



**Dr.WEB**  
Agent per Windows

# Manuale dell'utente



© 2020 Doctor Web. Tutti i diritti riservati

Il presente documento ha carattere puramente informativo e indicativo nei confronti del software della famiglia Dr.Web in esso specificato. Il presente documento non costituisce una base per conclusioni esaustive sulla presenza o assenza di qualsiasi parametro funzionale e/o tecnico nel software della famiglia Dr.Web e non può essere utilizzato per determinare la conformità del software della famiglia Dr.Web a qualsiasi requisito, specifica tecnica e/o parametro, nonché ad altri documenti di terze parti.

I materiali riportati in questo documento sono di proprietà Doctor Web e possono essere utilizzati esclusivamente per uso personale dell'acquirente del prodotto. Nessuna parte di questo documento può essere copiata, pubblicata su una risorsa di rete o trasmessa attraverso canali di comunicazione o nei mass media o utilizzata in altro modo tranne che per uso personale, se non facendo riferimento alla fonte.

### **Marchi**

Dr.Web, SplDer Mail, SplDer Guard, CureIt!, CureNet!, AV-Desk, KATANA e il logotipo Dr.WEB sono marchi commerciali registrati di Doctor Web in Russia e/o in altri paesi. Altri marchi commerciali registrati, logotipi e denominazioni delle società, citati in questo documento, sono di proprietà dei loro titolari.

### **Disclaimer**

In nessun caso Doctor Web e i suoi fornitori sono responsabili di errori e/o omissioni nel documento e di danni (diretti o indiretti, inclusa perdita di profitti) subiti dall'acquirente del prodotto in connessione con gli stessi.

**Agent Dr.Web per Windows**  
**Versione 11.5**  
**Manuale dell'utente**  
**17/04/2020**

Doctor Web, Sede centrale in Russia

Indirizzo: 125040, 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

|  |           |
|--|-----------|
| <b>1. Introduzione</b>   | <b>7</b>  |
| 1.1. Di che cosa tratta questa documentazione                        | 8         |
| 1.2. Segni e abbreviature utilizzati                                 | 8         |
| 1.3. Metodi di rilevamento delle minacce                             | 9         |
| <b>2. Requisiti di sistema</b>                                       | <b>13</b> |
| <b>3. Installazione, modifica e rimozione del programma</b>          | <b>15</b> |
| 3.1. Installazione tramite il pacchetto di installazione completo    | 15        |
| 3.2. Installazione tramite il pacchetto di installazione individuale | 18        |
| 3.3. Modifica dei componenti del programma                           | 22        |
| 3.4. Rimozione del programma   | 23        |
| <b>4. Per iniziare</b>   | <b>25</b> |
| 4.1. Verifica dell'antivirus   | 26        |
| <b>5. Strumenti</b>  | <b>28</b> |
| 5.1. Gestione quarantena   | 28        |
| 5.2. Supporto  | 29        |
| 5.2.1. Creazione del report  | 30        |
| <b>6. Scanner Dr.Web</b>   | <b>34</b> |
| 6.1. Avvio della scansione e le modalità di scansione                | 34        |
| 6.2. Azioni in caso di rilevamento delle minacce                     | 36        |
| 6.3. Avvio dello Scanner con i parametri della riga di comando       | 38        |
| 6.4. Scanner console   | 38        |
| 6.5. Avvio della scansione secondo il calendario                     | 39        |
| <b>7. Impostazioni</b>   | <b>40</b> |
| <b>8. Impostazioni principali</b>                                    | <b>41</b> |
| 8.1. Avvisi  | 41        |
| 8.2. Auto-protezione   | 44        |
| 8.3. Dispositivi   | 45        |
| 8.4. Avanzate  | 48        |
| 8.5. Server  | 51        |
| 8.6. Messaggi del server   | 54        |
| <b>9. Office control</b>   | <b>56</b> |
| 9.1. Configurazione del modulo Office control                        | 56        |



|   |            |
|---|------------|
| 9.1.1. Internet   | 57         |
| 9.1.2. Tempo  | 61         |
| 9.1.3. File e cartelle  | 62         |
| <b>10. Eccezioni</b>  | <b>64</b>  |
| <b>10.1. Siti</b>   | <b>64</b>  |
| <b>10.2. File e cartelle</b>  | <b>66</b>  |
| <b>10.3. Applicazioni</b>   | <b>69</b>  |
| <b>10.4. Antispam</b>   | <b>72</b>  |
| <b>11. Componenti di protezione</b>                                     | <b>75</b>  |
| <b>11.1. SpIDer Guard</b>   | <b>75</b>  |
| 11.1.1. Configurazione di SpIDer Guard                                  | 76         |
| <b>11.2. SpIDer Gate</b>  | <b>81</b>  |
| 11.2.1. Configurazione di SpIDer Gate                                   | 81         |
| <b>11.3. SpIDer Mail</b>  | <b>84</b>  |
| 11.3.1. Configurazione di SpIDer Mail                                   | 85         |
| 11.3.2. Antispam  | 89         |
| <b>11.4. Scanner</b>  | <b>91</b>  |
| <b>11.5. Firewall</b>   | <b>93</b>  |
| 11.5.1. Addestramento di Firewall                                       | 93         |
| 11.5.2. Configurazione di Firewall                                      | 96         |
| <b>11.6. Dr.Web per Microsoft Outlook</b>                               | <b>107</b> |
| 11.6.1. Scansione antivirus   | 108        |
| 11.6.2. Controllo antispam  | 110        |
| 11.6.3. Registrazione degli eventi                                      | 113        |
| 11.6.4. Statistiche   | 114        |
| <b>11.7. Protezione preventiva</b>                                      | <b>115</b> |
| <b>12. Statistiche</b>  | <b>120</b> |
| <b>13. Messaggi del server</b>  | <b>123</b> |
| <b>14. Supporto tecnico</b>   | <b>124</b> |
| <b>15. Allegato A. Parametri aggiuntivi da riga di comando</b>          | <b>125</b> |
| <b>15.1. Parametri per Scanner e Scanner console</b>                    | <b>125</b> |
| <b>15.2. Parametri per i pacchetti di installazione</b>                 | <b>131</b> |
| <b>15.3. Codici di ritorno</b>  | <b>134</b> |
| <b>16. Allegato B. Minacce informatiche e metodi per neutralizzarle</b> | <b>135</b> |
| <b>16.1. Classificazione delle minacce</b>                              | <b>135</b> |



|  |            |
|--|------------|
| <b>16.2. Azioni per neutralizzare le minacce</b>               | <b>140</b> |
| <b>17. Allegato C. Principi di denominazione delle minacce</b> | <b>141</b> |



## 1. Introduzione

Agent Dr.Web è studiato per proteggere la memoria di sistema, i dischi rigidi e i supporti rimovibili dei computer con i sistemi operativi della famiglia Microsoft® Windows® da qualsiasi tipo di minacce: virus, rootkit, programmi trojan, spyware, adware, strumenti di hacking e tutti i possibili tipi di oggetti malevoli provenienti da qualsiasi fonte esterna.

L'architettura di Agent Dr.Web è costituita da diversi moduli responsabili di varie funzionalità. Il motore antivirus e i database dei virus sono comuni a tutti i componenti e a tutte le piattaforme.

I componenti del prodotto vengono costantemente aggiornati e i database dei virus, i database delle categorie di risorse web e i database delle regole di filtraggio antispam dei messaggi email vengono regolarmente integrati con nuove firme delle minacce. Il continuo aggiornamento assicura il livello aggiornato della protezione dei dispositivi degli utenti, e inoltre delle applicazioni e dei dati utilizzati. Per una protezione aggiuntiva da programmi malevoli sconosciuti vengono utilizzati i metodi di analisi euristica implementati nel motore antivirus.

Agent Dr.Web è in grado di rilevare e rimuovere dal computer vari programmi indesiderati: adware, dialer, joke, riskware, hacktool. Per rilevare i simili programmi ed eseguire azioni sui file che li contengono, vengono utilizzati strumenti standard dei componenti antivirus Dr.Web.

Ciascuna delle soluzioni antivirus Dr.Web per i sistemi operativi della famiglia Microsoft® Windows® comprende il relativo set dei seguenti componenti di protezione:

[Scanner Dr.Web](#) — scanner antivirus con interfaccia grafica che viene avviato on-demand ed esegue la scansione antivirus del computer.

[Scanner console Dr.Web](#) — versione di Scanner Dr.Web con l'interfaccia a riga di comando.

[SpIDer Guard](#) — monitor antivirus che risiede nella memoria operativa scansionando i file che vengono creati e i processi che vengono avviati, nonché rilevando manifestazioni di attività di virus.

[SpIDer Mail](#) — monitor antivirus della posta per postazioni che intercetta le connessioni di qualsiasi client di posta sul computer ai server di posta attraverso i protocolli POP3/SMTP/IMAP4/NNTP (IMAP4 sta per IMAPv4rev1), rileva e neutralizza le minacce prima ancora che il client di posta riceva le email dal server o invii un'email sul server di posta. Il monitor di posta può inoltre controllare la presenza dello spam nelle email tramite Antispam Dr.Web.

[Dr.Web per Outlook](#) — plugin che controlla nelle caselle Microsoft Outlook la presenza di minacce e dello spam.

[SpIDer Gate](#) — modulo di scansione antivirus del traffico HTTP. Con le impostazioni predefinite il monitoraggio HTTP SpIDer Gate controlla automaticamente il traffico HTTP in arrivo e blocca la trasmissione di oggetti contenenti virus e altri programmi malevoli. Inoltre, di default è attivato il filtraggio URL dei siti non raccomandati e dei siti conosciuti come fonti di diffusione di virus.



**Office control** — componente che limita l'accesso a siti, file e cartelle, e inoltre consente di limitare il tempo di utilizzo della rete Internet e del computer per ciascun account di Windows.

**Firewall Dr.Web** — firewall personale studiato per proteggere il computer da accessi non autorizzati dall'esterno e per prevenire le fughe di informazioni importanti attraverso la rete.

**Agent Dr.Web** — modulo attraverso cui si configura e si gestisce il funzionamento dei componenti del prodotto.

**Protezione preventiva** — componente che controlla l'accesso agli oggetti critici del sistema e assicura l'integrità delle applicazioni in esecuzione e dei file dell'utente, nonché la protezione dagli exploit.

## 1.1. Di che cosa tratta questa documentazione

Questo manuale contiene le informazioni necessarie sull'installazione e sull'uso efficace del programma Dr.Web.

