionare la sezione **Aggiornamento dei database dei virus**.
3. Per non utilizzare la rete mobile per il download degli aggiornamenti, spuntare il flag **Aggiornamento tramite Wi-Fi**.

Se non vengono trovate reti Wi-Fi attive, viene suggerito di utilizzare internet mobile. La modifica di questa impostazione non influisce sull'utilizzo della rete mobile da parte delle altre funzioni dell'applicazione e del dispositivo mobile.

Durante un aggiornamento i dati vengono scaricati attraverso la rete. Per il trasferimento dei dati possono essere applicati costi aggiuntivi. Rivolgersi al proprio operatore di telefonia mobile per i dettagli.

In modalità di protezione centralizzata le impostazioni di aggiornamento possono essere modificate o bloccate secondo i criteri di sicurezza aziendali o la lista dei servizi pagati.

9.3. Copia di backup

È possibile esportare le impostazioni correnti dell'applicazione in un file nella memoria interna del dispositivo. Se necessario (per esempio se Dr.Web verrà reinstallato o utilizzato su un altro dispositivo), le impostazioni potranno essere importate da questo file.

In modalità di protezione centralizzata non sono disponibili l'importazione e l'esportazione delle impostazioni.

Per esportare le impostazioni correnti in file

1. Sulla schermata delle impostazioni (vedi Immagine 34) selezionare la sezione **Copia di backup**.
2. Inserire la password dell'account.

   La password è richiesta se il componente Antifurto Dr.Web è attivato e configurato.
3. Nella finestra che si è aperta selezionare **Esportazione delle impostazioni**.
4. Impostare una password che verrà utilizzata per proteggere il file delle impostazioni e quindi premere il pulsante **OK**.

Tutte le impostazioni vengono salvate nel file `Internal storage/Android/data/com.drweb/files/DrWebPro.bkp`.

Sui dispositivi con Android 11.0 o versioni successive il file con le impostazioni viene salvato nella cartella `Download/DrWeb`.

Per importare le impostazioni da file

1. Sulla schermata delle impostazioni (vedi Immagine 34) selezionare la sezione **Copia di backup**.
2. Inserire la password dell'account.

   La password è richiesta se il componente Antifurto Dr.Web è attivato e configurato.
3. Selezionare **Importazione delle impostazioni**.
4. Confermare di voler importare le impostazioni da file.
5. Trovare il file con le impostazioni nell'albero dei file e premerlo.
6. Immettere la password impostata per il file delle impostazioni e premere **OK**.

   Tutte le impostazioni correnti verranno rimosse e sostituite con quelle importate dal file.

9.4. Reset delle impostazioni

È possibile in qualsiasi momento resettare le impostazioni personalizzate dell'applicazione, tra cui quelle di filtraggio chiamate e messaggi, Antifurto Dr.Web, Firewall Dr.Web e Filtro URL, e ripristinare le impostazioni predefinite.

In modalità di protezione centralizzata il reset delle impostazioni non è disponibile.

Per resettare le impostazioni

1. Sulla schermata delle impostazioni (vedi Immagine 34) nella sezione **Reset delle impostazioni** selezionare la voce **Reset delle impostazioni**.
2. Inserire la password dell'account Dr.Web.
3. Confermare di voler ritornare alle impostazioni predefinite.

10. Modalità di protezione centralizzata

I computer e altri dispositivi su cui sono installati i componenti Dr.Web interagenti formano una *rete antivirus*. La rete antivirus ha un'architettura client-server. Il server gestisce il client tramite Agent Dr.Web. La modalità di protezione centralizzata è la modalità di funzionamento dell'applicazione sotto la gestione di Agent Dr.Web.

La versione di Dr.Web Mobile Security Suite descritta in questo manuale è compatibile con Dr.Web AV-Desk versioni 10 e 13 e Dr.Web Enterprise Security Suite versioni 10, 11, 12 e 13.

La modalità di protezione centralizzata è disponibile per le seguenti versioni Dr.Web:

- Le versioni scaricate dal sito dell'azienda Doctor Web https://download.drweb.com/android/.
- Le versioni scaricate dall'area personale del fornitore del servizio "Antivirus Dr.Web".
- Le versioni fornite dall'amministratore della rete antivirus aziendale dell'utente.

La modalità di protezione centralizzata non è disponibile:

- Per le versioni Dr.Web installate da Google Play.
- Per la versione installata da HUAWEI AppGallery.
- Per i dispositivi con Android TV.

Componenti controllati dal server di protezione centralizzata

Le impostazioni dei componenti di Dr.Web possono essere modificate o bloccate secondo i criteri di sicurezza aziendali o la lista dei servizi pagati.

Dal server di protezione centralizzata possono essere controllati i seguenti componenti:

- 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.
- SplDer Guard.
- Filtro chiamate ed SMS.
- Antifurto Dr.Web.
- Filtro URL.
- Filtro delle applicazioni.

Concessione di licenze in modalità di protezione centralizzata

In modalità di protezione centralizzata un file della chiave di licenza viene scaricato automaticamente dal server di protezione centralizzata, e la licenza personale non viene utilizzata. Se la licenza è scaduta o è stata bloccata ed è comparso l'avviso corrispondente,

contattare l'amministratore della rete antivirus aziendale per una nuova licenza o rinnovare l'abbonamento al servizio "Antivirus Dr.Web".

Aggiornamento dei database dei virus in modalità di protezione centralizzata

In modalità di protezione centralizzata viene bloccata la possibilità di aggiornare manualmente i database dei virus, gli aggiornamenti vengono scaricati automaticamente dal server di protezione centralizzata. Le impostazioni di aggiornamento possono essere modificate o bloccate secondo i criteri di sicurezza aziendali o la lista dei servizi pagati. Se sul server di protezione centralizzata è consentito l'avvio dell'applicazione in modalità mobile, quando la connessione al server di protezione centralizzata è interrotta, l'aggiornamento dei database dei virus può essere avviato manualmente.

Aggiornamento dell'applicazione in modalità di protezione centralizzata

Alcune versioni del server di protezione centralizzata supportano l'aggiornamento di Dr.Web Mobile Security Suite. Se nelle impostazioni dell'applicazione è spuntato il flag **Nuova versione**, si riceveranno gli avvisi sulla disponibilità di una nuova versione dell'applicazione che potrà essere prontamente installata. Contattare l'amministratore della rete antivirus aziendale per dettagli.

Per le versioni scaricate dal sito dell'azienda Doctor Web l'aggiornamento dal server di protezione centralizzata non è disponibile. Per tali versioni in modalità di protezione centralizzata è possibile solo l'aggiornamento dei database dei virus.

10.1. Passaggio alla modalità di protezione centralizzata

Per mettere l'applicazione in modalità di protezione centralizzata, connettersi al server di protezione centralizzata.

Per la connessione al server di protezione centralizzata 11.0.0 o versioni successive è richiesto Dr.Web 11.0.0 o versioni successive.

Dopo la connessione al server possono essere chiesti i seguenti permessi:

- Autorizzazioni principali (l'accesso a foto, contenuti multimediali e file, contatti ecc.) — per la maggior parte delle funzionalità dell'applicazione.
- Filtro chiamate ed SMS (utilizzo di Dr.Web come applicazione per le chiamate di default) — per il filtraggio delle chiamate e degli SMS in arrivo.
- Amministrazione del dispositivo — per la protezione dell'applicazione da disinstallazioni e la completa operatività di Antifurto.
- Accesso alle funzioni di accessibilità — per il filtraggio delle applicazioni e la completa operatività di Filtro URL, Antifurto e Parental control.

- Sovrapposizione sopra altre finestre — per il filtraggio delle applicazioni e il funzionamento di Firewall.

Connessione al server di protezione centralizzata

Connessione automatica

Le versioni Dr.Web fornite dall'amministratore della rete antivirus aziendale dell'utente o dal fornitore del servizio "Antivirus Dr.Web" si connettono al server di protezione centralizzata in maniera automatica. A questo scopo, il pacchetto di installazione deve essere avviato dalla memoria interna del dispositivo.

Connessione con l'inserimento dei parametri

Per la connessione al server di protezione centralizzata sono richiesti i parametri di connessione che vengono forniti dall'amministratore della rete antivirus aziendale dell'utente o dal fornitore del servizio "Antivirus Dr.Web".

1. Assicurarsi che sia disponibile una connessione di rete.
2. Sulla schermata **Impostazioni** (vedi Immagine 34) selezionare **Amministrazione**.

   Se sul dispositivo è attivato Antifurto Dr.Web, inserire la password dell'account Dr.Web.
3. Spuntare il flag **Agent Dr.Web**.

   Il flag **Agent Dr.Web** è impostato di default nelle versioni Dr.Web fornite dall'amministratore della rete antivirus aziendale dell'utente o dal fornitore del servizio "Antivirus Dr.Web".
4. Quando viene attivata la modalità di protezione centralizzata, vengono ripristinati gli ultimi parametri di connessione al server.

   Tuttavia, se sul dispositivo è salvato un file di configurazione, vengono utilizzati i parametri di connessione da questo file. Per utilizzare altri parametri di connessione, per esempio, quelli da un pacchetto di installazione, resettare i parametri di connessione.

   Se si connette al server per la prima volta o se i parametri di connessione sono cambiati, indicare i seguenti parametri:
   - Indirizzo IP del server di protezione centralizzata.
   - I 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 ci si riconnette al server, non sarà necessario inserirli di nuovo. Per connettersi come una nuova postazione (nuovo arrivo), premere **Menu** e selezionare l'opzione **Connettiti come nuovo arrivo**.
5. Premere il pulsante **Connettiti**.

Connessione con un file di configurazione

I parametri di connessione al server di protezione centralizzata sono contenuti nel file `install.cfg` che viene fornito dall'amministratore della rete antivirus aziendale dell'utente o dal fornitore del servizio "Antivirus Dr.Web".

1. Assicurarsi che sia disponibile una connessione di rete.
2. Mettere il file `install.cfg` nella cartella radice o in qualsiasi delle cartelle di primo livello di nidificazione della memoria interna del dispositivo.
3. Sulla schermata delle impostazioni (vedi Immagine 34) selezionare **Amministrazione**.

   Se sul dispositivo è attivato Antifurto Dr.Web, a passaggio alla sezione **Amministrazione** è necessario immettere la password dell'account Dr.Web.
4. Spuntare il flag **Agent Dr.Web**.

   Se il file è caricato sul dispositivo, i campi di immissione dei parametri di connessione al server verranno compilati in automatico.

   > Il flag **Agent Dr.Web** è impostato di default nelle versioni Dr.Web fornite dall'amministratore della rete antivirus aziendale o dal fornitore del servizio "Antivirus Dr.Web". 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 contiene parametri di connessione non validi, è necessario togliere e spuntare nuovamente il flag **Agent Dr.Web** ed inserire i parametri manualmente o utilizzare un file di configurazione con le impostazioni corrette.
5. Premere il pulsante **Connettiti**.

Reset dei parametri di connessione

1. Premere **Menu** sulla schermata di inserimento dei 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 rimosso. Se sul dispositivo è disponibile un altro file `install.cfg`, verranno utilizzati i parametri di connessione da questo file. Pertanto, i parametri di connessione verranno resettati solo dopo che verranno rimossi 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 traffico, non supportate da Dr.Web. Contattare l'amministratore della rete antivirus o il fornitore del servizio "Antivirus Dr.Web" per risolvere il problema.

La licenza (l'abbonamento) è scaduta. Contattare l'amministratore della rete antivirus per ottenere una licenza, o rinnovare l'abbonamento al servizio "Antivirus Dr.Web".

L'abbonamento è bloccato. Contattare il fornitore del servizio "Antivirus Dr.Web" per sbloccare l'abbonamento.

L'avvio di Dr.Web per Android è vietato sul server. 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 proibita dall'amministratore della rete antivirus.

10.2. Amministrazione

Se sul server di protezione centralizzata è attivata la possibilità di modificare la configurazione del Filtro delle applicazioni, è possibile selezionare applicazioni che è consentito avviare sul dispositivo.

È possibile consentire/vietare l'avvio sia delle applicazioni di sistema che delle applicazioni utente. Le applicazioni di sistema si trovano in cima alla lista e sono contrassegnate di default come consentite. Più in basso nella lista si trovano le applicazioni utente.

Per configurare il Filtro delle applicazioni

1. Sulla schermata principale di Dr.Web aprire la sezione **Amministrazione**.
2. Selezionare le applicazioni che saranno disponibili sul dispositivo.
3. Premere il pulsante **Consenti quelle selezionate**. Le impostazioni configurate verranno trasmesse sul server e salvate come le impostazioni individuali per il dispositivo.

> Le impostazioni di avvio applicazioni configurate sul dispositivo utente verranno applicate solo se sul server di protezione centralizzata per questo dispositivo è attivato il Filtro delle applicazioni.

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.

10.3. Passaggio alla modalità autonoma

Per mettere Dr.Web in modalità autonoma, aprire la schermata delle impostazioni (vedi Immagine 34) e selezionare la voce **Amministrazione**. Quindi deselezionare il flag **Agent Dr.Web**.

Quando viene attivata la modalità autonoma, vengono ripristinate tutte le impostazioni dell'antivirus definite prima del passaggio alla modalità centralizzata o le impostazioni di default. Inoltre, si recupera l'accesso a tutte le funzionalità di Dr.Web.

Per il funzionamento in modalità autonoma è richiesta una licenza personale valida. La licenza ricevuta automaticamente dal server di protezione centralizzata non può essere usata in questa modalità. Se necessario, è possibile acquistare o rinnovare una licenza personale.