Una descrizione dettagliata di tutti gli elementi dell'interfaccia grafica è contenuta nel sistema di guida disponibile per l'avvio da qualsiasi componente del programma.

Questo manuale contiene una descrizione dettagliata del processo di installazione, nonché le raccomandazioni iniziali per l'utilizzo e la risoluzione dei problemi più comuni legati alle minacce di virus. Principalmente, vengono considerate le modalità standard di funzionamento dei componenti del programma Dr.Web (le impostazioni predefinite).

Gli Allegati contengono informazioni dettagliate sulla configurazione del programma Dr.Web, destinate agli utenti esperti.



A causa del continuo sviluppo, l'interfaccia del programma può non coincidere con le immagini presentate in questo documento. Informazioni sempre aggiornate sono ritrovabili sull'indirizzo <https://download.drweb.com/doc>.

## 1.2. Segni e abbreviature utilizzati

In questo manuale vengono utilizzati i seguenti simboli:

| Simbolo               | Commento  |
|-----------------------|---|
|                       | Avviso di possibili situazioni di errore, nonché di punti importanti cui prestare particolare attenzione. |
| <i>Rete antivirus</i> | Un nuovo termine o un termine accentato nelle descrizioni.  |
| <indirizzo_IP>        | Campi in cui nomi di funzione vanno sostituiti con valori effettivi.                                      |





| Simbolo                    | Commento   |
|----------------------------|--|
| 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.   |
| C:\Windows\                | Nomi di file e directory, frammenti di codice.   |
| <a href="#">Allegato A</a> | Riferimenti incrociati ai capitoli del documento o collegamenti ipertestuali a risorse esterne.                      |

## 1.3. Metodi di rilevamento delle minacce

Tutti i prodotti antivirus sviluppati da Doctor Web impiegano un intero set di metodi di rilevamento delle minacce, il che consente di controllare oggetti sospetti con la massima accuratezza.

### Analisi basata sulle firme antivirali

Questo metodo di rilevamento viene impiegato in primo luogo. Si basa sulla ricerca delle firme delle minacce già conosciute nel contenuto dell'oggetto analizzato. La firma è una sequenza di byte continua finita, necessaria e sufficiente per identificare univocamente una minaccia. I contenuti dell'oggetto analizzato vengono confrontati con i checksum delle firme antivirali anziché con le firme antivirali stesse, il che consente di ridurre notevolmente le dimensioni delle registrazioni nei database dei virus, mantenendo allo stesso tempo l'univocità della corrispondenza e, di conseguenza, la correttezza del rilevamento delle minacce e della cura dell'infezione in oggetti contaminati. Le registrazioni nei database dei virus Dr.Web sono formati in modo tale che tramite una registrazione sia possibile rilevare intere classi o famiglie di minacce.

### Origins Tracing

È una tecnologia unica Dr.Web che consente di rilevare le minacce nuove o modificate di cui il comportamento malevolo o i metodi di infezione sono già conosciuti e descritti nei database dei virus. Viene impiegata dopo l'analisi basata su firme antivirus e protegge gli utenti che utilizzano le soluzioni antivirus Dr.Web dalle minacce quale il trojan-estorsore Trojan.Encoder.18 (anche conosciuto come "gpcode"). Inoltre, l'impiego della tecnologia Origins Tracing fa sì che l'analisi euristica abbia un numero notevolmente minore di falsi positivi. Ai nomi delle minacce rilevate tramite Origins Tracing viene aggiunto il postfisso `.Origin`.

### Emulazione di esecuzione

Il metodo di emulazione di esecuzione del codice software viene utilizzato per rilevare virus polimorfi e cifrati quando la ricerca per checksum di firme antivirali è non applicabile o notevolmente ostacolata a causa di impossibilità di costruire le firme antivirali affidabili. Il metodo



consiste nel simulare l'esecuzione del codice analizzato tramite un *emulatore* — un modello software del processore e dell'ambiente di esecuzione dei programmi. L'emulatore utilizza una zona di memoria protetta (*buffer di emulazione*). In tale caso le istruzioni non vengono trasmesse sulla CPU per essere effettivamente eseguite. Se il codice processato dall'emulatore è infetto, come risultato dell'emulazione verrà ripristinato il codice malevolo originale che può essere analizzato tramite l'analisi basata sulle firme antivirali.

## Analisi euristica

L'analisi euristica si basa su un set delle conoscenze *euristiche* (ipotesi la cui significatività statistica è stata empiricamente confermata) circa le caratteristiche del codice eseguibile malevolo o, al contrario, sicuro. Ogni caratteristica del codice ha un determinato peso (cioè un numero che indica l'importanza e la validità di tale caratteristica). Il peso può essere sia positivo, se la caratteristica indica la presenza di un comportamento malevolo del codice, che negativo, se la caratteristica non è peculiare delle minacce informatiche. Sulla base del peso complessivo attribuito al contenuto dell'oggetto, l'analisi euristica calcola la probabilità di presenza di un oggetto malevolo sconosciuto. Se questa probabilità eccede un determinato valore di soglia, l'analisi euristica conclude che l'oggetto analizzato è malevolo.

L'analisi euristica utilizza inoltre la tecnologia FLY-CODE — un universale algoritmo per lo spaccettamento di file. Questo metodo consente di costruire un presupposto euristico circa la presenza di oggetti malevoli negli oggetti compressi dai programmi di impacchettamento (packer), e non solo da quelli conosciuti dagli sviluppatori del prodotto Dr.Web, ma anche da quelli nuovi, non ancora studiati. Quando vengono controllati gli oggetti compressi, viene inoltre utilizzata la tecnologia di analisi dell'entropia di struttura che consente di rilevare minacce sulla base delle caratteristiche della posizione dei tratti del codice. Tramite questa tecnologia sulla base di una registrazione del database dei virus è possibile rilevare una serie di varie minacce compresse dall'uguale packer polimorfico.

Siccome l'analisi euristica è un sistema di verifica delle ipotesi in condizioni di incertezza, può commettere sia un tipo di errori (salta minacce sconosciute) e sia un altro tipo di errori (riconosce come dannoso un programma innocuo). Pertanto, agli oggetti contrassegnati dall'analisi euristica come "malevoli" viene attribuito lo stato "sospetti".

## Analisi comportamentale

I metodi di analisi comportamentale consentono di analizzare la sequenza delle azioni di tutti i processi nel sistema. Quando vengono rilevati segni di comportamento di programmi malevoli, le azioni di tale applicazione vengono bloccate.

### Dr.Web Process Heuristic

La tecnologia di analisi comportamentale Dr.Web Process Heuristic protegge dai programmi malevoli più recenti e pericolosi che sono capaci di evitare il rilevamento tramite i meccanismi tradizionali di firme antivirali e di analisi euristica.



Dr.Web Process Heuristic analizza il comportamento di ciascun programma in esecuzione e sulla base delle ultime conoscenze sul comportamento dei programmi malevoli, determina se un programma è pericoloso, dopo di che vengono adottate le misure necessarie per neutralizzare la minaccia.

Questa tecnologia di protezione dati permette di minimizzare le perdite dalle azioni di un virus sconosciuto con il minimo consumo di risorse del sistema protetto.

Dr.Web Process Heuristic controlla tutti i tentativi di modifica del sistema:

- riconosce i processi dei programmi malevoli che modificano in modo indesiderabile i file dell'utente (per esempio, i tentativi di criptazione da parte dei trojan cryptolocker), compresi quelli situati in directory disponibili via rete;
- impedisce i tentativi dei programmi malevoli di integrarsi nei processi di altre applicazioni;
- protegge le porzioni critiche del sistema dalle modifiche da parte dei programmi malevoli;
- rileva e termina gli script e i processi malevoli, sospetti o inattendibili;
- blocca la possibilità di modifica dei settori di avvio del disco da parte dei programmi malevoli per rendere impossibile l'avvio (per esempio, dei bootkit) sul computer;
- previene la disattivazione della modalità provvisoria di Windows, bloccando modifiche del registro;
- non permette ai programmi malevoli di modificare le regole di avvio di programmi;
- blocca il caricamento di driver nuovi o sconosciuti all'insaputa dell'utente;
- blocca l'esecuzione automatica di programmi malevoli, nonché di determinate applicazioni, quali gli anti-antivirus, non permettendo che si iscrivano al registro per il successivo avvio automatico;
- blocca i rami del registro responsabili dei driver di dispositivi virtuali, il che rende impossibile l'installazione di programmi trojan sotto le mentite spoglie di un nuovo dispositivo virtuale;
- non permette al software malevolo di compromettere il normale funzionamento dei servizi di sistema.

### **Dr.Web Process Dumper**

L'analisi integrata delle minacce pacchettizzate Dr.Web Process Dumper aumenta significativamente il livello di rilevamento delle minacce apparentemente "nuove" — cioè che sono conosciute dal database dei virus Dr.Web, ma sono nascoste sotto packer nuovi, nonché elimina la necessità di aggiungere al database dei virus sempre nuovi record di minacce. La compattezza mantenuta del database dei virus Dr.Web, a sua volta, non necessita di costante aumento dei requisiti di sistema e assicura le dimensioni tradizionalmente piccole degli aggiornamenti con la qualità di rilevamento e cura invariabilmente alta.

### **Dr.Web ShellGuard**

La tecnologia Dr.Web ShellGuard protegge il computer dagli *exploit* — oggetti malevoli che cercano di sfruttare le vulnerabilità per ottenere il controllo sulle applicazioni attaccate o sul sistema operativo in generale.



Dr.Web ShellGuard protegge le applicazioni più comuni installate su computer con Windows:

- i browser (Internet Explorer, Mozilla Firefox, Yandex.Browser, Google Chrome, Vivaldi Browser e altri ancora);
- le applicazioni MS Office, inclusa MS Office 2016;
- le applicazioni di sistema;
- le applicazioni che utilizzano le tecnologie java, flash e pdf;
- i lettori multimediali.

## Metodo di apprendimento automatico

Viene utilizzato per cercare e neutralizzare oggetti malevoli che ancora non ci sono nei database dei virus. Il vantaggio di questo metodo consiste nel riconoscimento di un codice malevolo senza eseguirlo, solo in base alle sue caratteristiche.

Il rilevamento delle minacce si basa sulla classificazione degli oggetti malevoli secondo determinati segni. Tramite la tecnologia di apprendimento automatico basato sul metodo dei vettori di supporto, vengono effettuate la classificazione e la registrazione nel database dei frammenti di codice dei linguaggi di scripting. In seguito gli oggetti controllati vengono analizzati in base alla conformità ai segni di codice malevolo. La tecnologia di apprendimento automatico automatizza l'aggiornamento della lista di questi segni e l'integrazione dei database dei virus. La tecnologia può funzionare anche senza connessione costante al cloud.

Il metodo di apprendimento automatico risparmia in modo significativo le risorse del sistema operativo in quanto non richiede l'esecuzione di codice per rilevare le minacce, mentre l'addestramento automatico dinamico del classificatore può essere effettuato anche senza aggiornamento costante dei database dei virus, utilizzato nell'analisi basata sulle firme antivirali.



## 2. Requisiti di sistema



Prima di installare il programma Dr.Web, è necessario:

- rimuovere dal computer altri programmi antivirus per prevenire possibili incompatibilità dei relativi componenti residenti in memoria con i componenti Dr.Web residenti in memoria;
- se verrà installato Firewall Dr.Web, è inoltre necessario rimuovere dal computer altri firewall;
- su Windows Server 2016 disattivare manualmente Windows Defender utilizzando criteri di gruppo;
- installare tutti gli aggiornamenti critici consigliati dal produttore del sistema operativo; se il produttore ha interrotto il supporto del sistema operativo, è consigliato passare a una versione del sistema operativo più recente.

L'uso del programma Dr.Web è possibile su un computer che soddisfa i seguenti requisiti:

| Componente        | Requisito  |
|-------------------|--|
| Processore        | Completo supporto del set di istruzioni i686.  |
| Sistema operativo | <p>In caso dei sistemi operativi a 32 bit:</p> <ul style="list-style-type: none"><li>• Windows XP con il pacchetto degli aggiornamenti SP2 e superiori;</li><li>• Windows Vista con il pacchetto degli aggiornamenti SP2 e superiori;</li><li>• Windows 7;</li><li>• Windows 8;</li><li>• Windows 8.1;</li><li>• Windows 10 19H1 o versioni inferiori;</li><li>• Windows Server 2003 con il pacchetto degli aggiornamenti SP1;</li><li>• Windows Server 2008 con il pacchetto degli aggiornamenti SP2 e superiori.</li></ul> <p>In caso dei sistemi operativi a 64 bit:</p> <ul style="list-style-type: none"><li>• Windows Vista con il pacchetto degli aggiornamenti SP2 e superiori;</li><li>• Windows 7;</li><li>• Windows 8;</li><li>• Windows 8.1;</li><li>• Windows 10 19H1 o versioni inferiori;</li><li>• Windows Server 2008 con il pacchetto degli aggiornamenti SP2 e superiori;</li><li>• Windows Server 2008 R2;</li></ul> |



| Componente                            | Requisito   |
|---------------------------------------|---|
|                                       | <ul style="list-style-type: none"><li>• Windows Server 2012;</li><li>• Windows Server 2012 R2;</li><li>• Windows Server 2016.</li></ul>   |
| Memoria operativa libera              | 512 MB o più.   |
| Risoluzione schermo                   | La risoluzione schermo consigliata è almeno 800x600.  |
| Supporto di ambienti virtuali e cloud | È supportato il funzionamento del programma nei seguenti ambienti: <ul style="list-style-type: none"><li>• VMware;</li><li>• Hyper-V;</li><li>• Xen;</li><li>• KVM.</li></ul>   |
| Altro                                 | <p>Per aggiornare i database dei virus Dr.Web e i componenti di Dr.Web, è necessaria una connessione al server di protezione centralizzata o alla rete Internet in Modalità mobile.</p> <p>Per il plugin Dr.Web per Outlook deve essere installato il client Microsoft Outlook di MS Office:</p> <ul style="list-style-type: none"><li>• Outlook 2000;</li><li>• Outlook 2002;</li><li>• Outlook 2003;</li><li>• Outlook 2007;</li><li>• Outlook 2010 con il pacchetto degli aggiornamenti SP2;</li><li>• Outlook 2013;</li><li>• Outlook 2016.</li></ul> |



Agent Dr.Web non è compatibile con i plugin Dr.Web per Microsoft Exchange Server, Dr.Web per IBM Lotus Domino, Dr.Web per Kerio WinRoute, Dr.Web per Kerio MailServer, Dr.Web per Microsoft ISA Server e Forefront TMG, Dr.Web per Qbik WinGate versioni 6.0 e inferiori.

I requisiti di configurazione ommessi coincidono con tali per i relativi sistemi operativi.



## 3. Installazione, modifica e rimozione del programma

Prima di iniziare a installare Agent Dr.Web, leggere i [requisiti di sistema](#), e inoltre si consigliano le seguenti azioni:

- installare tutti gli aggiornamenti critici rilasciati da Microsoft per la versione del sistema operativo in uso sul computer (possono essere scaricati e installati dal sito degli aggiornamenti Microsoft sull'indirizzo <https://windowsupdate.microsoft.com>);
- controllare il file system tramite gli strumenti di sistema ed eliminare eventuali difetti;
- chiudere le applicazioni attive.



Prima di installare, è inoltre necessario rimuovere dal computer altri programmi antivirus e firewall per prevenire possibili incompatibilità dei relativi componenti residenti in memoria.

L'installazione di Dr.Web deve essere eseguita da un utente con i permessi dell'amministratore di tale computer.

Ci sono due modi possibili per installare, modificare e rimuovere Dr.Web:

1. Su remoto — dal server di protezione centralizzata via rete. Si effettua dall'amministratore della rete antivirus, e l'intervento dell'utente non è richiesto.
2. Localmente — direttamente sulla macchina dell'utente. In questo caso per l'installazione di Dr.Web può essere utilizzato un [installer completo](#) o un [pacchetto di installazione individuale](#).

È possibile installare Dr.Web in una delle seguenti modalità:

- in modalità riga di comando;
- in modalità installazione guidata.

### 3.1. Installazione tramite il pacchetto di installazione completo

#### Installazione in modalità riga di comando

Per avviare l'installazione di Dr.Web in modalità riga di comando, andare alla cartella in cui è situato si trova il pacchetto, dopodiché inserire il nome del file di installazione eseguibile (`drweb-11.05.0-xxxxxxx-esuite-agent-full-windows.exe`) con i parametri richiesti.

La lista completa dei parametri della riga di comando per i pacchetti di installazione è riportata in [Allegato A](#).

## Installazione in modalità installazione guidata

1. Avviare il pacchetto di installazione fornito dall'amministratore. Si apre la finestra dell'Installazione guidata di Dr.Web.



Se sulla postazione sono già installati programmi antivirus, l'Installazione guidata cercherà di rimuoverli. Se il tentativo non è riuscito, è necessario rimuovere in autonomo il software antivirus utilizzato sulla postazione.

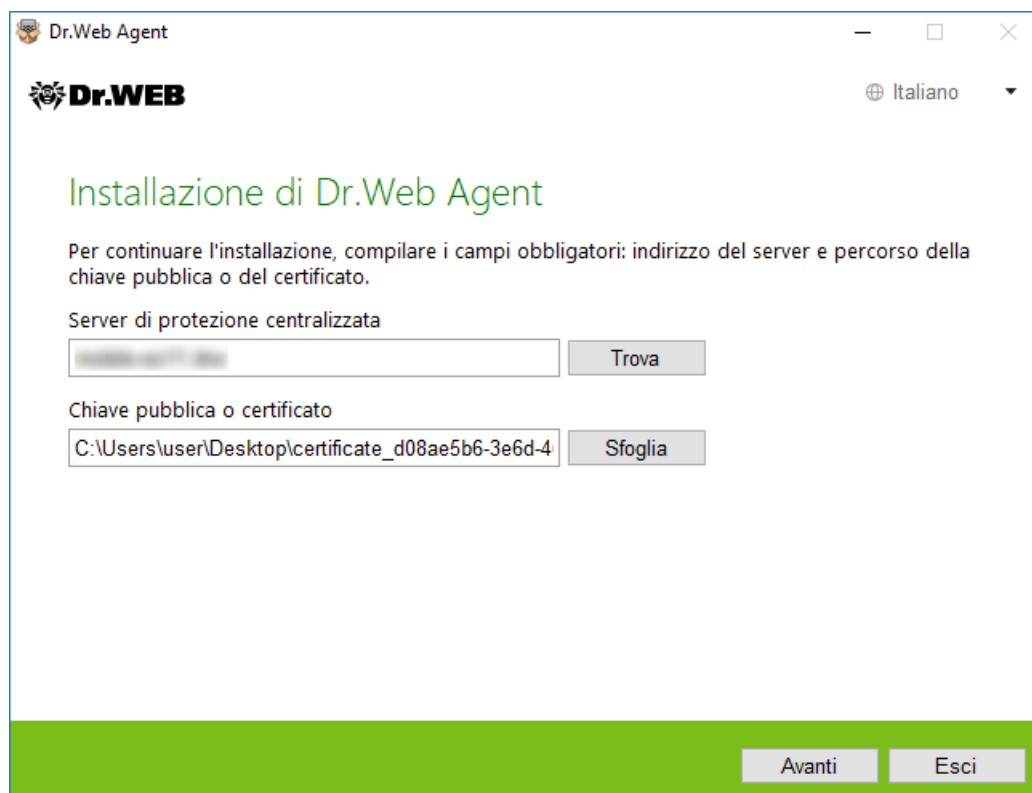


Immagine 1. Installazione guidata

2. Nel campo **Server di protezione centralizzata** inserire l'indirizzo di rete del server da cui verrà installato Dr.Web, e nel campo **Chiave pubblica o certificato** indicare il percorso completo della chiave di cifratura pubblica (**drwcsd.pub**) o del certificato con l'estensione **.pem** situato sul computer.  
Premere il pulsante **Avanti**.
3. L'Installazione guidata informerà che il software è pronto per l'installazione. È possibile avviare il processo di installazione con le impostazioni predefinite premendo **Installa**.  
Per selezionare in autonomo i componenti da installare, il percorso di installazione e alcuni altri parametri di installazione, premere **Parametri di installazione**. Questa opzione è destinata agli utenti esperti.
4. Premere **Avanti**.
5. Se al passaggio precedente si è premuto il pulsante **Installa**, passare al passaggio 8. Altrimenti, si apre la finestra **Parametri di installazione**.