11. Dr.Web su Android TV

Sulla schermata principale di Dr.Web (vedi Immagine 36) sono disponibili le seguenti opzioni:

- Eventi
- Scanner
- Firewall
- Auditor di sicurezza
- Varie

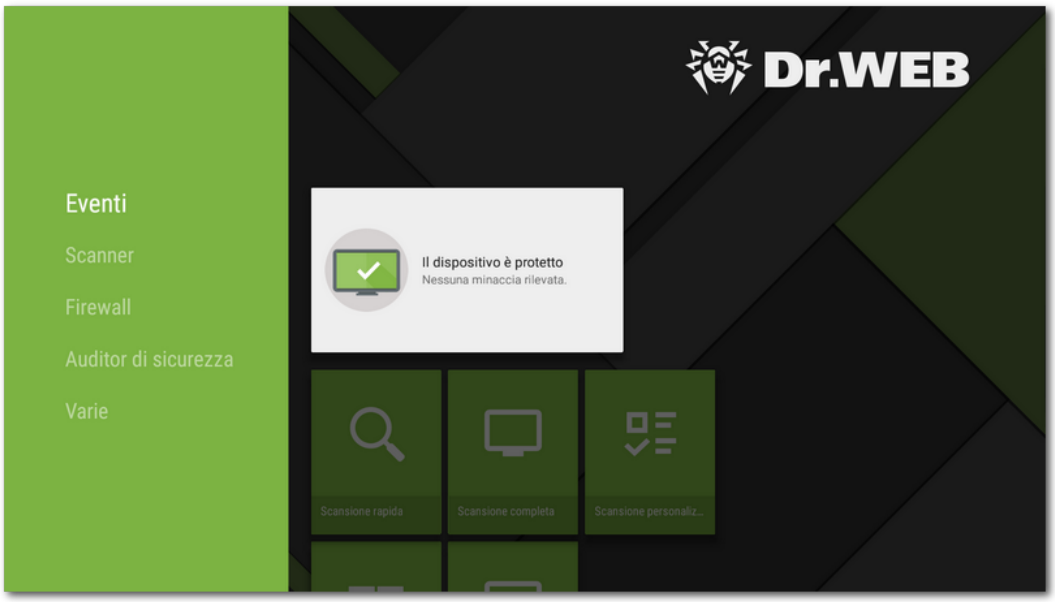

Immagine 36. Dr.Web su Android TV

Caratteristiche dell'utilizzo di Dr.Web su Android TV

Sui dispositivi con Android TV la modalità di protezione centralizzata non è disponibile.

Permessi

Al primo avvio l'applicazione chiederà di concedere i seguenti permessi:

- L'accesso a foto, multimedia e file sul dispositivo.
- L'accesso ai contatti.

Consentire all'applicazione di accedere alle funzioni e ai dati necessari.

Sui dispositivi con Android 11.0 o versioni successive l'applicazione chiede anche il permesso di accesso a tutti i file.

Per concedere l'accesso a tutti i file

1. Nella finestra della richiesta di permesso premere il pulsante **Vai su Impostazioni**.
2. Sulla schermata delle impostazioni di sistema Dr.Web selezionare la voce **Permessi**.
3. Selezionare la voce **File e contenuti multimediali**.
4. Selezionare l'opzione **Consenti sempre**.
5. Nella finestra di dialogo premere il pulsante **Consenti**.

Interfaccia

- Non è possibile creare un widget per il desktop.
- Non è disponibile la barra delle notifiche.

11.1. Eventi su Android TV

La barra **Eventi** mostra lo stato corrente di protezione del dispositivo.

- L'indicatore verde significa che il dispositivo è protetto. Non è richiesta alcuna azione aggiuntiva.
- L'indicatore giallo significa che Dr.Web ha rilevato problemi di sicurezza, per esempio, l'assenza della licenza, o una vulnerabilità. Per avere ulteriori informazioni sui problemi trovati e risolverli, selezionare la barra di stato.
- L'indicatore rosso significa che Dr.Web ha rilevato modifiche sospette all'area di sistema o minacce. Per aprire i risultati del controllo e neutralizzare le minacce, selezionare la barra di stato.

Se Dr.Web ha rilevato più eventi che richiedono attenzione, selezionare la barra di stato. Si aprirà la finestra **Eventi** in cui verranno visualizzati tutti i messaggi importanti.

11.2. Protezione antivirus su Android TV

- SpIDer Guard controlla il file system in tempo reale.
- Scanner Dr.Web consente di avviare manualmente una scansione per verificare presenza di minacce.
- Sulla schermata Risultati del controllo è possibile selezionare le azioni per neutralizzare le minacce alla sicurezza rilevate.

11.2.1. Protezione continua SpIDer Guard su Android TV

Attivazione della protezione continua

Quando Dr.Web viene aperto per la prima volta, la protezione continua viene avviata automaticamente dopo l'accettazione del Contratto di licenza. SpIDer Guard funziona a prescindere da quello se l'applicazione è in esecuzione o meno. Se SpIDer Guard rileva una modifica sospetta nell'area di sistema o una minaccia, nella parte inferiore dello schermo compare un messaggio di avviso.

Impostazione

Per attivare, configurare o disattivare la protezione continua, sulla schermata principale di Dr.Web selezionare **Varie** > **Impostazioni** > **SpIDer Guard** (vedi sezione Impostazioni Dr.Web su Android TV).

Statistiche

L'applicazione registra gli eventi relativi al funzionamento di SpIDer Guard: attivazione/disattivazione, rilevamento di minacce alla sicurezza e risultati della verifica della memoria del dispositivo e delle applicazioni che vengono installate. Le statistiche di SpIDer Guard vengono visualizzate nella sezione **Eventi** nella scheda **Statistiche** e sono ordinate per data (vedi sezione Statistiche).

11.2.2. Scanner Dr.Web su Android TV

Una scansione del sistema on demand 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 del file system se SpIDer Guard è stato inattivo per qualche tempo. Di solito in questo caso è sufficiente eseguire una scansione rapida del sistema.

Scansione

Per eseguire una scansione del sistema, sulla schermata principale di Dr.Web selezionare l'opzione **Scanner** (vedi Immagine 37) ed eseguire una delle seguenti azioni:

- Per avviare una scansione delle sole applicazioni installate, selezionare la voce **Scansione rapida**.
- Per avviare una scansione di tutti i file del sistema, selezionare la voce **Scansione completa**.
- Per verificare singoli file e cartelle, selezionare la voce **Scansione personalizzata** e quindi selezionare un oggetto da verificare nella finestra che è comparsa.

È possibile verificare una cartella per intero. Per farlo, selezionare l'opzione **Verifica cartella**. Per salire di un livello, selezionare l'opzione **Torna in alto**.

Se sul dispositivo sono disponibili i permessi di root, è possibile selezionare per la scansione le cartelle `/sbin` e `/data` locate nella cartella radice.

Dopo la fine della scansione sullo schermo vengono visualizzate le seguenti informazioni:

- Numero di oggetti scansionati.
- Numero di minacce rilevate.
- Ora di avvio della scansione.
- Durata della scansione.

Per aprire i risultati del controllo, selezionare **OK**.

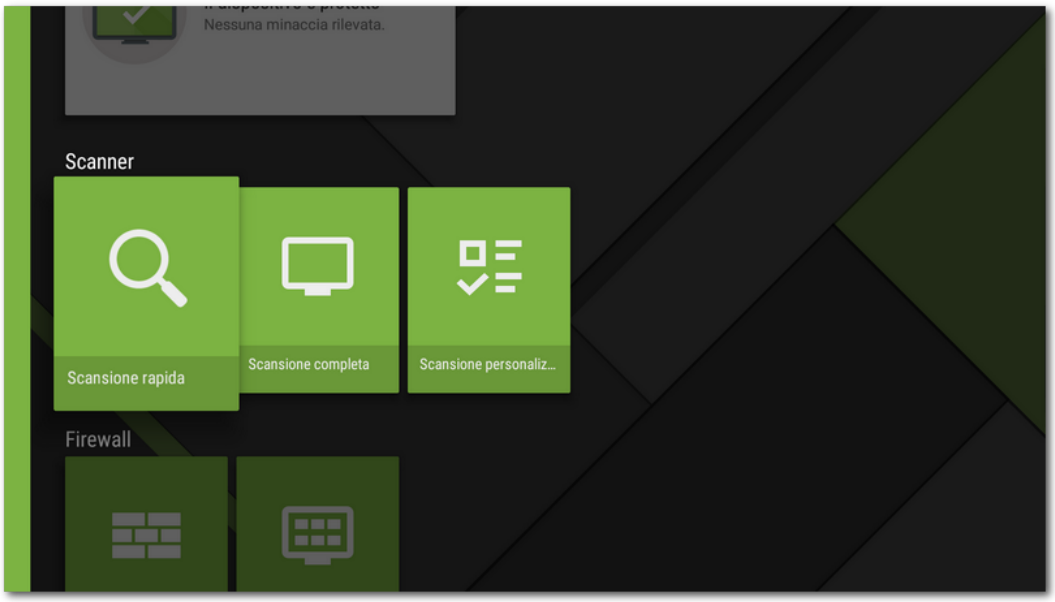

Immagine 37. Scanner Dr.Web

Impostazioni di Scanner Dr.Web

Per accedere alle impostazioni di Scanner Dr.Web, sulla schermata principale di Dr.Web selezionare **Varie** > **Impostazioni** > **Scanner** (vedi sezione Impostazioni Dr.Web su Android TV).

Statistiche

L'applicazione registra gli eventi relativi al funzionamento di Scanner Dr.Web (tipo di scansione, risultati della scansione, rilevamento di minacce alla sicurezza). Le azioni dell'applicazione vengono visualizzate nella sezione **Eventi** nella scheda **Statistiche**, ordinate per data (vedi sezione Statistiche).

11.2.3. Risultati del controllo su Android TV

Come aprire i risultati del controllo

Se il componente SplDer Guard rileverà una modifica sospetta nell'area di sistema o una minaccia, nella parte inferiore dello schermo comparirà un messaggio di avviso. Per aprire i risultati del controllo, sulla schermata principale di Dr.Web selezionare l'opzione **Eventi**.

Per aprire i risultati del controllo di Scanner Dr.Web, dopo la fine del controllo selezionare **OK**.

Neutralizzazione delle minacce

Sulla schermata **Risultati del controllo** è possibile visualizzare la lista delle minacce e modifiche sospette nell'area di sistema. Per ciascun oggetto sono indicati il suo tipo e nome, nonché l'icona dell'opzione che è raccomandata per questo oggetto.

Gli oggetti sono contrassegnati con colori diversi a seconda del grado di pericolo. Tipi di oggetti in ordine di diminuzione del pericolo:

1. Programma malevolo.
2. Riskware.
3. Hacktool.
4. Adware.
5. Modifiche nell'area di sistema:
   - File nuovi nell'area di sistema.
   - Modifica dei file di sistema.
   - Eliminazione dei file di sistema.
6. Joke.

Per visualizzare il percorso di un file, selezionare l'oggetto corrispondente. Nel caso di minacce rilevate in applicazioni è indicato anche il nome del pacchetto dell'applicazione.

Neutralizzazione di tutte le minacce

Per rimuovere tutte le minacce contemporaneamente

- Nell'angolo superiore destro della schermata **Risultati del controllo** selezionare **Menu** > **Elimina tutto**.

Per spostare in quarantena tutte le minacce contemporaneamente

- Nell'angolo superiore destro della schermata **Risultati del controllo** selezionare **Menu** >

Tutto in quarantena.

Neutralizzazione delle minacce una per una

Per ciascun oggetto è disponibile il proprio set di opzioni. Per espandere una lista delle opzioni, selezionare un oggetto. Le opzioni consigliate sono elencate per prime. Selezionare una delle opzioni:

Cura per curare un'applicazione infetta.

L'opzione è disponibile per alcune minacce nelle applicazioni di sistema, se sul dispositivo sono disponibili i permessi di root.

Elimina per rimuovere completamente una minaccia dalla memoria del dispositivo.

In alcuni casi Dr.Web non può rimuovere applicazioni che utilizzano le funzioni di accessibilità Android. Se Dr.Web non rimuoverà un'applicazione dopo la selezione dell'opzione **Elimina**, passare a modalità provvisoria e rimuovere l'applicazione manualmente. Se a Dr.Web è concesso l'accesso alle funzioni di accessibilità, l'applicazione verrà rimossa automaticamente dopo la selezione dell'opzione **Elimina**.

L'opzione non è disponibile per le minacce nelle applicazioni di sistema nei seguenti casi:

- Se sul dispositivo non sono disponibili i permessi di root.
- Se la rimozione di un'applicazione può compromettere l'operatività del dispositivo.
- Se è stata rilevata una versione di una minaccia. Per determinare se un'applicazione rappresenta davvero una minaccia, segnalare un falso positivo.

In quarantena per spostare la minaccia in una cartella isolata (vedi sezione Quarantena).

Se una minaccia è stata rilevata in un'applicazione installata, non può essere spostata in quarantena. In questo caso l'opzione **In quarantena** non è disponibile.

Ignora per lasciare temporaneamente intatta la modifica nell'area di sistema o la minaccia.

Blocca per disattivare l'accesso dell'applicazione alle connessioni internet.

L'opzione è disponibile per le minacce nelle applicazioni di sistema.