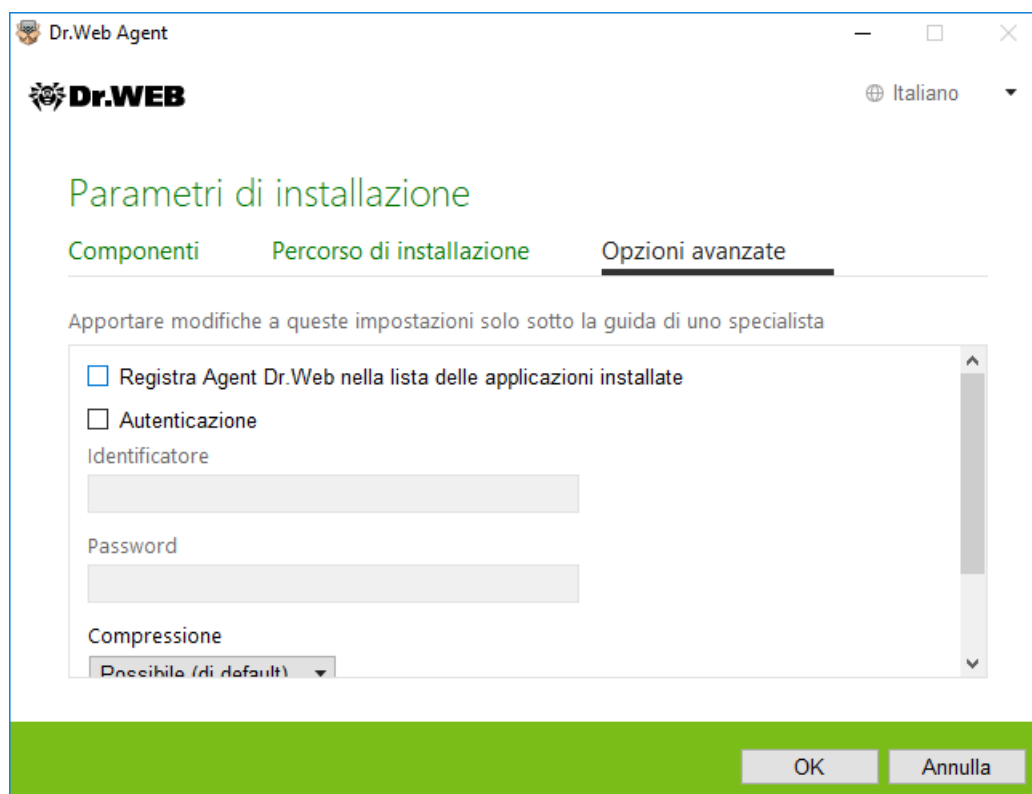
Nella scheda **Componenti** è possibile selezionare i componenti Dr.Web da installare.

Attivare i flag di fronte ai componenti che si vogliono installare sul computer. Di default sono selezionati tutti i componenti ad eccezione di Firewall Dr.Web.

6. Nella scheda **Percorso di installazione** è possibile indicare la cartella di installazione in cui verrà installato Agent Dr.Web.

Di default è la cartella DrWeb situata nella cartella Program Files sul disco di sistema. Per modificare il percorso di installazione, premere il pulsante **Sfoggia** e indicare il percorso desiderato.

7. Nella scheda **Opzioni avanzate** è possibile indicare impostazioni aggiuntive.



**Immagine 2. Installazione guidata, impostazioni avanzate**

Se necessario, spuntare il flag **Registra Agent Dr.Web nella lista delle applicazioni installate**. Questa opzione consente, tra le altre cose, di [rimuovere](#) il programma Dr.Web tramite il Pannello di controllo di Windows.

Per l'autenticazione manuale sul server di protezione centralizzata spuntare il flag **Autenticazione**. Quindi è necessario impostare i parametri di autenticazione della postazione:

- **Identificatore** della postazione sul server;
- **Password** per l'accesso al server.

In questo caso la postazione otterrà l'accesso senza una conferma manuale da parte dell'amministratore sul server.

Nelle liste a cascata **Compressione** e **Cifratura** impostare le rispettive modalità per il traffico tra il server e Dr.Web.

Per salvare le modifiche apportate, premere **OK**, dopodiché premere il pulsante **Installa**.



- Inizierà l'installazione di Dr.Web. Non è richiesto alcun intervento da parte dell'utente.
- Dopo il completamento dell'installazione il programma avviserà della necessità di riavviare il computer. Premere il pulsante **Riavvia adesso**.

## 3.2. Installazione tramite il pacchetto di installazione individuale

### Installazione in modalità riga di comando

Per avviare l'installazione di Dr.Web in modalità riga di comando, andare alla cartella in cui si trova il pacchetto, dopo di che inserire il nome del file eseguibile di installazione (drweb\_ess\_windows\_<Station\_name>.exe) con i parametri richiesti.

La lista completa dei parametri della riga di comando per i pacchetti di installazione è riportata in [Allegato A](#).

### Installazione in modalità installazione guidata

- Avviare il pacchetto di installazione fornito dall'amministratore. Si apre l'Installazione guidata di Dr.Web.



Se sulla postazione sono già installati programmi antivirus, l'Installazione guidata cercherà di rimuoverli. Se il tentativo non è riuscito, è necessario rimuovere in autonomo il software antivirus utilizzato sulla postazione.

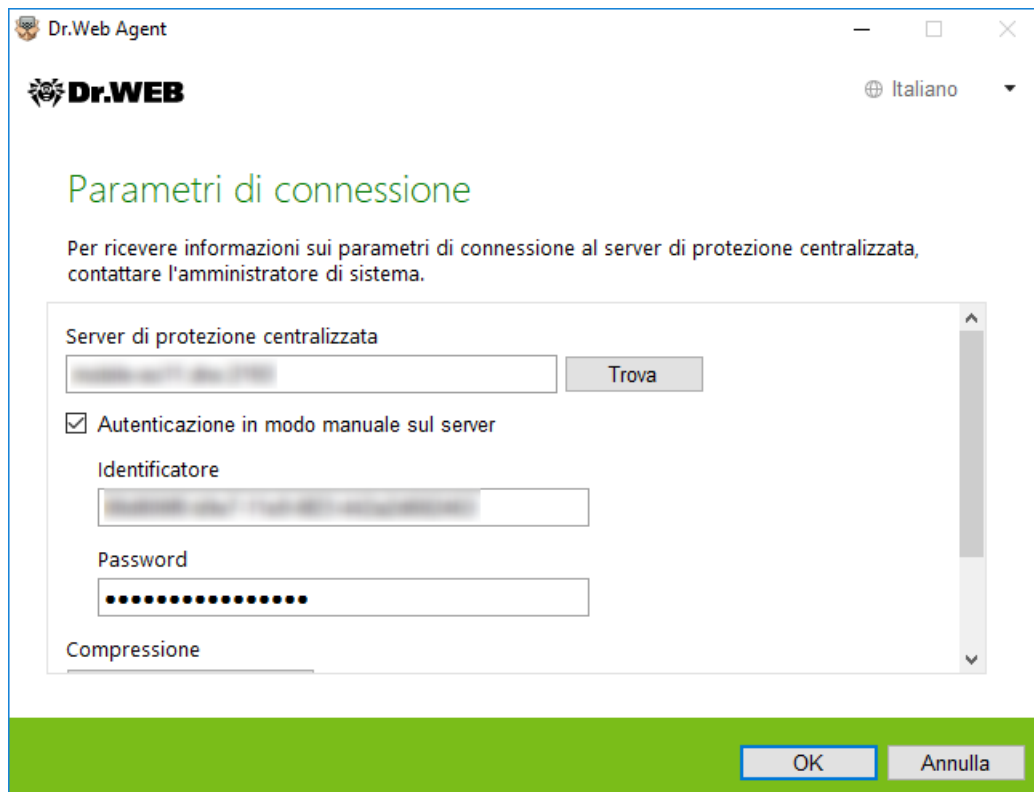


**Immagine 3. Installazione guidata**

2. Premere **Avanti**.
3. Al passaggio successivo della procedura guidata indicare il percorso della chiave di cifratura pubblica (**drwcsd.pub**) o del certificato con l'estensione **.pem** situato sul computer.
4. È possibile modificare i parametri della connessione al server di protezione centralizzata. A questo scopo fare clic sul link corrispondente, si apre la finestra **Parametri di connessione**.



Si raccomanda vivamente di non cambiare nulla senza il consenso dell'amministratore della rete antivirus.



**Immagine 4. Impostazione dei parametri della connessione al server di protezione centralizzata**



Per informazioni sui parametri della connessione al server di protezione centralizzata contattare l'amministratore.

Nel campo **Server di protezione centralizzata** impostare l'indirizzo di rete del server da cui verrà installato Dr.Web. Il campo viene compilato automaticamente, vengono indicati i dati del server su cui è stato creato il file di installazione.

Per l'opzione di autenticazione manuale sul server attivare il flag corrispondente. Quindi è necessario impostare i parametri di autenticazione della postazione:

- **Identificatore** della postazione sul server;
- **Password** per l'accesso al server.

In questo caso la postazione otterrà l'accesso senza una conferma manuale da parte dell'amministratore sul server.



Se Dr.Web viene installato tramite un file di installazione creato nel Pannello di controllo Dr.Web, i campi **Identificatore** e **Password** per l'opzione di autenticazione manuale vengono compilati automaticamente.

Nelle liste a cascata **Compressione** e **Cifratura** impostare le rispettive modalità per il traffico tra il server e Dr.Web.

Per salvare le modifiche apportate, premere **OK**, dopo di che premere **Avanti**.



Se la connessione non è stata stabilita, controllare i parametri di rete in base al link e/o ripetere il tentativo di connessione premendo il pulsante corrispondente.

- Se la connessione al server di protezione centralizzata è riuscita, si apre una finestra con un messaggio che dice che il software è pronto per l'installazione. È possibile avviare il processo di installazione con le impostazioni predefinite premendo il pulsante **Installa**.

Per selezionare in autonomo i componenti da installare, il percorso di installazione e alcuni altri parametri di installazione, premere **Parametri di installazione**. Questa opzione è destinata agli utenti esperti.

- Se al passaggio precedente si è premuto il pulsante **Installa**, passare al passaggio 8. Altrimenti, si apre la finestra **Parametri di installazione**.

Nella scheda **Componenti** è possibile selezionare i componenti Dr.Web da installare.

Attivare i flag di fronte ai componenti che si vogliono installare sul computer. Di default sono selezionati tutti i componenti ad eccezione di Firewall Dr.Web.

- Nella scheda **Percorso di installazione** è possibile indicare la cartella di installazione in cui verrà installato **Agent Dr.Web**. Di default è la cartella DrWeb situata nella cartella Program Files sul disco di sistema. Per modificare il percorso di installazione, premere il pulsante **Sfoglia** e indicare il percorso desiderato.
- Nella scheda **Opzioni avanzate** è possibile indicare impostazioni aggiuntive per l'installazione del programma Dr.Web.