Invia al laboratorio o **Falso positivo** per inviare il file al laboratorio antivirus Doctor Web per l'analisi. L'analisi mostrerà se questa è davvero una minaccia o un falso positivo. Se si è verificato un falso positivo, esso verrà corretto. Per ricevere i risultati dell'analisi, indicare un indirizzo email.

Se il file è stato correttamente inviato al laboratorio, all'oggetto viene automaticamente applicata l'azione **Ignora**.

L'opzione **Invia al laboratorio** è disponibile solo per file eseguibili aggiunti o modificati nell'area di sistema: `.jar`, `.odex`, `.so`, file di formato APK, ELF ecc.

L'opzione **Falso positivo** è disponibile solo per versioni di minacce e per le minacce nell'area di sistema.

Maggiori informazioni su Internet per aprire la pagina con la descrizione dell'oggetto

rilevato sul sito Doctor Web.

11.3. Firewall Dr.Web su Android TV

Firewall Dr.Web protegge il dispositivo da accessi non autorizzati dall'esterno e previene fughe di dati importanti attraverso la rete. Questo componente consente di controllare connessioni e il trasferimento di dati attraverso Internet e di bloccare connessioni inattendibili.

Caratteristiche dell'utilizzo

Firewall Dr.Web è realizzato sulla base della tecnologia di VPN per Android, il che gli permette di funzionare senza l'ottenimento dei permessi di superutente (root) sul dispositivo. La realizzazione della tecnologia di VPN su Android è associata con alcune limitazioni:

- In primo luogo, in ciascun momento solo un'applicazione alla volta sul dispositivo può utilizzare la VPN. Di conseguenza, quando un'applicazione abilita la VPN sul dispositivo, si apre una finestra con la richiesta del permesso di utilizzare la VPN per questa applicazione. Se l'utente concede tale permesso, l'applicazione inizia a utilizzare la VPN; mentre un'altra applicazione che utilizzava la VPN fino a quel momento perde questa possibilità. Tale richiesta compare alla prima attivazione di Firewall Dr.Web e successivamente ad ogni riavvio del dispositivo. Inoltre, può comparire anche quando la VPN viene richiesta da altre applicazioni. La VPN deve essere condivisa nel tempo tra le applicazioni, e Firewall è in grado di funzionare solo quando possiede completamente i permessi di utilizzo della VPN.
- L'abilitazione di Firewall Dr.Web può portare all'impossibilità di connettere il dispositivo su cui è in esecuzione ad altri dispositivi direttamente attraverso Wi-Fi o una rete locale. Questo dipende dal modello del dispositivo e dalle applicazioni utilizzate per la connessione.
- Con Firewall Dr.Web attivato non è possibile utilizzare il dispositivo come un punto di accesso Wi-Fi.

La tecnologia VPN per Android viene utilizzata solo per l'implementazione delle funzioni di Firewall, tuttavia, non viene creato alcun tunnel VPN e il traffico internet non viene cifrato.

Per attivare Firewall Dr.Web

1. Sulla schermata principale di Dr.Web selezionare l'opzione **Firewall** (vedi Immagine 38).
2. Eseguire una delle seguenti azioni:
   - Utilizzare l'interruttore a destra della voce **Log**.
   - Selezionare la voce **Traffico** o **Log** e premere **Attiva**.

Di default Firewall è disattivato. Dr.Web chiede il permesso di connessione alla VPN. Per il funzionamento di Firewall, è necessario concedere questo permesso.

Se nel processo di funzionamento il permesso di utilizzare VPN passa a un'altra applicazione, Firewall Dr.Web viene disattivato, di cui viene visualizzato un avviso corrispondente.

Se si utilizza il dispositivo in modalità di accesso limitato (profilo ospite), le impostazioni di Firewall Dr.Web non saranno disponibili.

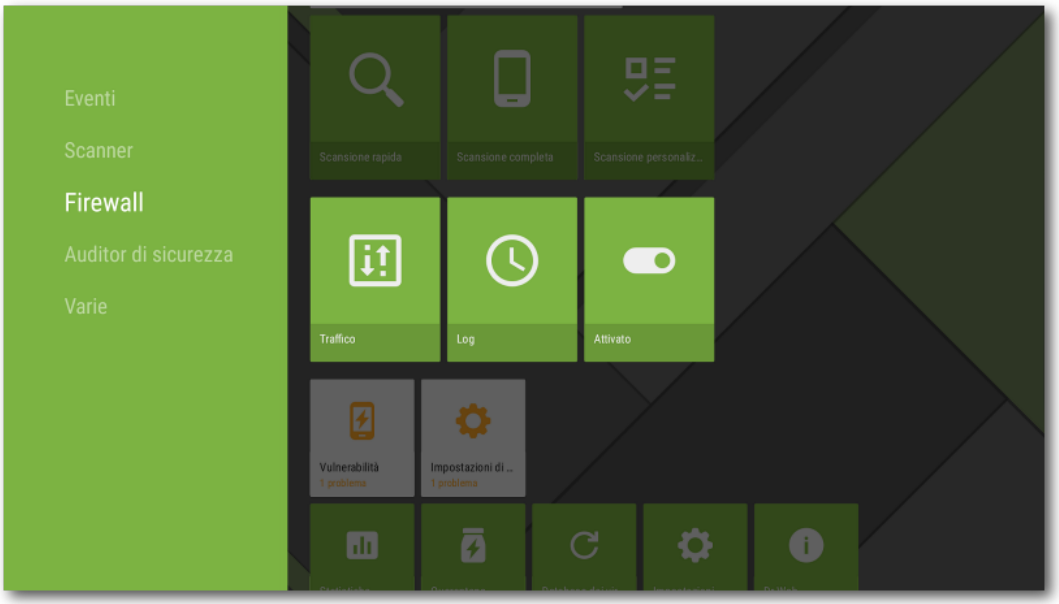

Immagine 38. Firewall Dr.Web su Android TV

11.3.1. Attività delle connessioni di rete su Android TV

Le informazioni sull'attività delle connessioni di rete possono essere ottenute sulla schermata **Traffico**. Sulla schermata sono disponibili due schede: **Applicazioni attive** e **Tutte le applicazioni** (v. Immagine 39).

Scheda Applicazioni attive

Sulla scheda viene visualizzata in tempo reale la lista delle connessioni avviate dalle applicazioni installate sul dispositivo.

Per ciascuna applicazione sulla scheda **Applicazioni attive** vengono visualizzate le seguenti informazioni:

- Quantità complessiva di traffico in entrata e in uscita sulle connessioni stabilite.
- Accesso al trasferimento dati via Wi-Fi.
- Presenza di impostazioni utente. Le applicazioni con accesso a trasferimento dati modificato sono contrassegnate dal badge .

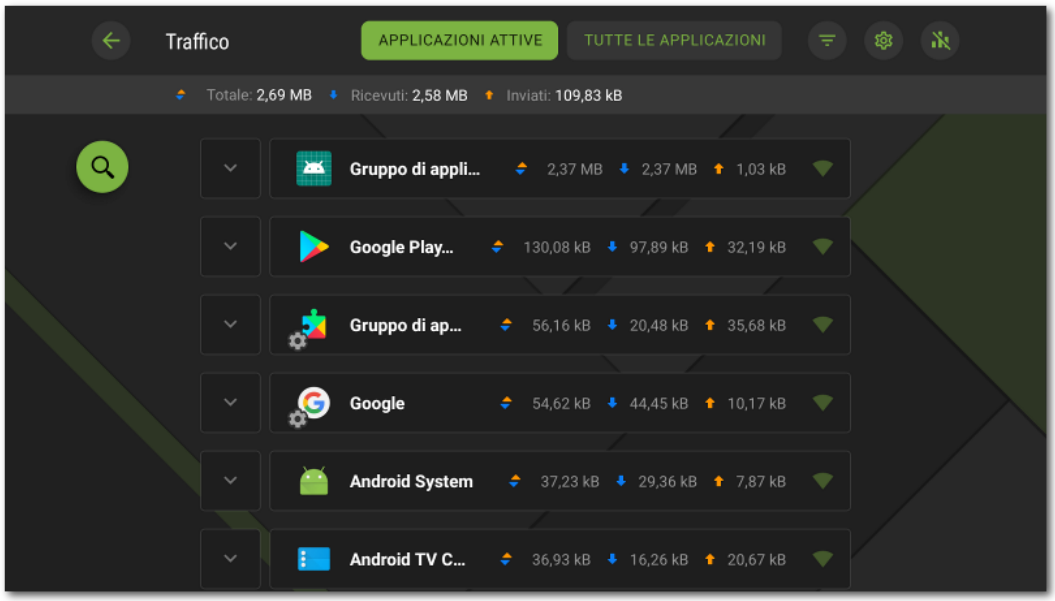

Immagine 39. Scheda Applicazioni attive

Connessioni delle applicazioni

Premere l'icona ⌄ a sinistra del nome di un'applicazione per vedere informazioni dettagliate sulle connessioni stabilite dall'applicazione:

- lista delle connessioni stabilite;
- quantità di traffico in entrata e in uscita su ciascuna delle connessioni stabilite;
- presenza per la connessione di una regola:
  - 🟢 di permesso,
  - 🔴 di divieto,
  - 🟠 di reindirizzamento,
  - ○ nessuna regola impostata.

Premere la riga di una connessione per passare alla schermata Connessione.

Scheda Tutte le applicazioni

È possibile visualizzare informazioni sul traffico internet utilizzato dalle applicazioni installate sul dispositivo, nonché configurare per esse le regole di accesso a risorse di rete sulla scheda **Tutte le applicazioni**.

Sulla scheda **Tutte le applicazioni** è visualizzata la quantità totale di dati trasmessi via rete, nonché la quantità di traffico ricevuto e inviato. È possibile visualizzare la lista delle applicazioni (gruppi di applicazioni) per ciascuna di cui è indicata la quantità di traffico internet consumato.

Per ciascuna applicazione sulla scheda **Tutte le applicazioni** vengono visualizzate le seguenti informazioni:

- Quantità complessiva di traffico in entrata e in uscita sulle connessioni stabilite.
- Accesso al trasferimento dati via Wi-Fi.
- Presenza di impostazioni utente. Le applicazioni con accesso a trasferimento dati modificato sono contrassegnate dal badge .

Filtraggio e ordinamento delle applicazioni

Per filtrare od ordinare la lista delle applicazioni, premere l'icona nell'angolo superiore destro dello schermo e selezionare i parametri di filtraggio od ordinamento richiesti:

- Visualizzare le applicazioni con traffico zero.
- Ordinare:
  - traffico decrescente — le applicazioni con il maggior traffico in cima alla lista;
  - traffico crescente — le applicazioni con il minor traffico in cima alla lista;
  - in ordine alfabetico dalla A alla Z;
  - in ordine alfabetico dalla Z alla A.

Di default le applicazioni sono ordinate per traffico decrescente (le applicazioni con il maggior traffico si trovano in cima alla lista), le applicazioni con traffico zero sono visualizzate. Per ripristinare la vista della lista applicazioni di default, premere **Resetta** sulla schermata **Filtro**.

Ricerca

Per passare rapidamente a un'applicazione richiesta, utilizzare la ricerca per nome di applicazione. Per fare ciò, premere l'icona nella parte sinistra dello schermo e inserire la richiesta nel campo di ricerca.

Impostazioni

Per configurare le impostazioni per tutte le applicazioni, sulla schermata **Traffico** premere nell'angolo superiore destro dello schermo.

Sono disponibili le seguenti impostazioni:

- **Utilizza protocollo IPv6**. Consente di attivare o disattivare l'utilizzo del protocollo IPv6 in parallelo a IPv4.
- **Consenti protocollo DNS sopra TCP**. Consente di attivare o disattivare l'utilizzo del protocollo DNS sopra TCP per il reindirizzamento di richieste DNS e l'occultamento di nomi a dominio.

L'utilizzo del protocollo DNS sopra TCP può ostacolare la visualizzazione di nomi a dominio sulle schermate Firewall.

L'impostazione funziona su dispositivi che supportano questo tipo di protocollo. Di default l'impostazione è disattivata.

- **Vieta connessioni per nuove applicazioni**. Consente di vietare l'accesso alla rete per le applicazioni che vengono installate dopo l'attivazione dell'impostazione. L'impostazione è attiva di default.
- **Vieta connessioni per tutte le applicazioni**. Consente di vietare l'accesso alla rete per tutte le applicazioni installate sul dispositivo. Se l'accesso alla rete verrà concesso a una delle applicazioni, l'impostazione verrà disattivata.
- **Conserva regole e statistiche dopo la rimozione di applicazioni**. Consente di conservare i dati di un'applicazione rimossa dal dispositivo per il periodo di tempo selezionato: una settimana, un mese o un anno.

Rimozione delle statistiche, impostazioni e regole per applicazioni

Per rimuovere le statistiche, le impostazioni e le regole per tutte le applicazioni

1. Sulla schermata **Traffico** premere nell'angolo superiore destro dello schermo.
2. Spuntare il flag di fronte all'opzione richiesta e premere **Cancella**.

11.3.2. Elaborazione del traffico delle applicazioni su Android TV

Firewall Dr.Web consente di configurare l'elaborazione del traffico internet a livello di applicazioni e in questo modo controllare l'accesso di programmi e processi a risorse di rete. È possibile visualizzare informazioni sul traffico internet utilizzato da un'applicazione installata sul dispositivo, nonché configurare per essa le regole di accesso a risorse di rete sulla schermata dell'applicazione (vedi Immagine 40).

Sulla schermata sono disponibili due schede:

- Sulla scheda Statistiche è possibile visualizzare statistiche di utilizzo del traffico internet, nonché modificare le impostazioni individuali dell'applicazione.
- Sulla scheda Regole è possibile gestire le regole delle connessioni avviate dall'applicazione.

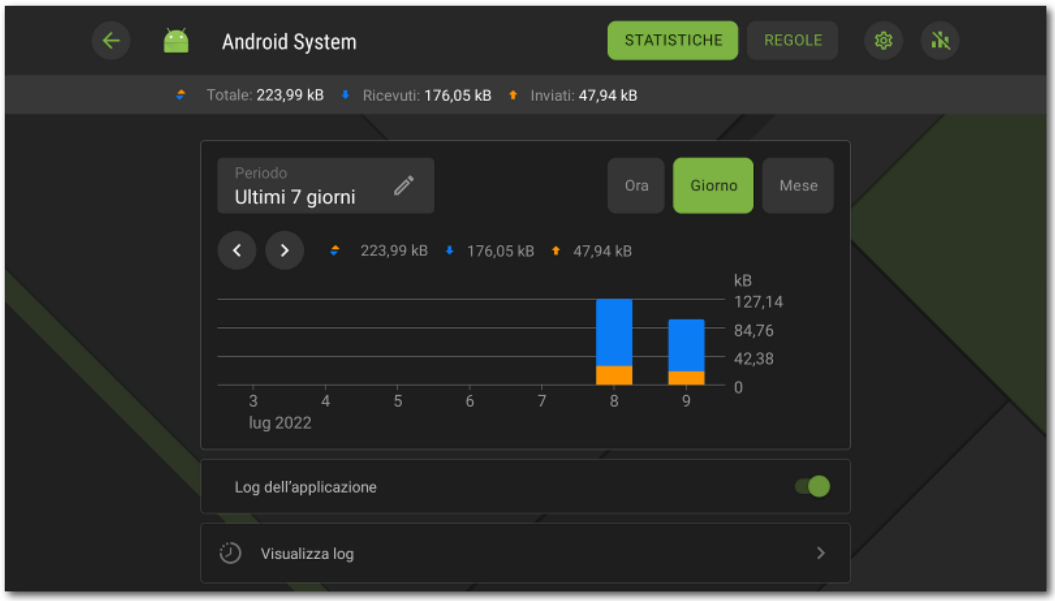

Immagine 40. Schermata di un'applicazione

Gruppo di applicazioni

Alcune applicazioni di servizio possono essere unite in un gruppo di applicazioni. Per visualizzare la lista delle applicazioni incluse nel gruppo, sulla schermata dell'applicazione premere il contatore a destra dell'intestazione **Gruppo di applicazioni**.

11.3.2.1. Statistiche e impostazioni di un'applicazione su Android TV

Sulla scheda **Statistiche** della schermata con informazioni dettagliate sul traffico di un'applicazione (gruppo di applicazioni) è possibile visualizzare le statistiche sull'utilizzo di internet da questa applicazione sotto forma di un diagramma (vedi Immagine 41), e inoltre, modificare le impostazioni di Firewall per questa applicazione.

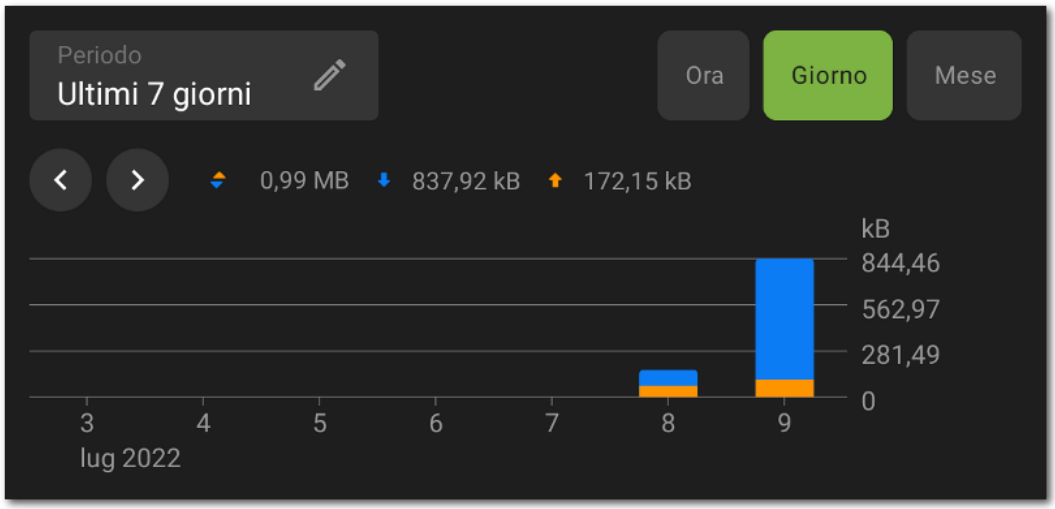

Immagine 41. Statistiche sull'uso del traffico internet

Statistiche di utilizzo del traffico internet

Sul diagramma il traffico in uscita è contrassegnato in arancione e quello in entrata in blu. Sopra il diagramma sono riportati i valori numerici del traffico consumato (totale, in uscita e in entrata).

Visualizzando le statistiche di utilizzo del traffico internet, è possibile eseguire le seguenti azioni:

- Selezionare il periodo di tempo per la visualizzazione delle statistiche nel campo corrispondente sopra il diagramma. È possibile visualizzare le statistiche per il giorno corrente, gli ultimi 7 giorni, il mese corrente, il mese precedente o impostare in autonomo un periodo di tempo indicando le date di inizio e di fine.
- Configurare nei limiti del periodo selezionato la visualizzazione delle statistiche per ora, giorno o mese tramite le opzioni sopra il diagramma.

Rimozione delle statistiche

- Rimozione delle statistiche per tutte le applicazioni:
  1. Sulla schermata **Firewall** selezionare **Traffico**.
  2. Sulla schermata **Traffico** premere nell'angolo superiore destro.
  3. Spuntare il flag **Statistiche delle applicazioni** e premere **Cancella**.
- Rimozione delle statistiche per una singola applicazione:
  1. Sulla schermata **Traffico** selezionare l'applicazione per cui si vogliono cancellare le statistiche.
  2. Sulla schermata dell'applicazione premere nell'angolo superiore destro.
  3. Spuntare il flag **Statistiche dell'applicazione** e premere **Cancella**.

Dopo la rimozione di un'applicazione dal dispositivo, le statistiche dell'applicazione verranno rimosse automaticamente entro 5 minuti.

Log dell'applicazione

Gli eventi relativi all'attività di rete delle applicazioni installate sul dispositivo vengono registrati nei log delle applicazioni. Utilizzare l'interruttore per iniziare o riprendere la registrazione del log dell'applicazione. Per passare al log, premere **Visualizza log**.

Impostazioni dell'applicazione

Per passare alle impostazioni di un'applicazione (gruppo di applicazioni), sulla scheda **Statistiche** premere nell'angolo superiore destro dello schermo (vedi Immagine 40).

Accesso al trasferimento dati via Wi-Fi

Utilizzare l'interruttore per vietare o consentire il trasferimento dati via Wi-Fi per questa applicazione. Di default l'accesso è consentito. L'indicatore di accesso viene visualizzato a destra nella riga dell'applicazione sulla schermata **Traffico** (indicatore verde — accesso consentito, quello grigio — accesso vietato).

Blocca tutte le connessioni eccetto quelle consentite dalle regole

Per vietare di default tutte le connessioni per un'applicazione, utilizzare l'interruttore **Blocca tutte le connessioni eccetto quelle consentite dalle regole**. Se non verranno impostate regole di permesso per l'applicazione, l'applicazione non potrà stabilire alcuna connessione.

Con l'attivazione dell'impostazione **Blocca tutte le connessioni eccetto quelle consentite dalle regole** per l'applicazione verrà automaticamente aggiunta una regola di permesso per la porta 53. La presenza della regola (per i protocolli DNS, UDP o ALL) è obbligatoria per il funzionamento delle regole di permesso con nomi a dominio.

Per il corretto funzionamento dell'impostazione in presenza delle regole di permesso con nomi a dominio, è inoltre necessario disattivare l'utilizzo del server DNS privato nelle impostazioni del dispositivo.

Non controllare l'applicazione

L'impostazione non è disponibile per alcune applicazioni di sistema.

Firewall Dr.Web è implementato sulla base di VPN per Android. La VPN ostacola il funzionamento delle applicazioni che utilizzano una tecnologia incompatibile con VPN, per esempio, Wi-Fi Direct. Ciò può portare all'impossibilità di connessione del dispositivo ad altri dispositivi. In questo caso, non è consigliabile disattivare completamente Firewall Dr.Web. Disattivare invece il controllo Firewall Dr.Web per l'applicazione (gruppo di applicazioni) richiesta. Per fare ciò, utilizzare l'interruttore **Non controllare l'applicazione**.

Si consiglia di disattivare il controllo di Firewall Dr.Web solo per le applicazioni di cui ci si fida.

Se questa opzione è attivata, Firewall Dr.Web non controlla le connessioni di rete di questa applicazione, anche se nelle impostazioni di Firewall Dr.Web sono impostate limitazioni. Il traffico dell'applicazione non viene calcolato.

11.3.2.2. Regole delle connessioni su Android TV

Il traffico delle applicazioni viene gestito a livello di connessioni che vengono stabilite dalle applicazioni. È possibile impostare le regole di permesso, di divieto e di reindirizzamento per le connessioni a indirizzi IP e porte specifici per ciascuna applicazione installata sul dispositivo.

Connessioni

Le informazioni generali su ciascuna connessione sono presentate sulla schermata **Connessione** (v. Immagine 42). Per passare a questa schermata, eseguire una delle seguenti azioni:

- Sulla scheda Applicazioni attive della schermata **Traffico** premere l'icona ⌄ a sinistra del nome di un'applicazione e quindi premere la riga di una connessione.
- Nel log di Firewall:
  - In modalità di raggruppamento per data: premere la riga di una connessione.
  - In modalità di raggruppamento per nome di applicazione: espandere la lista delle connessioni di un'applicazione tramite l'icona ⌄ a sinistra del nome dell'applicazione e quindi premere la riga di una connessione.
- Nel log di un'applicazione espandere la lista delle connessioni tramite l'icona ⌄ a destra della data di un evento e quindi premere la riga di una connessione.

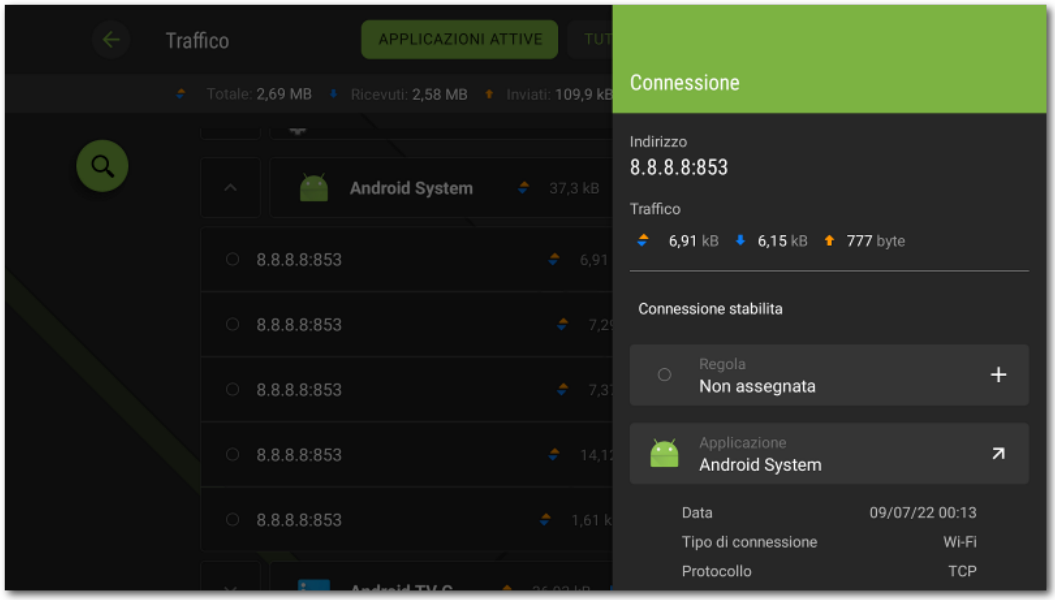

Immagine 42. Schermata Connessione

Sulla schermata **Connessione** sono disponibili le seguenti informazioni:

- indirizzo e porta della connessione;
- nome dell'host (se disponibile);
- quantità di traffico in entrata e in uscita ricevuto o trasmesso dalla connessione;
- stato della connessione;
- regola della connessione;
- applicazione che ha stabilito la connessione;
- data e ora;
- tipo di connessione;
- protocollo.

Le regole delle connessioni sono disponibili sulla scheda Regole della schermata di un'applicazione.

Regole delle connessioni

Creazione delle regole

Per creare una nuova regola per una connessione

1. Per una connessione senza regole:
   - Sulla schermata **Connessione** premere l'icona + a destra della voce **Regola**.

Per qualsiasi connessione:

- Sulla schermata di un'applicazione sulla scheda **Regole** premere l'icona  nella parte sinistra dello schermo.