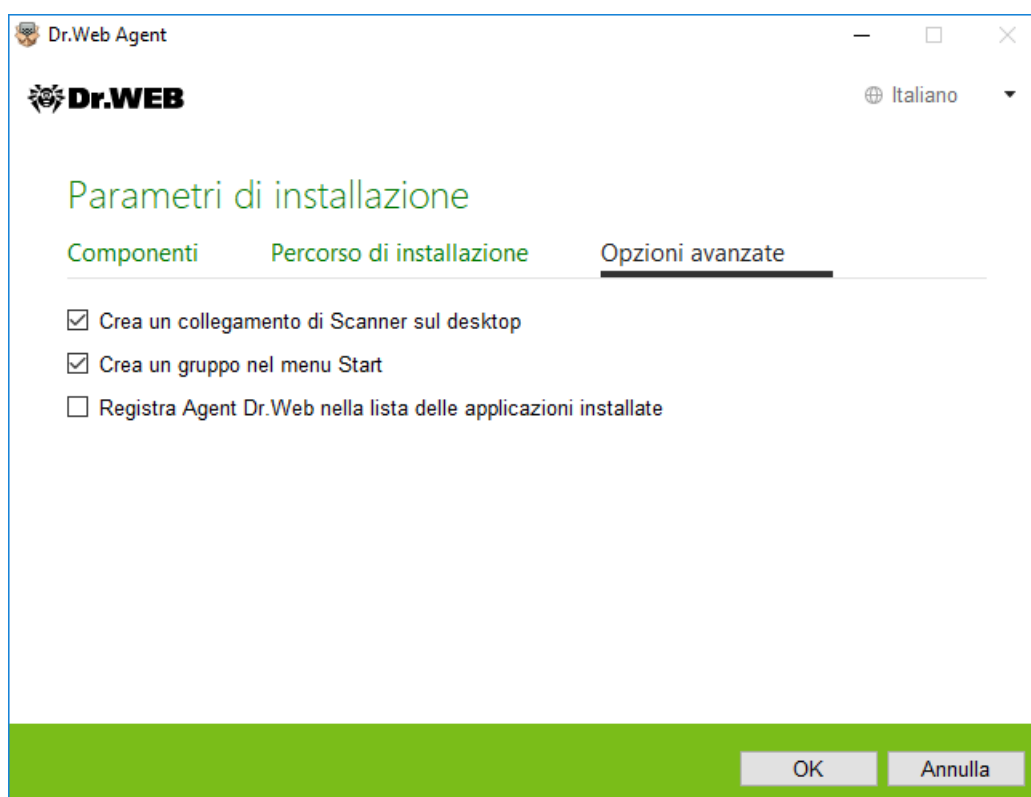


Immagine 5. Installazione guidata, impostazioni avanzate



Se necessario, attivare il flag **Registra Agent Dr.Web nella lista delle applicazioni installate**. Questa opzione consente, tra le altre cose, di [rimuovere](#) il programma Dr.Web tramite il Pannello di controllo di Windows.

Per salvare le modifiche apportate, premere **OK**, quindi premere **Installa**.

9. Inizierà l'installazione di Dr.Web. Non è richiesto alcun intervento da parte dell'utente.
10. Dopo il completamento dell'installazione la procedura guidata avviserà della necessità di riavviare il computer. Premere il pulsante **Riavvia adesso**.

## Errore del servizio BFE durante l'installazione del programma Dr.Web

Per il funzionamento di alcuni componenti di Dr.Web è necessario che sia in esecuzione il servizio modulo di filtraggio di base (BFE). Se questo servizio è mancante o danneggiato, l'installazione di Dr.Web sarà impossibile. Un servizio BFE danneggiato o mancante può indicare la presenza di minacce per la sicurezza del computer.

**Se il tentativo di installazione di Dr.Web è terminato con l'errore del servizio BFE, eseguire le seguenti azioni:**

1. Eseguire una scansione del sistema della postazione tramite l'utility di cura CureNet! da Doctor Web. È possibile richiedere una versione di prova dell'utility (diagnostica senza funzione di cura) sull'indirizzo: <https://download.drweb.com/curenet/>.  
Per informazioni sulle condizioni di uso e sul costo della versione completa dell'utility, consultare l'indirizzo <https://estore.drweb.com/utilities/>.
2. Ripristinare il servizio BFE. Per fare ciò, è possibile utilizzare l'utility per la risoluzione dei problemi nel funzionamento del firewall da Microsoft (per i sistemi operativi Windows 7 e superiori). L'utility può essere scaricata sul sito: <https://support.microsoft.com/en-us/help/17613/automatically-diagnose-and-fix-problems-with-windows-firewall>.
3. Avviare l'Installazione guidata di Dr.Web ed eseguire l'installazione secondo la procedura standard sopra riportata.

Se il problema persiste, contattare il servizio di supporto tecnico dell'azienda Doctor Web.

## 3.3. Modifica dei componenti del programma

1. Per rimuovere o modificare componenti Dr.Web, andare alla sezione del Pannello di controllo di Windows dedicata all'installazione e alla rimozione dei programmi.
2. Nella lista dei programmi installati selezionare la riga con il nome del programma.
3. Premere **Modifica**, si aprirà la finestra di Procedura guidata di rimozione/modifica dei componenti del programma.



**Immagine 6. Procedura guidata di rimozione/modifica dei componenti**

4. Selezionare una delle opzioni:

- **Modifica componenti.** Nella finestra che si è aperta spuntare i flag di fronte ai componenti che si vogliono aggiungere, o togliere i flag di fronte ai componenti da rimuovere. Dopo aver definito la configurazione richiesta, premere **Applica**.
- **Ripristina programma,** se è necessario ripristinare la protezione antivirus sul computer. Questa funzione viene utilizzata quando alcuni componenti del programma Dr.Web sono stati danneggiati.
- **Rimuovi programma,** per [rimuovere](#) tutti i componenti installati.

### 3.4. Rimozione del programma



Per poter rimuovere Dr.Web localmente, questa opzione deve essere consentita dall'amministratore sul server di protezione centralizzata.

Dopo la rimozione di Dr.Web il computer non sarà protetto da virus e altri programmi malevoli.

### Rimozione di Dr.Web tramite il Pannello di controllo di Windows



Questo metodo di rimozione è disponibile solo se tramite l'Installazione guidata è stato spuntato il flag **Registra Agent Dr.Web nella lista delle applicazioni installate**.

Se Dr.Web è stato installato in background, la rimozione di Dr.Web tramite i mezzi standard sarà disponibile solo se nell'installazione è stata utilizzata l'opzione -regagent.

1. Per rimuovere Agent Dr.Web avviare il componente di rimozione di programmi del sistema operativo Windows.
2. Nella lista che si è aperta selezionare la riga con il nome del programma.
3. Premere il pulsante **Rimuovi**.
4. Nella finestra **Parametri da conservare** spuntare i flag di fronte agli elementi da mantenere dopo la rimozione del programma. Gli oggetti e i parametri salvati possono essere utilizzati dal programma in caso di un'altra installazione. Di default sono selezionate tutte le opzioni — **Quarantena, Impostazioni Dr.Web Agent** e **Copie di file protette**. Premere il pulsante **Installa**.
5. Nella finestra successiva, per confermare la rimozione di Dr.Web, premere il pulsante **Rimuovi**.
6. Le modifiche diventeranno effettive dopo il riavvio del computer. È possibile differire il processo di riavvio, premendo il pulsante **Più tardi**. Premere il pulsante **Riavvia adesso** per completare immediatamente la procedura di rimozione dei componenti o modifica della lista dei componenti Dr.Web.

## Rimozione in modalità riga di comando

Per rimuovere Dr.Web in modalità riga di comando, inserire il nome del file eseguibile (`win-es-agent-setup.exe`) con i parametri richiesti.



Il file `win-es-agent-setup.exe` è situato nella cartella `C:\ProgramData\Doctor Web\Setup\`.


Per esempio se viene eseguito il seguente comando, Dr.Web verrà rimosso in background e il computer verrà riavviato:

```
win-es-agent-setup.exe /instMode remove /silent yes
```





## 4. Per iniziare




Dopo l'installazione del programma Dr.Web, all'area di notifica di Windows viene aggiunta l'icona .



L'icona Dr.Web non viene visualizzata nell'area di notifica se l'amministratore della rete antivirus ha impostato tale opzione sul server di protezione centralizzata.

Se il programma non è in esecuzione, nel menu **Start** espandere il gruppo **Dr.Web** e selezionare la voce **SpIDer Agent**.

L'icona Dr.Web rispecchia lo stato attuale del programma:


-  — tutti i componenti necessari per la protezione del computer sono in esecuzione e funzionano correttamente, è attiva una connessione al server di protezione centralizzata;
-  — l'auto-protezione di Dr.Web o almeno uno dei componenti importanti sono disattivati, il che indebolisce la protezione dell'antivirus e del computer; o il programma è in attesa di connessione con il server, ma la connessione non è ancora stata stabilita. Probabilmente, il server ha rifiutato la connessione della postazione o ha negato l'accesso alle proprie risorse. Attivare Auto-protezione o il componente disattivato, attendere la connessione con il server o rivolgersi all'amministratore della rete antivirus se la connessione non viene stabilita, attendere la connessione con il server o rivolgersi al provider se la connessione non viene stabilita;
-  — il programma è in attesa di avvio dei componenti dopo la partenza del sistema operativo, attendere l'avvio dei componenti del programma; o un errore si è verificato nel corso dell'avvio di uno dei componenti chiave di Dr.Web, il computer è a rischio di infezione. Se l'icona non cambia, rivolgersi all'amministratore della rete antivirus.

Inoltre, secondo le [impostazioni](#), sopra l'icona  possono apparire vari suggerimenti-avvisi.

Per accedere al menu Dr.Web, fare clic sull'icona  nell'area di notifica di Windows.



Si può accedere alle impostazioni e ai componenti di protezione, nonché disattivare componenti solo se si hanno i permessi di amministratore.

Nel menu Dr.Web  sono concentrati gli strumenti principali di gestione e le impostazioni del programma.

**Strumenti.** Apre un menu che concede l'accesso alle sezioni:


- [Gestione quarantena](#);
- [Supporto](#).





**Componenti di protezione.** Un accesso veloce alla lista dei componenti di protezione in cui è possibile attivare o disattivare ciascuno dei componenti.