2. Nella finestra che si è aperta selezionare il tipo di regola:
   - 🟢 di permesso,
   - 🔴 di divieto,
   - 🟠 di reindirizzamento.
3. Verificare la correttezza dell'indirizzo IP/nome host. Se nessun indirizzo è indicato, indicare un indirizzo IP valido (in formato a.b.c.d per indirizzi IPv4 o [a:b:c:d:e:f:g:h] per indirizzi IPv6), un intervallo di indirizzi IP (in formato a1.b1.c1.d1-a2.b2.c2.d2 o [a1:b1:c1:d1:e1:f1:g1:h1]-[a2:b2:c2:d2:e2:f2:g2:h2]) o una rete intera (in formato a.b.c.0/n, dove n è un numero compreso tra 1 e 32). Se viene creata una regola di reindirizzamento, indicare l'indirizzo di reindirizzamento nel campo sottostante. Invece di un indirizzo, è possibile indicare un nome host.
4. Premere **Altri parametri** per configurare l'impostazione aggiuntiva **Protocollo** — protocollo di rete per la connessione.
5. Premere **Salva**.

Le applicazioni con regole delle connessioni impostate sono contrassegnate dal badge ⚙.

Visualizzazione delle regole

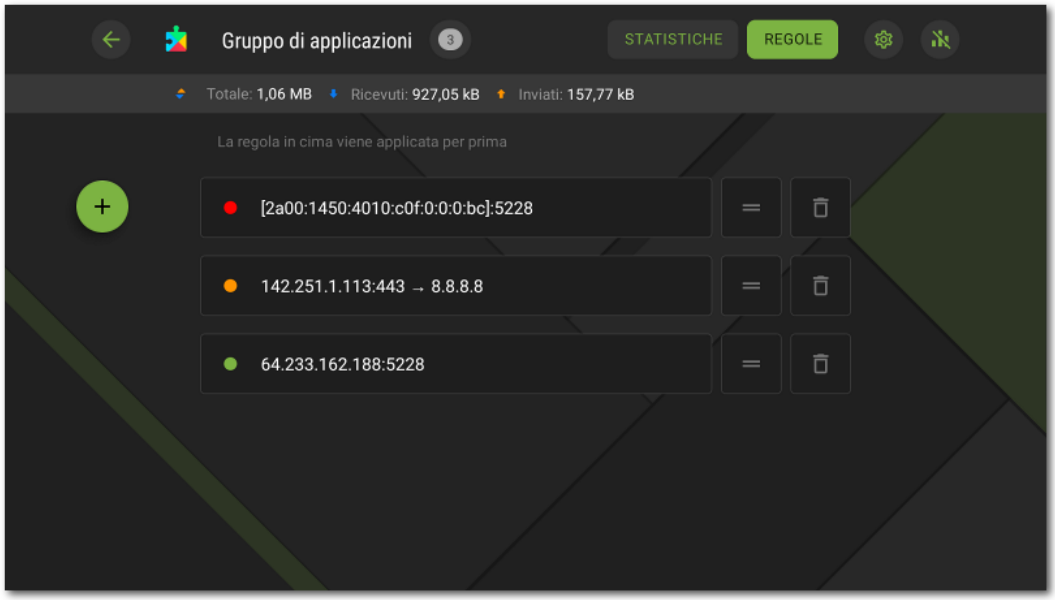

Immagine 43. Scheda Regole

Per vedere le regole delle connessioni di un'applicazione

- Aprire la schermata di un'applicazione e passare alla scheda **Regole** (v. Immagine 43).

La scheda contiene la lista di tutte le regole impostate per tale applicazione nell'ordine in cui sono applicate.

Per modificare l'ordine di applicazione delle regole

- Premere e tenere premuta l'icona ═ di fronte alla regola che si vuole spostare, e trascinare la regola nella posizione desiderata nella lista.

Modifica delle regole

Per modificare una regola esistente

1. Eseguire una delle seguenti azioni:
   - Sulla schermata **Connessione** premere l'icona ✎ a destra della regola.
   - Sulla schermata di un'applicazione sulla scheda **Regole** premere la riga di una regola.
2. Apportare le modifiche richieste.
3. Premere **Salva**.

Rimozione delle regole

Per rimuovere una regola

- Sulla schermata di modifica della regola:
  1. Premere **Rimuovi regola**.
  2. Nella finestra che si è aperta premere **Elimina**.
- Sulla scheda **Regole** della schermata di un'applicazione:
  1. Premere l'icona a destra di una regola.
  2. Nella finestra che si è aperta premere **Elimina**.

Per rimuovere tutte le regole per una determinata applicazione

1. Sulla schermata di un'applicazione sulla scheda **Regole** premere l'icona nell'angolo superiore destro dello schermo.
2. Nella finestra che si è aperta spuntare il flag **Regole per l'applicazione** e premere **Cancella**.

Per rimuovere tutte le regole per tutte le applicazioni

1. Sulla schermata **Firewall** selezionare **Traffico**.
2. Sulla schermata **Traffico** premere l'icona nell'angolo superiore destro dello schermo.
3. Nella finestra che si è aperta spuntare il flag **Impostazioni e regole per le applicazioni** e premere **Cancella**.

Blocca tutte le connessioni eccetto quelle consentite dalle regole

È possibile vietare tutte le connessioni di un'applicazione, eccetto quelle consentite dalle regole, tramite l'interruttore corrispondente sulla schermata delle impostazioni dell'applicazione.

11.3.2.3. Log di un'applicazione su Android TV

I log delle applicazioni contengono una lista di eventi relativi alle connessioni di rete di una determinata applicazione installata sul dispositivo.

Per attivare la registrazione del log di un'applicazione

1. Sulla schermata **Traffico** selezionare l'applicazione richiesta.
2. Sulla schermata dell'applicazione utilizzare l'interruttore **Log dell'applicazione**.

Per aprire il log di un'applicazione

1. Sulla scheda **Traffico** selezionare nella lista l'applicazione richiesta.
2. Sulla schermata dell'applicazione premere **Visualizza log**.

Visualizzazione del log di un'applicazione

Tutti gli eventi dell'applicazione sono raggruppati per data. Per visualizzare la lista degli eventi per una determinata data, selezionare una data nella lista.

Per ciascun evento vengono visualizzate le seguenti informazioni:

- indirizzo e porta della connessione;
- traffico consumato;
- presenza per la connessione di una regola:
  - 🟢 di permesso,
  - 🔴 di divieto,
  - 🟠 di reindirizzamento,
  - ○ nessuna regola impostata.

Premere la riga di una connessione per passare alla schermata Connessione e configurare regole per essa.

Per ripulire il log di un'applicazione

1. Sulla schermata **Log dell'applicazione** premere l'icona nell'angolo superiore destro dello schermo.
2. Premere **Cancella**.

Per disattivare la registrazione del log di un'applicazione

1. Sulla schermata **Traffico** selezionare l'applicazione richiesta.
2. Sulla schermata dell'applicazione utilizzare l'interruttore **Log dell'applicazione**.

11.3.3. Log di Firewall Dr.Web su Android TV

Per visualizzare la lista di tutti gli eventi relativi al funzionamento di Firewall Dr.Web, sulla schermata **Firewall** selezionare **Log**.

Nel log di Firewall (vedi Immagine 44) vengono visualizzate le seguenti informazioni sull'evento:

- nome dell'applicazione;

- indirizzo e porta della connessione (nonché indirizzo di reindirizzamento, se è impostata la regola corrispondente);
- traffico consumato;
- data e ora dell'evento;
- presenza di una regola per la connessione.

Tramite il clic su un evento si apre la schermata Connessione.

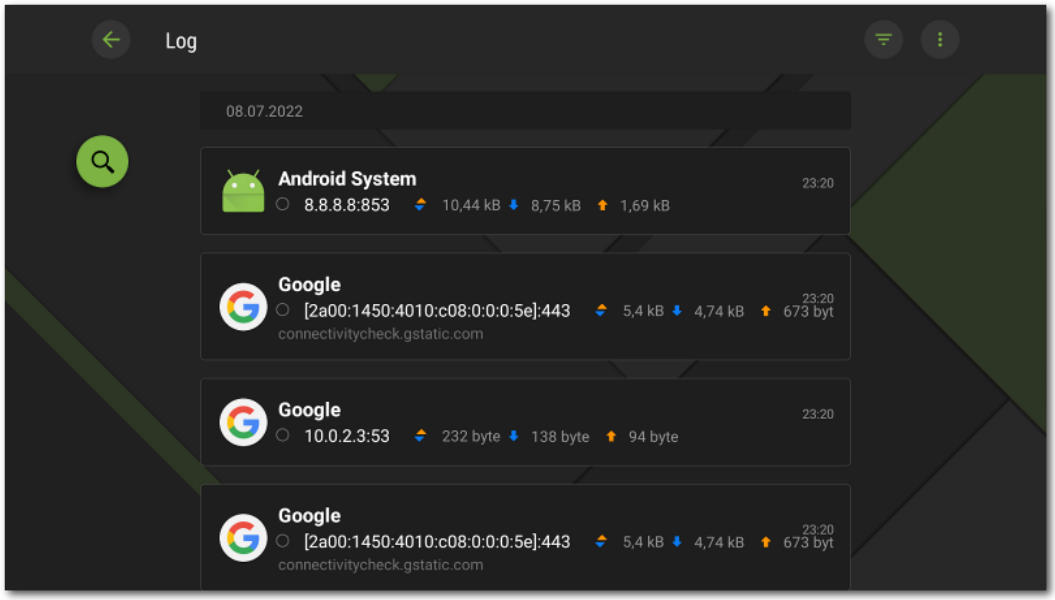

Immagine 44. Log di Firewall Dr.Web

Per filtrare od ordinare gli eventi nel log di Firewall

1. Premere l'icona nell'angolo superiore destro della schermata **Log**.
2. Selezionare i parametri di filtraggio od ordinamento richiesti:
   - Ordinare:
     - prima più recenti — gli ultimi eventi in cima al log;
     - prima meno recenti — gli ultimi eventi in fondo al log;
     - in ordine alfabetico dalla A alla Z;
     - in ordine alfabetico dalla Z alla A.
   - Visualizzare le connessioni:
     - stabilite,
     - resettate,
     - reindirizzate,
     - con errore.

Di default gli eventi sono ordinati per data (gli ultimi eventi si trovano in cima al log), tutti i tipi di connessioni sono visualizzati. Per ripristinare la vista del log di default, premere **Resetta** sulla schermata **Filtro**.

Per comodità di visualizzazione del log è anche possibile raggruppare gli eventi per applicazione.

Per raggruppare gli eventi per applicazione

- Sulla schermata **Log** premere ⋮ nell'angolo superiore destro e utilizzare l'interruttore **Raggruppa per nome dell'applicazione**.

Per eseguire una ricerca nel log di Firewall

- Premere l'icona  nella parte sinistra dello schermo e inserire la richiesta nel campo di ricerca.

Per ripulire il log di Firewall

1. Sulla schermata **Log** premere ⋮ nell'angolo superiore destro e selezionare l'opzione **Cancella il log**.
2. Confermare l'azione premendo il pulsante **Cancella**.

Dimensione del log

Di default per il file di log è impostata una dimensione pari a 5 MB.

Per modificare la dimensione massima consentita del file di log

1. Sulla schermata **Log** premere ⋮ nell'angolo superiore destro e selezionare l'opzione **Dimensione del log**.
2. Nella finestra che si è aperta modificare il valore e premere **Salva**.

La dimensione massima del log deve essere maggiore di 0 MB e minore o pari a 99 MB.

11.4. Auditor di sicurezza su Android TV

Dr.Web analizza la sicurezza del dispositivo e suggerisce come risolvere i problemi e le vulnerabilità individuati attraverso un componente specifico — Auditor di sicurezza. Il componente inizia a funzionare automaticamente dopo il primo avvio dell'applicazione e la registrazione della licenza.

Possibili problemi e modi per risolverli

Dr.Web rileva i seguenti problemi di sicurezza:

- Vulnerabilità
- Impostazioni di sistema, che influiscono sulla sicurezza del dispositivo.
- Amministratori del dispositivo nascosti
- Applicazioni che sfruttano la vulnerabilità Fake ID

Per aprire la lista dei problemi di sicurezza rilevati (v. Immagine 45), sulla schermata principale di Dr.Web selezionare **Auditor di sicurezza**.

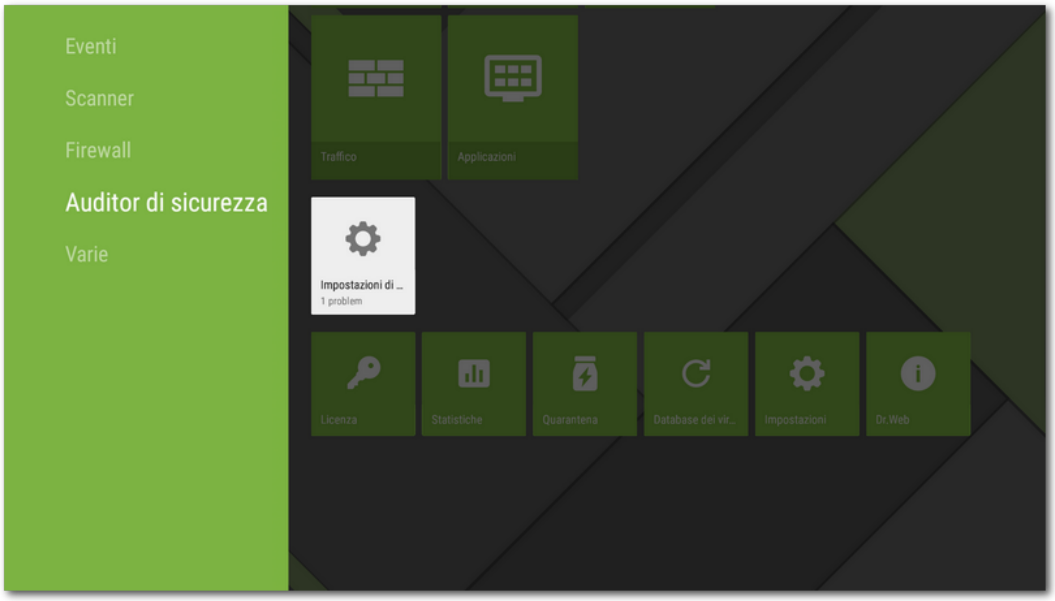

Immagine 45. Auditor di sicurezza

Vulnerabilità

Una *vulnerabilità* è un difetto nel codice software che può essere sfruttato dai malintenzionati per disturbare il funzionamento del sistema.

Auditor di sicurezza rileva nel sistema del dispositivo le seguenti vulnerabilità: BlueBorne, EvilParcel, Extra Field, Fake ID, Janus, ObjectInputStream Serialization, OpenSSLX509Certificate, PendingIntent, SIM Toolkit, Stagefright e Stagefright 2.0.

Utilizzando le vulnerabilità, i malintenzionati possono aggiungere un codice software alle applicazioni le quali di conseguenza possono iniziare a svolgere funzioni che rappresentano una minaccia per la sicurezza del dispositivo.

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 le falle potrebbero essere riparate. Se gli aggiornamenti non sono disponibili, è consigliabile installare applicazioni solo da fonti affidabili.

Permessi di root

Il dispositivo può diventare vulnerabile a diversi tipi di minacce se su di esso sono disponibili i permessi di root, cioè sono state apportate le modifiche volte ad ottenere i permessi di superutente (root). Questo permette di modificare e rimuovere i file di sistema, il che può portare all'inoperatività del dispositivo. Se queste modifiche sono state apportate 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 svolgere qualche attività, è consigliabile essere particolarmente attenti, installando applicazioni da fonti sconosciute.

Impostazioni di sistema

Auditor di sicurezza rileva le seguenti impostazioni di sistema che influiscono sulla sicurezza del dispositivo:

- **Debugging permesso**. Il debug tramite USB è progettato per sviluppatori e consente di copiare dati da un computer su un dispositivo con Android e viceversa, installare applicazioni sul dispositivo, visualizzare dati dei log delle applicazioni installate e inoltre rimuoverli in alcuni casi. Se non si è sviluppatori e non si usa la modalità di debug, è consigliabile disattivarla. Per passare alla sezione corrispondente delle impostazioni di sistema, selezionare **Impostazioni** sulla schermata con informazioni dettagliate su questo problema.
- **Installazione da sorgenti sconosciute permessa**. L'installazione di applicazioni da sorgenti sconosciute è la principale causa di diffusione delle minacce ai dispositivi Android. Le applicazioni scaricate da una sorgente diversa dalla directory delle applicazioni ufficiale con un'elevata probabilità possono rivelarsi pericolose e arrecare danno al dispositivo. Per ridurre il rischio di installazione di applicazioni non sicure, è consigliabile vietare l'installazione di applicazioni da sorgenti sconosciute. Per passare alla sezione corrispondente delle impostazioni di sistema, selezionare **Impostazioni** sulla schermata con informazioni dettagliate su questo problema. Inoltre, è consigliabile verificare la presenza di minacce in tutte le applicazioni che si vogliono installare. Prima di eseguire una verifica, è necessario assicurarsi che i database dei virus Dr.Web siano aggiornati.
- **Avvisi Dr.Web bloccati**. In questo caso Dr.Web non può informare prontamente di minacce rilevate. Questo riduce la sicurezza del dispositivo e può portare all'infezione. Pertanto, è consigliabile passare alle impostazioni del dispositivo e attivare gli avvisi Dr.Web.
- **Installato un certificato radice personalizzato**. Se sul dispositivo sono stati rilevati certificati personalizzati, le relative informazioni verranno visualizzate in Auditor di sicurezza. A causa di certificati personalizzati installati, terze parti possono visualizzare le attività di rete dell'utente. Se non si conosce lo scopo dei certificati rilevati, è consigliato rimuoverli dal dispositivo.

Amministratori del dispositivo nascosti

Le applicazioni che sono attivate come amministratori del dispositivo, ma sono assenti dalla lista amministratori nella sezione corrispondente delle impostazioni del dispositivo non possono essere rimosse con strumenti standard del sistema operativo. Con grande probabilità tali applicazioni non sono sicure.

Se non si sa perché un'applicazione nasconde la sua presenza nella lista degli amministratori del dispositivo, è consigliato rimuoverla. Per rimuovere un'applicazione, selezionare **Elimina** sulla schermata con informazioni dettagliate sul problema relativo a questa applicazione.

Applicazioni che sfruttano la vulnerabilità Fake ID

Se sul dispositivo sono state rilevate applicazioni che utilizzano la vulnerabilità Fake ID, esse verranno visualizzate in una categoria separata di Auditor di sicurezza. Queste applicazioni possono essere malevole, quindi è consigliabile rimuoverle. Per rimuovere un'applicazione, selezionare **Elimina** sulla schermata con informazioni dettagliate sul problema relativo a questa applicazione o utilizzare gli strumenti del sistema operativo.

11.5. Varie

La sezione **Varie** (vedi Immagine 46) consente di passare alle impostazioni dell'applicazione, accedere alla quarantena e alle statistiche. È possibile ottenere informazioni sulla versione dell'applicazione, sulla licenza e sulle date di attivazione e scadenza. Inoltre, è possibile visualizzare la data dell'ultimo aggiornamento dei database dei virus ed eseguire un aggiornamento manualmente.

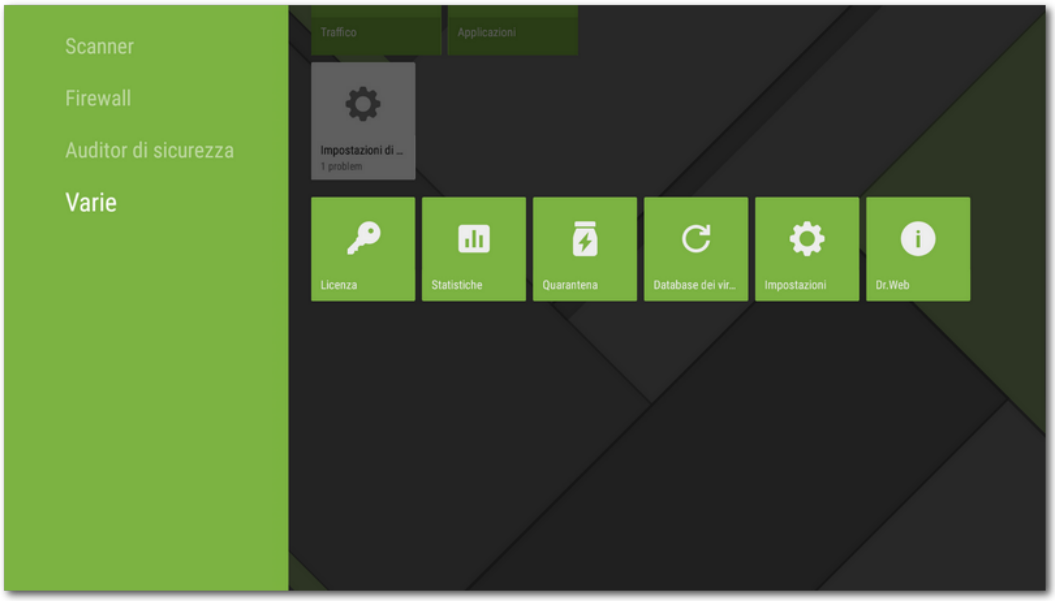

Immagine 46. Varie

Licenza

È possibile visualizzare le date di registrazione e di scadenza della licenza.

Da questa finestra è inoltre possibile acquistare e attivare una nuova licenza.

Statistiche

La sezione **Statistiche** consente di visualizzare informazioni circa i risultati di una verifica tramite Scanner Dr.Web, l'attivazione/la disattivazione del componente SpIDer Guard, le minacce rilevate e le azioni eseguite per neutralizzarle (vedi sezione Statistiche).

Quarantena

Quarantena — una cartella specifica progettata per l'isolamento e l'archiviazione sicura delle minacce rilevate (vedi sezione Quarantena).

Database dei virus

Per rilevare le minacce alla sicurezza, Dr.Web utilizza database dei virus speciali che contengono informazioni su tutte le minacce informatiche per dispositivi con sistema operativo Android, conosciute dagli specialisti Doctor Web. I database dei virus richiedono un aggiornamento periodico in quanto nuovi programmi malevoli compaiono regolarmente. A tale scopo nell'applicazione è implementata la possibilità di aggiornamento dei database dei virus via internet.

Aggiornamento

Per scoprire se è necessario aggiornare manualmente i database dei virus:

1. Aprire la sezione **Database dei virus**.
2. Nella finestra che si è aperta si vedono lo stato dei database dei virus e la data dell'ultimo aggiornamento.

   Se i database dei virus sono obsoleti, è necessario eseguire un aggiornamento manualmente. Per fare ciò, selezionare **Aggiorna** sulla barra a destra.

Subito dopo aver installato l'applicazione, è consigliabile aggiornare i database dei virus in modo che Dr.Web possa utilizzare le più recenti informazioni sulle minacce conosciute. Le firme antivirali dei virus, le informazioni sulle loro caratteristiche e sui loro modelli di comportamento vengono aggiornate non appena gli specialisti del laboratorio antivirus Doctor Web rilevano nuove minacce, talvolta fino a diverse volte all'ora.

Impostazioni

La sezione **Impostazioni** consente di configurare i componenti di protezione antivirus, definire le impostazioni generali dell'applicazione, attivare e disattivare la funzione di invio delle statistiche e ripristinare le impostazioni dell'applicazione alle impostazioni predefinite (vedi sezione Impostazioni Dr.Web su Android TV).

Dr.Web

Sulla schermata **Dr.Web** è possibile visualizzare la versione dell'applicazione. Su questa schermata sono inoltre disponibili i link del sito ufficiale dell'azienda Doctor Web.

11.5.1. Impostazioni Dr.Web su Android TV

Impostazioni generali

- **Suono** permette di configurare gli avvisi sonori per segnalare che una minaccia è stata rilevata, rimossa o messa in quarantena. Di default gli avvisi sonori sono attivati.
- **Invio delle statistiche** permette di attivare o disattivare l'invio di statistiche all'azienda Doctor Web.
- **Opzioni avanzate** contiene le seguenti impostazioni aggiuntive:
  - **Applicazioni di sistema** permette di attivare o disattivare l'avviso sulle minacce nelle applicazioni di sistema che non possono essere rimosse senza compromettere l'operatività del dispositivo. Di default questa opzione è disattivata.

SpIDer Guard

- **File in archivi** permette di attivare il controllo di file in archivi compressi.

Di default il controllo di archivi è disattivato. L'attivazione del controllo di archivi può influire sulle prestazioni del sistema. La disattivazione del controllo di archivi non influisce sul livello di protezione in quanto SpIDer Guard controlla i file APK di installazione indipendentemente dal valore impostato del parametro **File in archivi**.

- **Scheda SD incorporata e supporti rimovibili** permette di attivare la verifica della scheda SD incorporata e di supporti rimovibili ad ogni collegamento. Se questa impostazione è attivata, la verifica viene avviata ogni volta che il componente SpIDer Guard viene attivato.
- **Area di sistema** permette di tenere traccia di modifiche nell'area di sistema. Se questa impostazione è attivata, SpIDer Guard tiene traccia di modifiche (aggiunta, modifica e rimozione di file) e informa sulla rimozione di qualsiasi file, nonché sull'aggiunta e la modifica di file eseguibili: `.jar`, `.odex`, `.so`, file di formato APK, ELF ecc.

- **Controllo ripetuto dell'area di sistema** permette di avviare un nuovo controllo dell'area di sistema. SpIDer Guard ricontrollerà tutte le minacce nell'area di sistema che precedentemente sono state ignorate.
- **Avvisi dell'area di sistema** permette di attivare gli avvisi sulla modifica a qualsiasi file (non solo a un file eseguibile) nell'area di sistema.
- **Opzioni avanzate** permette di attivare e disattivare il controllo della presenza nel sistema di adware e riskware (compresi gli hacktool e joke).

Scanner

- **File in archivi** permette di attivare il controllo di file in archivi compressi.

Di default il controllo di archivi è disattivato. L'attivazione del controllo di archivi può influire sulle prestazioni del sistema. La disattivazione del controllo di archivi non influisce sul livello di protezione in quanto Scanner Dr.Web controlla i file di installazione `.apk` indipendentemente dal valore impostato del parametro **File in archivi**.

- **Opzioni avanzate** permette di attivare e disattivare il controllo della presenza nel sistema di adware e riskware (compresi gli hacktool e joke).

Ancora

- **Reset delle impostazioni** permette di resettare in qualsiasi momento le impostazioni personalizzate dell'applicazione e di ripristinare le impostazioni predefinite.
- **Nuova versione** (l'opzione è disponibile per la versione installata dal sito dell'azienda Doctor Web) permette di impostare la verifica della disponibilità di una nuova versione a ogni aggiornamento dei database dei virus dell'applicazione. Quando compare una nuova versione dell'applicazione, si riceverà un avviso standard e si potrà scaricare e installare prontamente la nuova versione.