**Scanner.** Un accesso veloce all'avvio di diversi tipi di scansione.

**Messaggi del server.** Apre una finestra di visualizzazione dei messaggi del server.

**Modalità di operazione** . Consente di passare da modalità utente a modalità amministratore. Di default Dr.Web si avvia in una modalità limitata — la modalità utente in cui non sono disponibili [Impostazioni](#) e la configurazione di [Componenti di protezione](#). Per passare all'altra modalità, fare clic sul lucchetto. Se è attivo l'UAC, il sistema operativo visualizzerà una richiesta di aumento dei permessi. Inoltre, per cambiare la modalità, sarà necessario immettere la password se nella sezione [Impostazioni](#) è stata attivata l'opzione **Proteggi da password le impostazioni Dr.Web**. Notare che il programma ritorna in modalità utente 15 minuti dopo il passaggio a modalità amministratore. Se al termine di questo periodo si continua a gestire le impostazioni, il programma ritornerà in modalità utente dopo la chiusura della finestra di configurazione.

**Statistiche** . Apre una finestra che contiene informazioni sul funzionamento dei componenti durante la sessione corrente (il numero di oggetti controllati, infetti e sospetti, le azioni eseguite ecc.).

**Impostazioni** . Apre una finestra che concede l'accesso alle impostazioni principali, alle impostazioni dei componenti di protezione, nonché al modulo Office control e alle eccezioni.



Non è possibile modificare le impostazioni e disattivare qualche componente se l'amministratore del server di protezione centralizzata a cui si connette Dr.Web non ha autorizzato tali azioni.

Per l'accesso alle impostazioni dei componenti è necessario immettere la password se nella sezione [Impostazioni](#) è stata attivata l'opzione **Proteggi da password le impostazioni Dr.Web**.

Se si è dimenticata la password delle impostazioni del prodotto, rivolgersi all'amministratore della rete antivirus.

**Guida** . Apre la guida.

## 4.1. Verifica dell'antivirus

### Verifica tramite il file EICAR

È possibile verificare l'operatività dei programmi antivirus che rilevano i virus sulla base delle firme antivirali, utilizzando il file di test EICAR (European Institute for Computer Anti-Virus Research).



Molti sviluppatori degli antivirus usano per questo scopo lo stesso programma standard test.com. Questo programma è stato specificamente sviluppato affinché l'utente, senza esporre a pericolo il proprio computer, possa vedere come l'antivirus installato segnalerà il rilevamento di un virus. Il programma test.com non è malevolo di per sé, ma viene processato come un virus dalla maggior parte dei programmi antivirus. Dr.Web denomina questo "virus" nel seguente modo: EICAR Test File (Not a Virus!). Gli altri programmi antivirus lo denominano in un modo simile.

Il programma test.com è un file COM di 68 byte e come risultato della sua esecuzione nella console viene visualizzato il messaggio di testo: EICAR-STANDARD-ANTIVIRUS-TEST-FILE!

Il file test.com è composto soltanto dai caratteri di testo che formano la seguente stringa:

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

Se si creerà un file contenente la stringa sopracitata e si salverà il file sotto il nome test.com, come risultato si otterrà un programma che è il "virus" descritto sopra.



Quando funziona [in modalità ottimale](#), SpIDer Guard non interrompe l'avvio del file di test EICAR e non determina questa operazione come pericolosa poiché questo file non rappresenta alcuna minaccia al computer. Tuttavia, quando tale file viene copiato o creato sul computer, SpIDer Guard elabora automaticamente il file come un programma malevolo e di default lo mette in Quarantena.



## 5. Strumenti

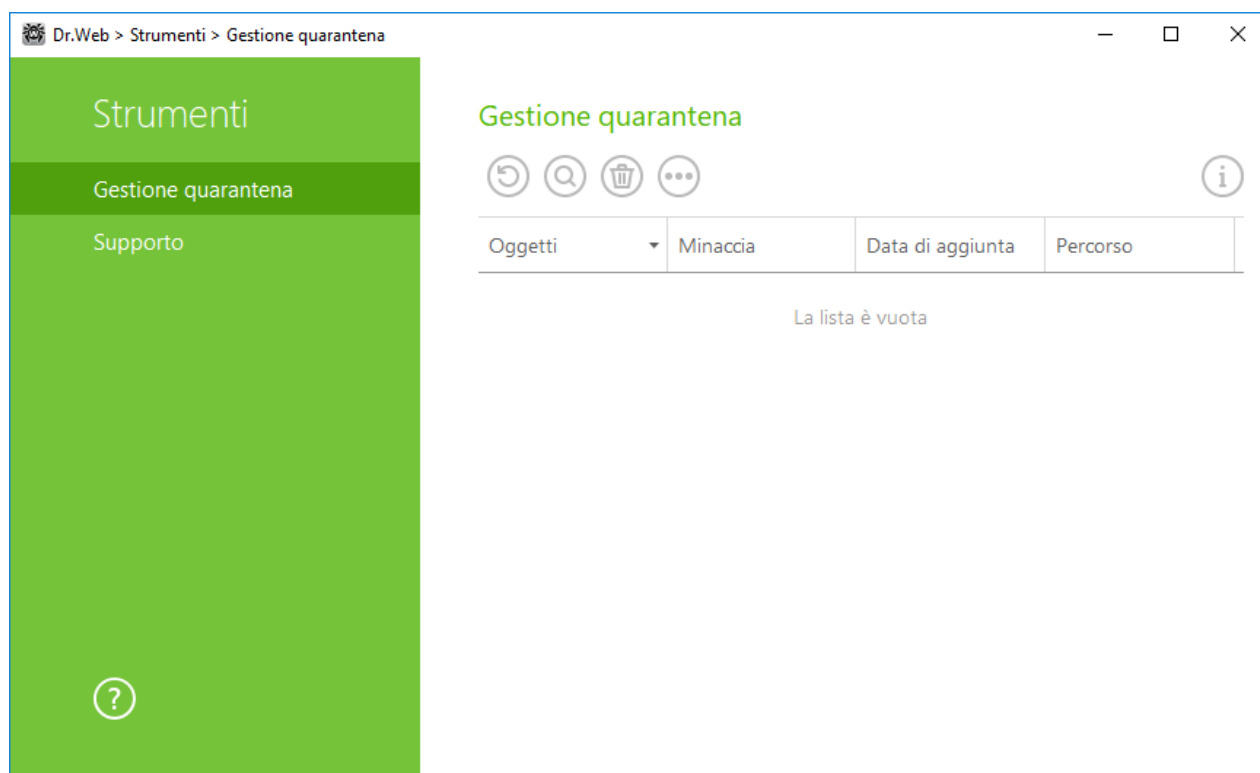
Aprire il menu Dr.Web  e avviare **Strumenti**. Affinché siano disponibili tutte le opzioni, passare a [modalità amministratore](#).

Per visualizzare la lista di file isolati e per ripristinare file da quarantena, selezionare [Gestione quarantena](#).

In caso di domande o problemi di funzionamento di Dr.Web, selezionare la sezione [Supporto](#).

### 5.1. Gestione quarantena

In questa finestra vengono riportate le informazioni sul contenuto della quarantena che serve a isolare i file sospetti per la presenza di oggetti malevoli. Inoltre, in quarantena vengono messe le copie di backup dei file processati da Dr.Web.



**Immagine 7. Oggetti in quarantena**

Nelle [impostazioni di Gestione quarantena](#) si può attivare un'opzione che definisce la modalità di isolamento degli oggetti infetti rilevati su supporti rimovibili. Se viene attivata questa opzione, tali minacce vengono messe in una cartella di quarantena sullo stesso supporto e non vengono cifrate. In tale caso la cartella di quarantena viene creata solo se il supporto è scrivibile. L'utilizzo di cartelle separate e la rinuncia alla cifratura sui supporti rimovibili consentono di prevenire l'eventuale perdita di dati.




Nella parte centrale della finestra viene visualizzata una tabella con le informazioni sullo stato della quarantena che comprende i seguenti campi:

- **Oggetti** — una lista dei nomi degli oggetti messi in quarantena;
- **Minaccia** — la classificazione del programma malevolo, determinata da Dr.Web quando l'oggetto veniva spostato in quarantena in modo automatico;
- **Data di aggiunta** — la data in cui l'oggetto è stato spostato in quarantena;
- **Percorso** — il percorso completo in cui si trovava l'oggetto prima dello spostamento in quarantena.



Nella finestra Gestione quarantena i file sono visibili solo agli utenti che hanno accesso ad essi. Per visualizzare oggetti nascosti, è necessario avere i privilegi di amministratore.

Le copie di backup messe in quarantena di default non vengono visualizzate nella tabella. Per vederle nella lista degli oggetti, premere il pulsante  e dalla lista a cascata selezionare la voce **Mostra le copie di backup**.

### Gestione degli oggetti in quarantena

In [modalità amministratore](#) per ciascun oggetto sono disponibili i seguenti pulsanti di gestione:


- **Ripristina** — per spostare uno o più oggetti selezionati sotto il nome impostato nella cartella richiesta;



Utilizzare questa funzione solo se si è certi che l'oggetto è sicuro.

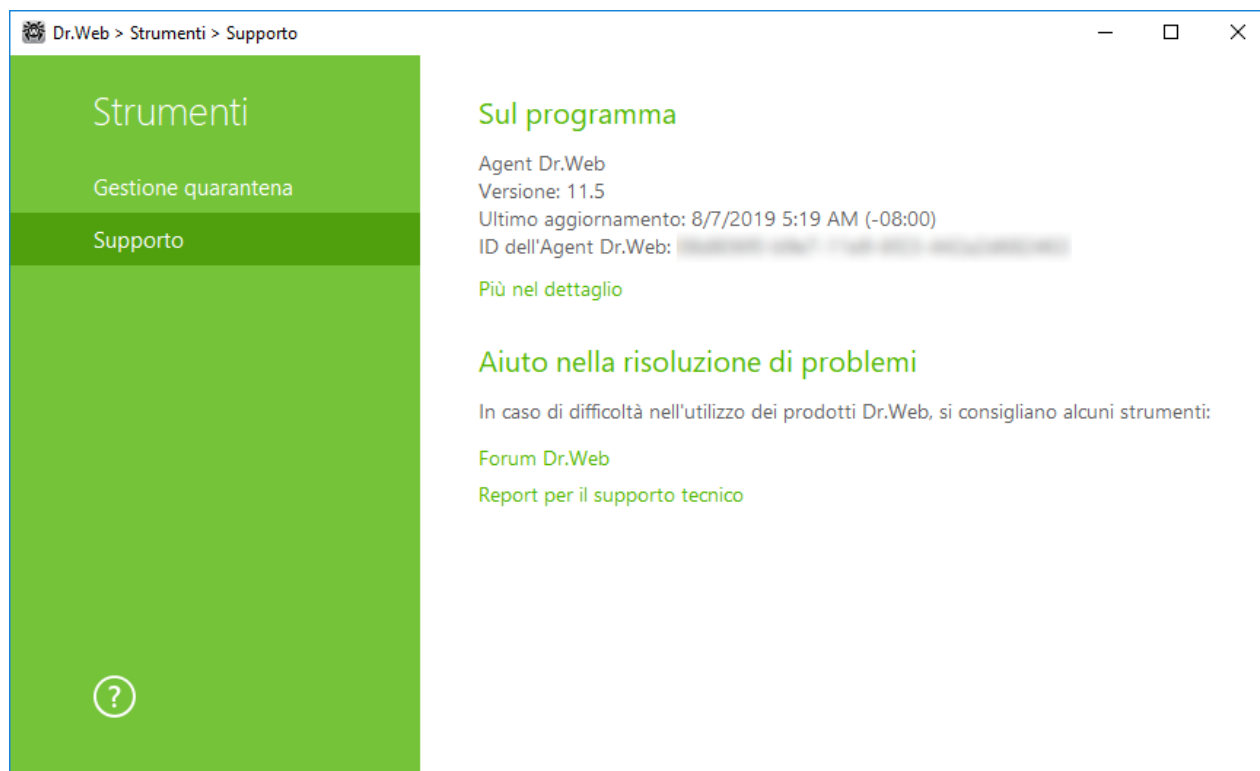
- **Ricontrolla** — per scansionare nuovamente un oggetto messo in quarantena.
- **Rimuovi** — per rimuovere uno o più oggetti selezionati da quarantena e dal sistema.