12. Supporto tecnico

Se si riscontrano problemi con l'installazione o il funzionamento dei prodotti della società, prima di contattare per l'assistenza il servizio di supporto tecnico, provare a trovare una soluzione nei seguenti modi:

1. Leggere le ultime versioni delle descrizioni e dei manuali sull'indirizzo https://download.drweb.com/doc/.
2. Leggere la sezione delle domande ricorrenti sull'indirizzo https://support.drweb.com/show_faq/.
3. Visitare i forum della società Doctor Web sull'indirizzo https://forum.drweb.com/.

Se provati questi modi, non si è riusciti a risolvere il problema, è possibile utilizzare uno dei seguenti modi per contattare il servizio di supporto tecnico della società Doctor Web:

1. Compilare il modulo web nella relativa sezione della pagina https://support.drweb.com/.
2. Chiamare il numero +7 (495) 789-45-86 o 8-800-333-7932 (numero gratuito per utenti in Russia).

Le informazioni sulle rappresentanze regionali e sedi della società Doctor Web sono ritrovabili sul sito ufficiale sull'indirizzo https://company.drweb.com/contacts/offices/.

13. Si è dimenticata la password?

Se si è dimenticata la password dell'account Dr.Web, resettarla e impostarne una nuova:

- Tramite email. Questo indirizzo email è stato indicato durante la creazione dell'account o la configurazione di Antifurto Dr.Web.
- Tramite SMS. Questa opzione è disponibile solo nella versione dell'applicazione dal sito se alla lista degli amici in Antifurto è aggiunto almeno un numero di telefono.
- Tramite l'avviso. Questa opzione è disponibile se almeno un amico ha confermato la richiesta di amicizia nell'applicazione Dr.Web Security Space.
- Facendo una richiesta al servizio di supporto tecnico. Il servizio di supporto tecnico potrà aiutare l'utente solo se si assicurerà che l'utente è il proprietario del dispositivo.

> ⚠ Se Dr.Web funziona in modalità di protezione centralizzata e Antifurto Dr.Web è configurato sul server, non sarà possibile impostare una nuova password nei modi indicati. In questo caso contattare l'amministratore della rete antivirus aziendale o il fornitore del servizio "Antivirus Dr.Web" e utilizzare un codice di ripristino di caratteri o QR.

Resettare la password tramite email

Nel pannello per il reset della password tramite email (vedi Immagine 47) sono indicati:

Chiave. Questa è una sequenza di caratteri univoca che è stata generata per l'account.

Indirizzo email. Questo indirizzo è stato utilizzato durante la creazione dell'account o la configurazione di Antifurto Dr.Web.

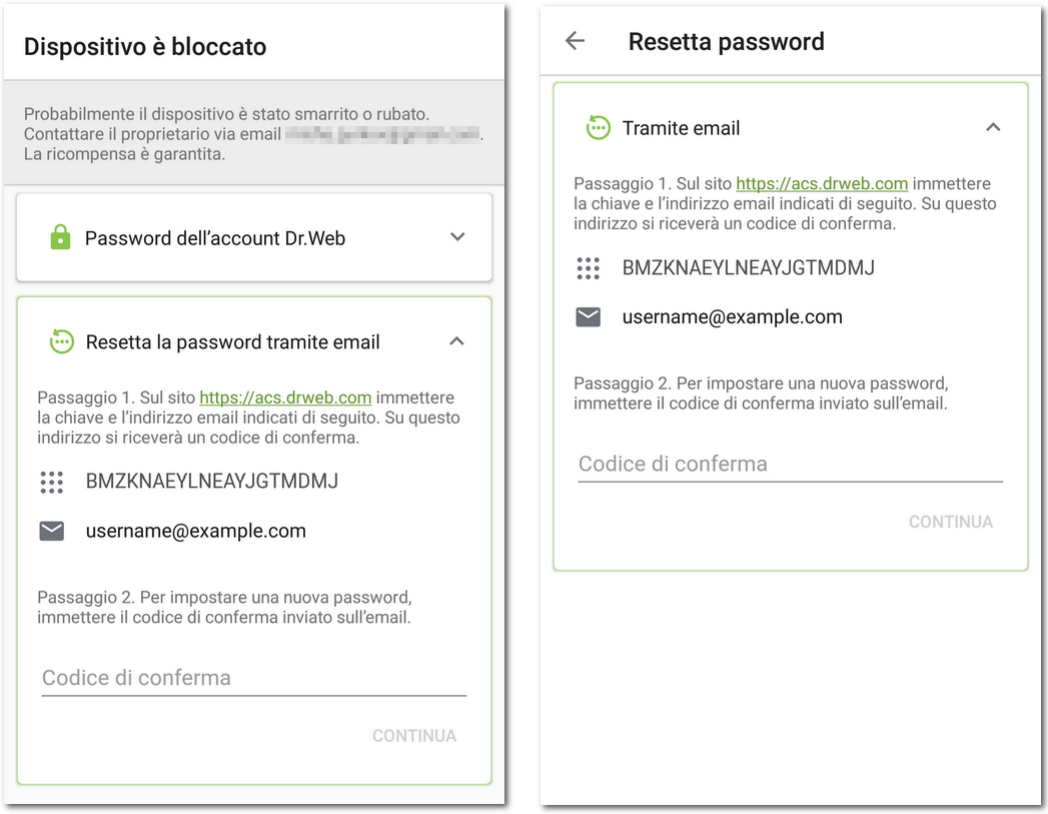

Immagine 47. Resettare la password tramite email

Dispositivo bloccato (a sinistra) e quello non bloccato (a destra)

Per resettare la password

1. Su un computer o qualsiasi altro dispositivo aprire la pagina web dell'account Dr.Web: https://acs.drweb.com (vedi Immagine 48).

> Se è installato Dr.Web 11.1.3 o versioni precedenti, per resettare la password, passare alla pagina di Antifurto Dr.Web https://antitheft.drweb.com/ o aggiornare l'applicazione alla versione 12.

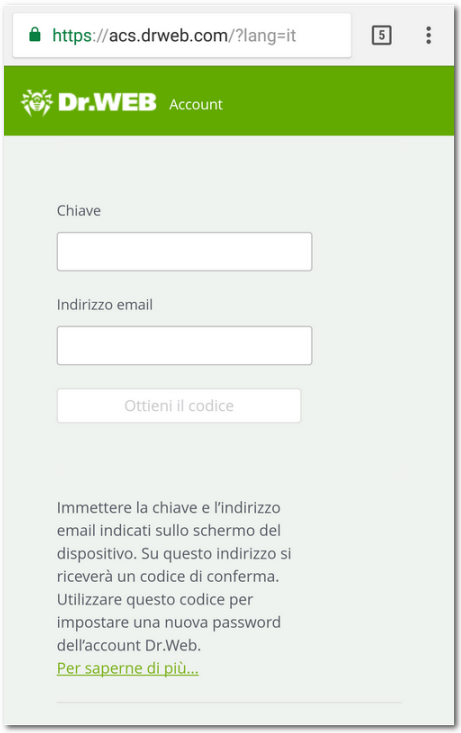

Immagine 48. Account Dr.Web

2. In questa pagina inserire la chiave e l'indirizzo email (vedi Immagine 49) indicati nell'applicazione Dr.Web.

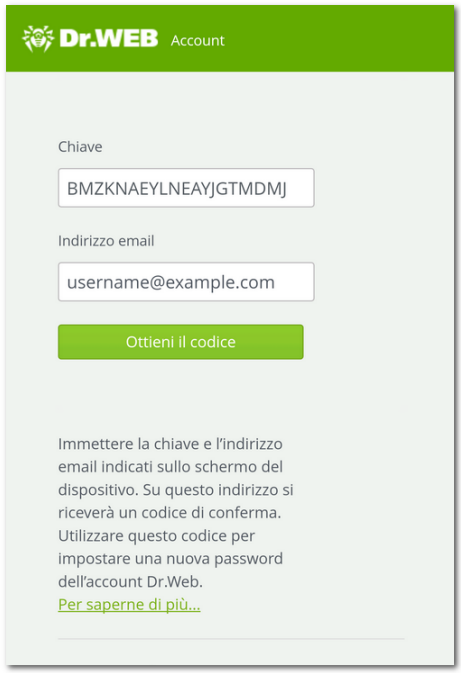

Immagine 49. Immissione della chiave e dell'indirizzo email

3. Premere il pulsante **Ottieni il codice**.

Se i dati sono stati inseriti correttamente, comparirà un messaggio che informa che all'indirizzo email è stata inviata un'email con un codice di conferma (vedi Immagine 50).

Se non si riceverà l'email entro 10 minuti:

1. Controllare la cartella Spam.
2. Provare a inserire nuovamente i dati. Probabilmente, è stata inserita una chiave sbagliata o è stato inserito un indirizzo email diverso da quello indicato nell'applicazione Dr.Web.
3. Se dopo queste azioni l'email non è stata ricevuta, contattare il servizio di supporto tecnico Doctor Web. Per farlo, premere **Non si è ricevuta l'email?** (vedi Immagine 50).

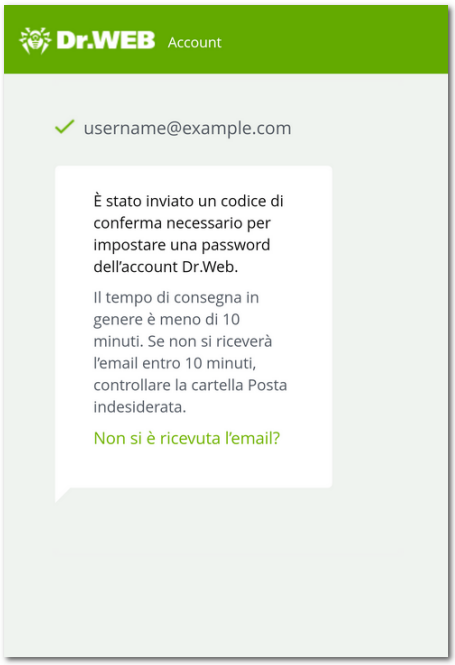

Immagine 50. Avviso sull'invio del codice di conferma

4. Aprire l'email arrivato dal servizio "Account Dr.Web". Nell'email è indicato un codice di conferma.

5. Nell'applicazione Dr.Web inserire il codice di conferma nel campo **Codice di conferma** (vedi Immagine 51).

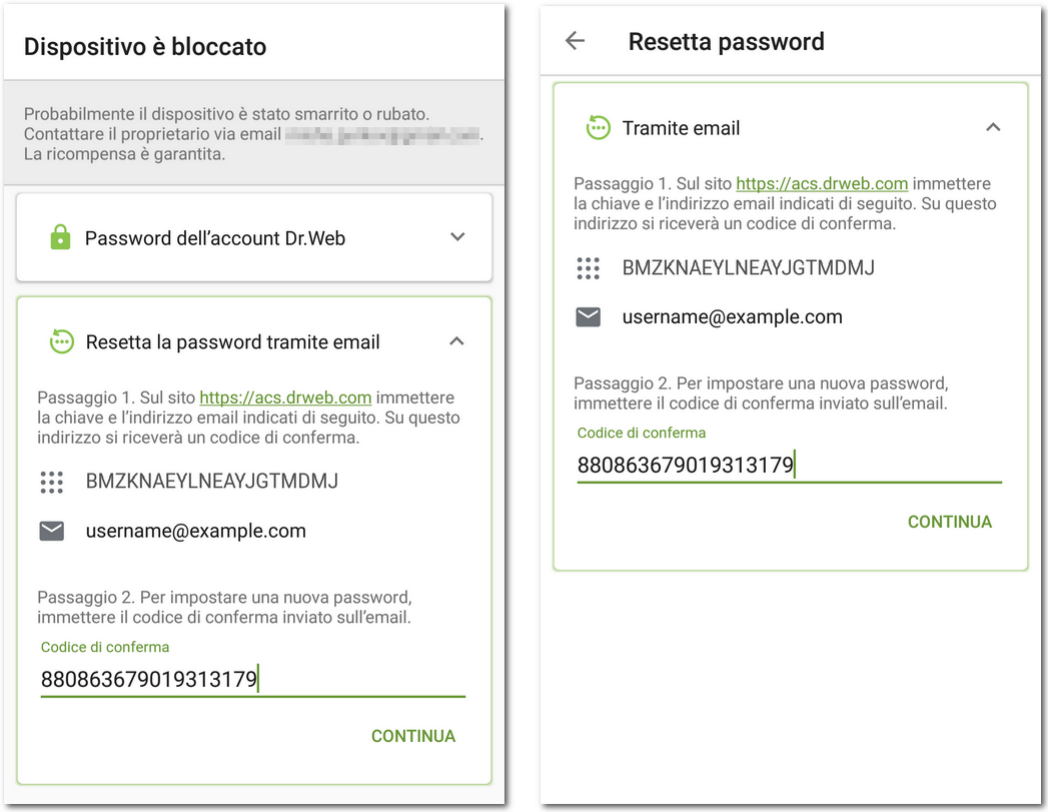

Immagine 51. Immissione del codice di conferma ricevuto via email

Dispositivo bloccato (a sinistra) e quello non bloccato (a destra)

6. Premere **Continua**.
7. Nella schermata **Cambia password** inserire una nuova password. La password deve contenere almeno 4 caratteri.

   Premere l'icona a destra del campo di immissione per visualizzare i caratteri che vengono digitati. Per nascondere i caratteri, premere l'icona .
8. Ripetere la password e premere **Salva**.