Queste azioni inoltre sono disponibili nel menu contestuale quando si fa clic con il pulsante destro del mouse su uno o più oggetti selezionati.

Per eliminare tutti gli oggetti da quarantena, premere il pulsante  e dalla lista a cascata selezionare la voce **Rimuovi tutto**.

## 5.2. Supporto

Questa sezione contiene le informazioni sulla versione del prodotto, sui componenti inclusi, sulla data dell'ultimo aggiornamento, nonché link utili che possono aiutare a trovare risposte a domande o risolvere problemi sorti nel corso del funzionamento di Dr.Web.



**Immagine 8. Informazioni sulla versione del prodotto e supporto**

Utilizzare uno dei seguenti strumenti se si hanno domande.

**Forum Dr.Web.** Apre il forum Dr.Web sull'indirizzo <https://forum.drweb.com>.

**Report per il supporto tecnico.** Avvia una procedura guidata che consente di [creare un report](#) contenente informazioni importanti circa il sistema e il funzionamento del computer.


Se il problema non è stato risolto dopo la lettura dei materiali sul forum Dr.Web, è possibile compilare un modulo web di domanda nella sezione corrispondente della pagina <https://support.drweb.com>. Alla richiesta è possibile allegare un report per il supporto tecnico, schermate e altre informazioni necessarie.

Per trovare la rappresentanza più vicina di Doctor Web e tutte le informazioni di contatto necessarie per l'utente, consultare l'indirizzo <https://company.drweb.com/contacts/moscow>.

### 5.2.1. Creazione del report

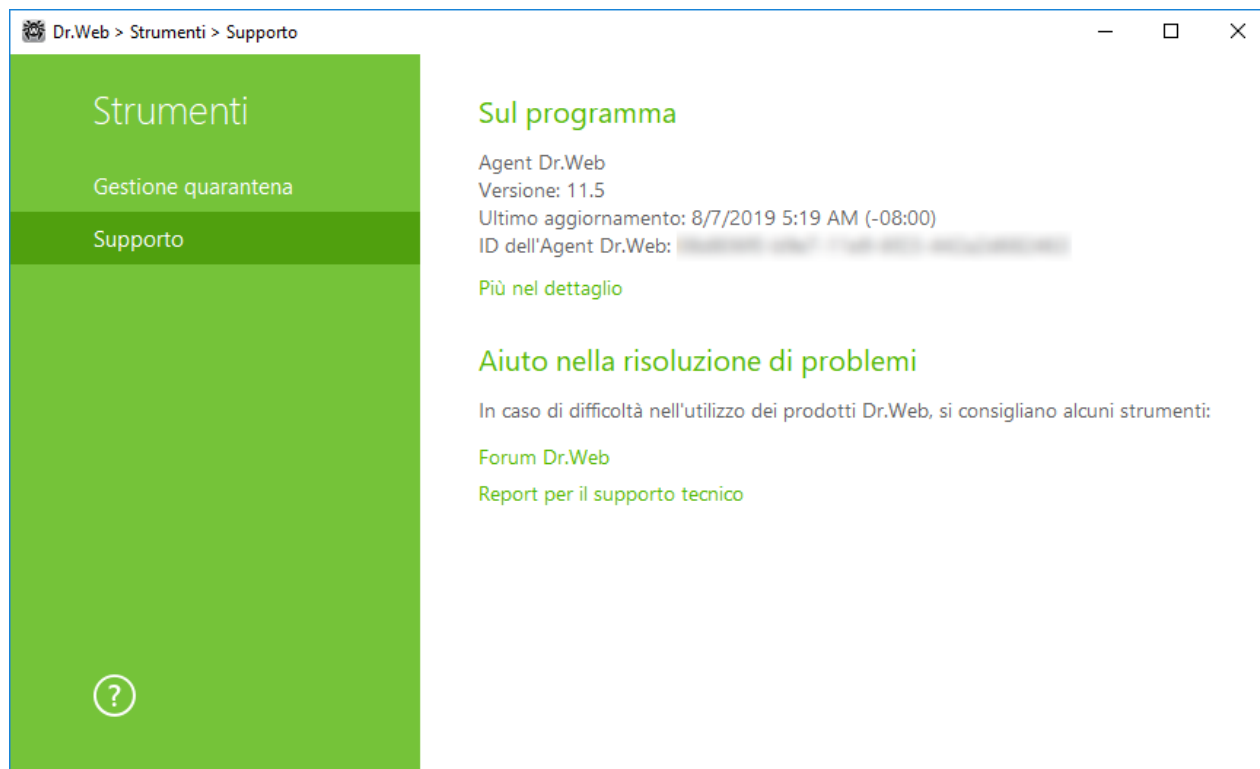
Quando si rivolge all'amministratore della rete antivirus, è possibile generare un report sul sistema operativo e sul funzionamento di Dr.Web.

#### Per creare il report

1. Aprire il menu .
2. Andare alla voce **Strumenti**.



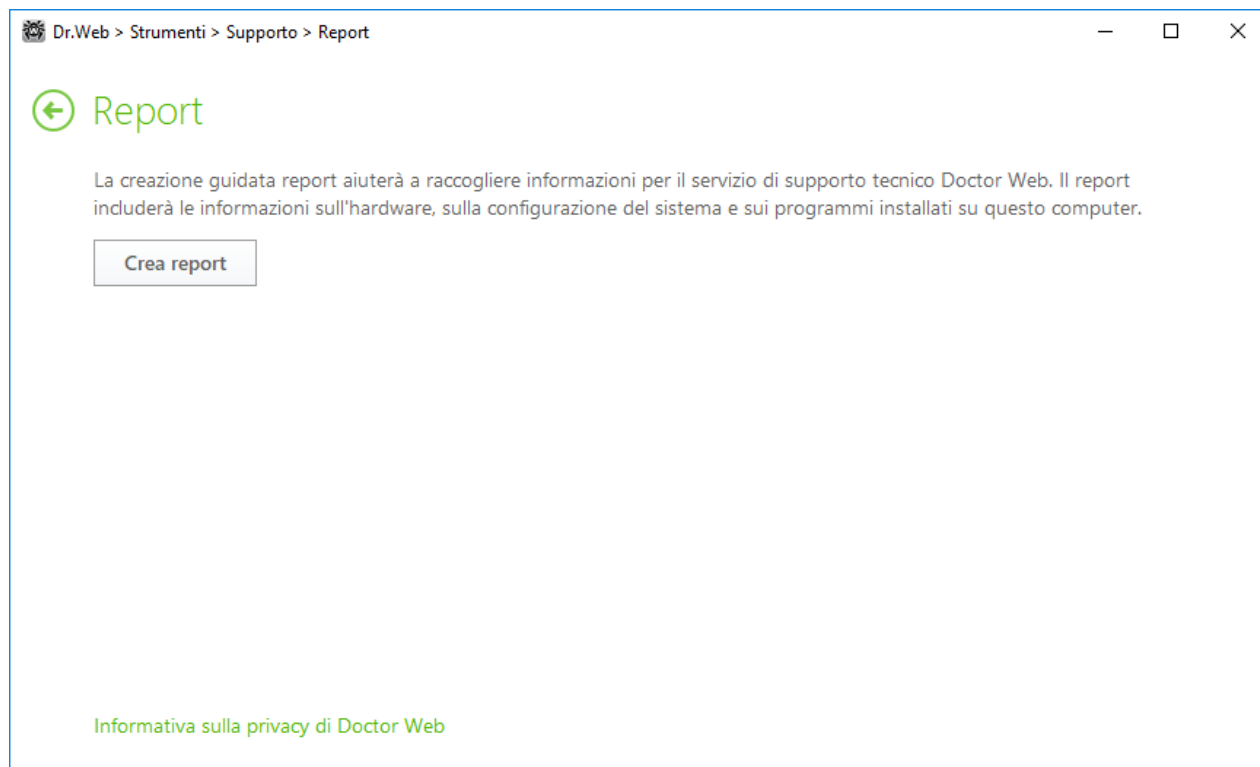
### 3. Selezionare **Supporto**.



**Immagine 9. Supporto**

### 4. Premere il link **Report per il supporto tecnico**.

### 5. Nella finestra che si è aperta premere il pulsante **Crea report**.



**Immagine 10. Creazione del report**



Il report verrà raccolto automaticamente e salvato come un archivio nella cartella Doctor Web situata nella cartella del profilo dell'utente %USERPROFILE%.

Per generare il report, premere il pulsante corrispondente. Il report includerà:

1. Informazioni tecniche sul sistema operativo:
  - informazioni generali sul computer;
  - sui processi in esecuzione;
  - sui task pianificati;
  - sui servizi, driver;
  - sul browser predefinito;
  - sulle applicazioni installate;
  - sui criteri di restrizione;
  - sul file HOSTS;
  - sui server DNS;
  - sulle registrazioni del log degli eventi di sistema;
  - un elenco delle directory di sistema;
  - i rami del registro;
  - i provider Winsock;
  - le connessioni di rete;
  - i report del programma debug Dr.Watson;
  - l'indice di prestazioni.
2. Informazioni sulle Soluzioni antivirus Dr.Web.
3. Informazioni sui plugin Dr.Web:
  - Dr.Web per IBM Lotus Domino;
  - Dr.Web per Kerio MailServer;
  - Dr.Web per Kerio WinRoute.