Resettare la password tramite un SMS dal numero di un amico

È possibile resettare la password con questo metodo se sono soddisfatte le seguenti condizioni:

1. Sul dispositivo è installata la versione dell'applicazione dal sito Doctor Web.
2. Il dispositivo è acceso e si trova nell'area di copertura della rete.
3. Sul dispositivo è attivato Antifurto Dr.Web.
4. Alla lista Mi fido di in Antifurto è aggiunto almeno un numero di telefono.
5. Il numero da cui verrà inviato il comando SMS è aggiunto alla lista Mi fido di.

6. Si conosce il numero telefonico della SIM utilizzata sul dispositivo. Il comando SMS può essere inviato solo a questo numero.

   Se non si conosce questo numero, inserire una SIM con un numero conosciuto.

> Se sul dispositivo si utilizzano due SIM alla volta, inviare il comando SMS a qualsiasi di questi numeri.

Per resettare la password

1. Inviare un SMS con il testo **#RESETPASSWORD#** al dispositivo dal numero di un amico.

   La lista dei numeri da cui è possibile inviare il comando SMS si trova sulla schermata **Dispositivo è bloccato** o **Resetta password** (vedi Immagine 52). Il comando SMS non fa distinzione tra maiuscole e minuscole.

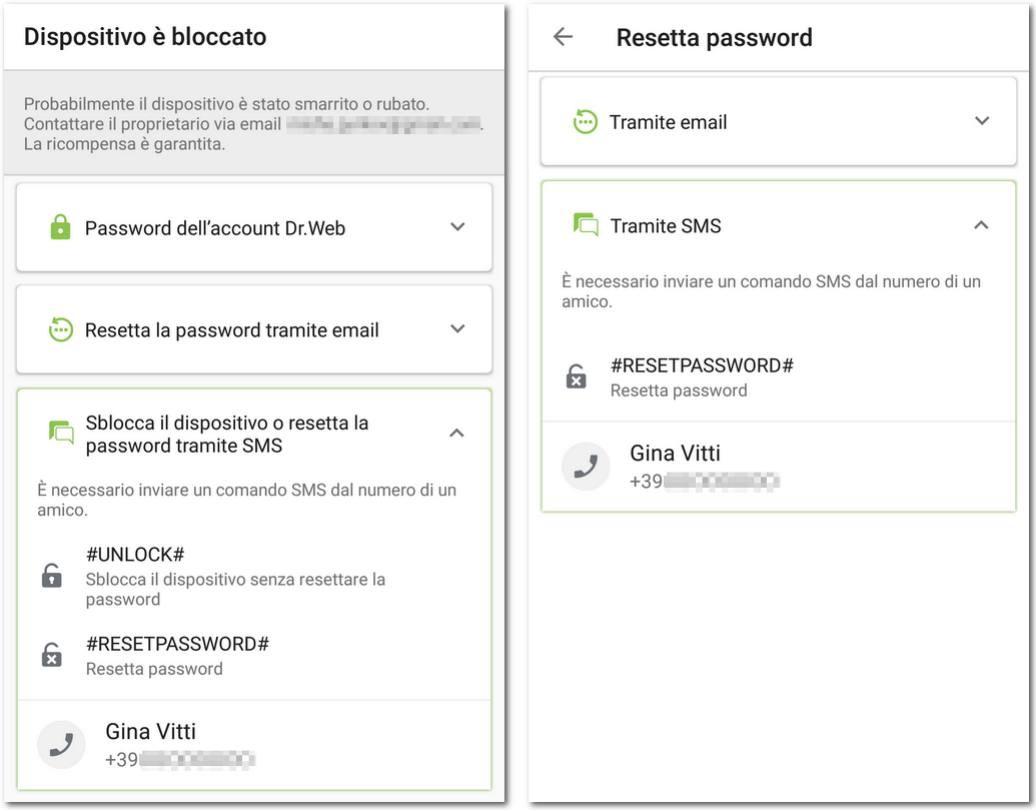

Immagine 52. Resettare la password tramite un SMS dal numero di un amico

Dispositivo bloccato (a sinistra) e quello non bloccato (a destra)

2. Dopo la ricezione dell'SMS sul dispositivo compare automaticamente la schermata **Cambia password**. Inserire una nuova password. Se il dispositivo era bloccato, esso viene sbloccato.

> Se il dispositivo è bloccato, è possibile sbloccarlo senza resettare la password. Per fare ciò, inviare al dispositivo il comando SMS **#UNLOCK#**.

Resettare la password tramite avviso

È possibile resettare la password tramite un avviso se sono soddisfatte le seguenti condizioni:

- **Per il dispositivo dell'utente**
  1. Il dispositivo è acceso ed è connesso a internet.
  2. Antifurto Dr.Web è attivato.
  3. Alla lista Mi fido di in Antifurto è aggiunto almeno un indirizzo email.
- **Per il dispositivo dell'amico**
  - Se il dispositivo dell'utente è bloccato:
    1. Il dispositivo dell'amico è acceso ed è connesso a internet.
    2. Sul dispositivo dell'amico è installata l'applicazione Dr.Web Light o Dr.Web Security Space.
    3. L'amico ha confermato la richiesta di amicizia dell'utente nel componente Aiuto all'amico o in Antifurto Dr.Web. Per ricevere l'avviso, i componenti devono essere attivati.
  - Se il dispositivo dell'utente non è bloccato:
    1. Il dispositivo dell'amico è acceso ed è connesso a internet.
    2. Sul dispositivo dell'amico è installata l'applicazione Dr.Web Security Space.
    3. L'amico ha confermato la richiesta di amicizia dell'utente in Antifurto Dr.Web. Per ricevere l'avviso, il componente deve essere attivato.

Per resettare la password

1. Inviare l'avviso all'amico. Per fare ciò, premere l'icona ➤ (vedi Immagine 53).
2. Far sapere all'amico il codice di conferma indicato sullo stesso pannello.

   L'amico deve inserire il codice di conferma sul suo dispositivo e inviare ad Antifurto il comando di reset della password.
3. Dopo la ricezione del comando sul dispositivo compare automaticamente la schermata **Cambia password**. Inserire una nuova password. Se il dispositivo era bloccato, esso viene sbloccato.

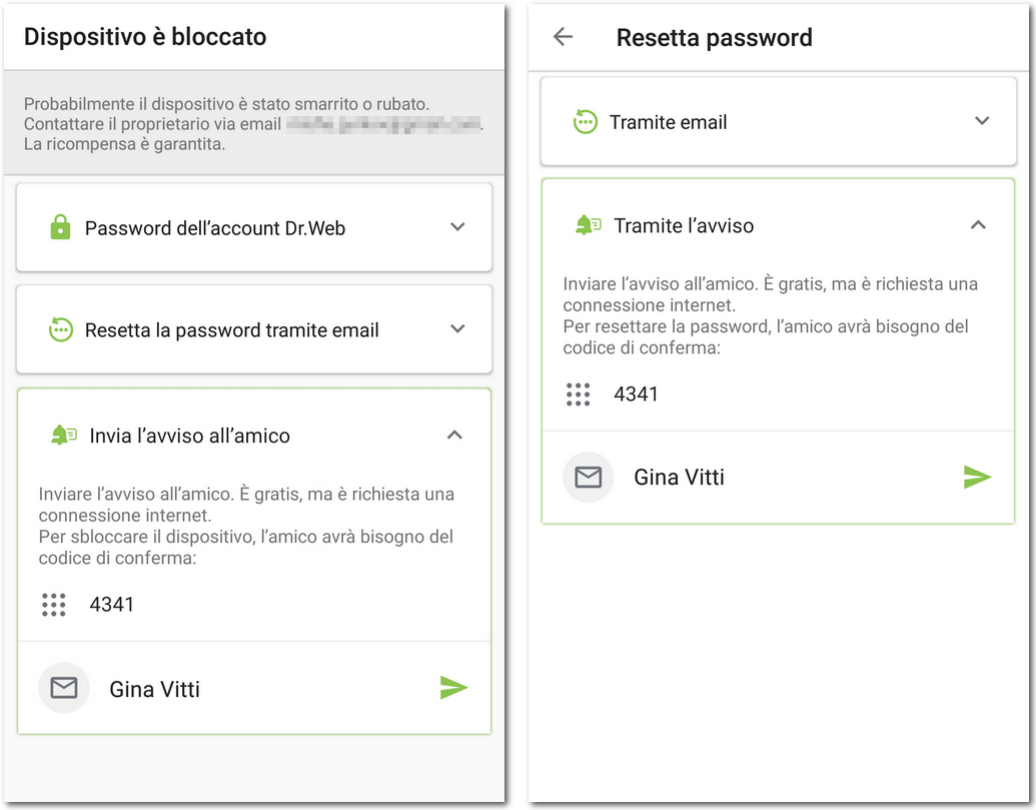

Immagine 53. Resettare la password tramite avviso

Dispositivo bloccato (a sinistra) e quello non bloccato (a destra)

Resettare la password facendo una richiesta al servizio di supporto tecnico

Se non si riesce a sbloccare il dispositivo o impostare una nuova password in autonomo, inviare una richiesta al servizio di supporto tecnico Dr.Web:

1. Aprire la pagina del servizio di supporto tecnico: https://support.drweb.com/.
2. Nella sezione **Supporto tecnico** selezionare la voce **Funzionamento del programma Dr.Web**.
3. Sulla pagina che si è aperta indicare i dati della licenza o il numero dell'ordine.
4. Nella scheda **Per privati** selezionare la voce **Android**.
5. Sulla pagina che si è aperta compilare tutti i campi.
6. Allegare alla richiesta i seguenti file:
   - Una foto della schermata **Dispositivo è bloccato** o **Resetta password** su cui sono distinguibili la chiave e l'indirizzo email (vedi Immagine 47).
   - Se si ha ancora la confezione originale del dispositivo, assicurarsi di allegare alla richiesta una foto della confezione con il numero IMEI (l'identificatore di 15 cifre del dispositivo univoco).
   - Una foto o una copia scannerizzata dello scontrino di acquisto del dispositivo.

- Una foto o una copia scannerizzata del certificato di garanzia compilato.
- Documenti che confermano il pagamento della licenza Dr.Web (email dal negozio online, documento di pagamento ecc.) Se la licenza è stata vinta in un'asta Dr.Web, specificare il login del proprio profilo sul sito Doctor Web. Se viene utilizzata una versione di prova, saltare questo passaggio.

> ⚠ Il testo sulle immagini deve essere chiaramente leggibile: gli specialisti del servizio di supporto tecnico devono assicurarsi che l'autore della richiesta sia il proprietario del dispositivo e della licenza Dr.Web.

7. Premere il pulsante **Invia**.

   All'indirizzo email indicato nella richiesta si riceverà un'email con un link alla richiesta. Nella pagina della richiesta sarà indicato un codice di conferma.
8. Nella schermata **Dispositivo è bloccato** o **Resetta password** inserire il codice di conferma nel campo **Codice di conferma** (vedi Immagine 51) e premere **Continua**.
9. Nella schermata **Cambia password** inserire una nuova password. La password deve contenere almeno 4 caratteri.

   Premere l'icona a destra del campo di immissione per visualizzare i caratteri che vengono digitati. Per nascondere i caratteri, premere l'icona .
10. Ripetere la password e premere **Salva**.

Sbloccare il dispositivo tramite una richiesta all'amministratore

Se Dr.Web funziona in modalità di protezione centralizzata e Antifurto Dr.Web è configurato sul server, per sbloccare il dispositivo, è necessario contattare l'amministratore della rete antivirus aziendale o il fornitore del servizio "Antivirus Dr.Web". È possibile utilizzare due metodi di sblocco:

- Tramite codice QR:
  1. Contattare l'amministratore della rete antivirus aziendale o il fornitore del servizio "Antivirus Dr.Web" in qualsiasi modo possibile.
  2. Trasmettere all'amministratore il codice QR dalla schermata **Dispositivo è bloccato**. Premere e tenere premuto il codice QR per salvarlo sul dispositivo. È anche possibile trasmettere una foto della schermata su cui sia chiaramente visibile il codice QR.

     L'amministratore invierà all'utente un codice QR di conferma dello sblocco del dispositivo.
  3. Assicurarsi di aver ricevuto il codice QR di sblocco, e premere **Continua**.
  4. Nella finestra che si è aperta premere il pulsante **Scansiona codice QR** e puntare la fotocamera del dispositivo sul codice QR di sblocco ottenuto dall'amministratore.

     Se il codice QR viene riconosciuto con successo, il dispositivo verrà sbloccato.
- Tramite codice di caratteri:
  1. Sulla schermata **Dispositivo è bloccato** premere **Altro metodo**.

2. Contattare l'amministratore della rete antivirus aziendale o il fornitore del servizio "Antivirus Dr.Web" in qualsiasi modo possibile.
3. Comunicare all'amministratore l'identificatore e il codice di ripristino visualizzati sulla schermata **Dispositivo è bloccato**.

   L'amministratore invierà all'utente un codice di sblocco del dispositivo.
4. Assicurarsi di aver ricevuto il codice di sblocco, e premere **Continua**.
5. Nella finestra che si è aperta nel campo **Codice di sblocco** inserire il codice ottenuto dall'amministratore e premere **Sblocca**.

   Se il codice di sblocco è stato inserito correttamente, il dispositivo verrà sbloccato.

Se per qualche motivo non è possibile completare la procedura di sblocco del dispositivo tramite il metodo che si è scelto, è possibile passare al metodo alternativo premendo **Altro metodo** sulla schermata **Dispositivo è bloccato**.

Per resettare la password dopo aver sbloccato il dispositivo, contattare l'amministratore della rete antivirus aziendale o il fornitore del servizio "Antivirus Dr.Web".