Informazioni sul funzionamento dei Prodotti antivirus Dr.Web sono locate nel Log degli eventi del sistema operativo Windows, nella sezione **Log delle applicazioni e dei servizi di** → **Doctor Web**.

### Creazione del report dalla riga di comando

Per generare un report, utilizzare il seguente comando:

```
/auto
```

Per esempio: dwsysinfo.exe /auto

Il report verrà salvato come un archivio nella cartella Doctor Web situata nella cartella del profilo dell'utente %USERPROFILE%.





Inoltre è possibile utilizzare il comando:

```
/auto/report : [<percorso completo dell'archivio>]
```

dove:

- <percorso completo dell'archivio> — percorso del file di report.

Per esempio: `dwsysinfo.exe /auto /report:C:\report.zip`



## 6. Scanner Dr.Web

Scanner Dr.Web per Windows è progettato per la scansione antivirus dei settori di avvio, della memoria, nonché di singoli file e di oggetti inclusi in strutture composte (archivi compressi, container di file, email con allegati). La scansione viene eseguita con l'utilizzo di tutti i [metodi di rilevamento](#) delle minacce.

Se rileva un oggetto malevolo, Scanner Dr.Web solo avvisa della minaccia. Il report sui risultati della scansione viene riportato in una tabella in cui è possibile selezionare l'azione desiderata per processare l'oggetto rilevato malevolo o sospetto. È possibile applicare le azioni predefinite a tutte le minacce rilevate o selezionare un metodo di processamento desiderato per singoli oggetti.


Le azioni predefinite sono ottimali per la maggior parte degli usi, ma se necessario, è possibile modificarle nella [finestra di configurazione](#) dei parametri di funzionamento di Scanner Dr.Web. Mentre l'azione per un singolo oggetto può essere selezionata dopo la fine di una scansione, le impostazioni generali per la neutralizzazione di tipi di minacce specifiche devono essere configurate prima dell'inizio della scansione.

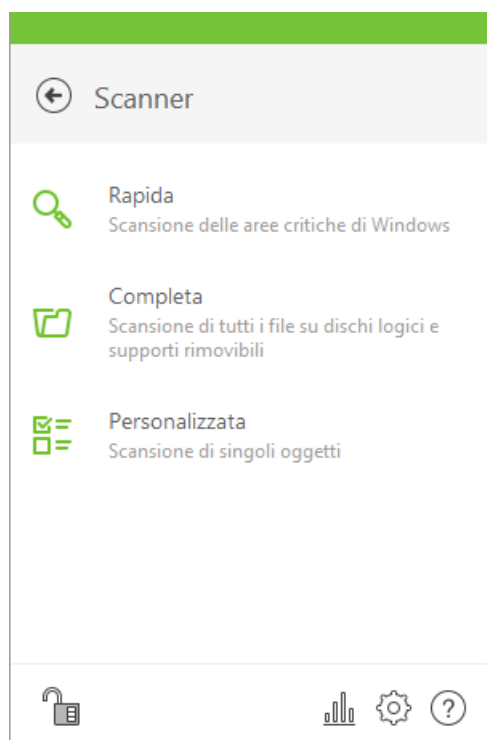
### 6.1. Avvio della scansione e le modalità di scansione



Se si usano i sistemi operativi Windows Vista, Windows Server 2003 e superiori, è consigliabile avviare Scanner Dr.Web con i permessi di amministratore. Altrimenti, non verranno controllati i file e le cartelle a cui un utente senza permessi di amministratore non può accedere (comprese le cartelle di sistema).

#### Avvio di Scanner Dr.Web

1. Nel [menu](#)  selezionare la voce **Scanner**. Si apre un menu per l'accesso rapido all'avvio di diversi tipi di scansione.



**Immagine 11. Selezione della modalità di scansione dello scanner**

2. Selezionare la modalità di scansione richiesta:

- la voce **Personalizzata** per verificare i soli oggetti specificati dall'utente. Si apre la finestra di selezione dei file da verificare tramite Scanner Dr.Web;
- la voce **Rapida** per verificare le sole aree critiche di Windows;
- la voce **Completa** per verificare tutti i file.

Per avviare Scanner con le impostazioni predefinite per verificare un file o una directory specifica, selezionare nel menu contestuale dell'icona del file o della directory (sul Desktop o nell'Esplora risorse del sistema operativo Windows) la voce **Scansiona tramite Dr.Web**.

### Configurazione di Scanner Dr.Web

È possibile configurare i parametri di funzionamento, nonché le reazioni di Scanner Dr.Web alle minacce rilevate nella sezione **Impostazioni** → **Componenti di protezione** → **Scanner**.

## Descrizione delle modalità di scansione

### Scansione rapida

In questa modalità vengono controllati i seguenti oggetti:

- settori di avvio di tutti i dischi;
- memoria operativa;
- cartella principale del disco di avvio;



- cartella di sistema di Windows;
- cartella Documenti;
- file temporanei;
- punti di ripristino del sistema;
- ricerca dei rootkit (se il processo di scansione è stato avviato dall'account amministratore).




Gli archivi compressi e i file di email non vengono controllati in questa modalità.

### Scansione completa

In questa modalità viene eseguita una scansione completa della memoria operativa e di tutti i dischi rigidi (compresi i settori di avvio), nonché viene controllata la presenza di rootkit.

### Scansione personalizzata

Se si seleziona questa modalità, nella finestra di Scanner Dr.Web si impostano gli oggetti da verificare: qualsiasi file e cartella, nonché gli oggetti quale la memoria operativa, i settori di avvio ecc. Per iniziare la verifica degli oggetti selezionati, premere il pulsante **Avvia la scansione**. Per aggiungere oggetti alla lista, premere il pulsante .

### Processo di scansione

Dopo l'inizio della scansione, nella parte destra della finestra diventano disponibili i pulsanti **Pausa** e **Stop**. In qualsiasi fase della scansione sono possibili le seguenti operazioni:

- Per sospendere la scansione, premere il pulsante **Pausa**. Per riprendere la scansione dopo una pausa, premere il pulsante **Riprendi**.
- Per interrompere completamente la scansione, premere il pulsante **Stop**.

Da questa finestra è possibile tornare alla finestra di selezione della modalità di scansione.



Il pulsante **Pausa** non è disponibile durante la scansione della memoria operativa e dei processi.

## 6.2. Azioni in caso di rilevamento delle minacce

Dopo la fine di una scansione Scanner Dr.Web solo informa delle minacce rilevate e offre di applicarci le azioni di neutralizzazione più ottimali. È possibile neutralizzare contemporaneamente tutte le minacce rilevate. Per farlo, dopo la fine della scansione selezionare tutte le minacce e premere il pulsante **Neutralizza**, e Scanner Dr.Web applicherà le azioni ottimali predefinite a tutte le minacce rilevate.



Premuto il pulsante **Neutralizza**, le azioni vengono applicate agli oggetti selezionati nella tabella. È necessario selezionare manualmente oggetti o gruppi di oggetti specifici a cui si vuole applicare azioni dopo che viene premuto il pulsante **Neutralizza**. A tale scopo utilizzare i flag accanto ai nomi degli oggetti o il menu a cascata nell'intestazione della tabella.

## Scelta dell'azione

1. Nel campo **Azione** nella lista a cascata selezionare l'azione desiderata per ciascun oggetto (di default Scanner Dr.Web offre il valore ottimale).
2. Premere il pulsante **Neutralizza**. Scanner Dr.Web neutralizzerà contemporaneamente tutte le minacce selezionate.

Esistono le seguenti limitazioni:

- non è possibile curare oggetti sospetti;
- non è possibile spostare o rimuovere gli oggetti che non sono file (per esempio settori di avvio);
- non è possibile applicare qualsiasi azione a singoli file situati all'interno degli archivi compressi, dei pacchetti di installazione o inclusi come parte delle email — l'azione in tali casi viene applicata soltanto a tutto l'oggetto per intero.

Di default un report sul funzionamento del programma dettagliato viene salvato nel file di log `dwscanner.log` situato nella cartella `%USERPROFILE%\Doctor Web`.

| Nome di colonna | Descrizione   |
|-----------------|---|
| Oggetto         | In questa colonna è indicato il nome dell'oggetto infetto o sospetto (nome di file — se è infetto un file, <b>Boot sector</b> se è infetto un settore di avvio, <b>Master Boot Record</b> se è infetto l'MBR di un disco rigido).   |
| Minaccia        | In questa colonna è indicato il nome del virus o della variante del virus secondo la classificazione interna di Doctor Web (variante di un virus conosciuto è un codice ottenuto tramite una modifica del virus conosciuto, in questo caso viene riconosciuto dallo scanner, ma ad esso non possono essere applicati gli algoritmi di cura studiati per il virus originale). In caso degli oggetti sospetti viene indicato che l'oggetto "è probabilmente infetto" e viene indicato il tipo di possibile virus secondo la classificazione dell'analisi euristica. |
| Azione          | In questa colonna è indicata l'azione raccomandata per la minaccia trovata. Premere la freccia su questo pulsante per impostare un'azione per la minaccia selezionata.<br><br>È possibile applicare l'azione indicata sul pulsante separatamente senza neutralizzare le altre minacce. Per farlo premere questo pulsante.   |
| Percorso        | In questa colonna è indicato il percorso completo del file corrispondente.  |



Se nelle [impostazioni](#) di Scanner Dr.Web è stata selezionata la voce **Neutralizza le minacce rilevate** per l'impostazione **Al termine della scansione**, la neutralizzazione delle minacce verrà eseguita in maniera automatica.

### 6.3. Avvio dello Scanner con i parametri della riga di comando

È possibile avviare Scanner Dr.Web in modalità a riga di comando. Tale modo permette di configurare come parametri di avvio le impostazioni aggiuntive della sessione di scansione corrente e una lista di oggetti da scansionare.

La sintassi del comando di avvio è la seguente:

```
[<percorso_del_programma>] dwscanner [<opzioni>] [<oggetti>]
```

La lista degli oggetti di scansione può essere vuota o contenere diversi elementi separati da spazi. Se il percorso degli oggetti di scansione non è indicato, la ricerca viene eseguita nella cartella di installazione di Dr.Web.

Le seguenti varianti di indicazione degli oggetti di scansione sono le più comuni:

- /FAST — esegui una [scansione rapida](#) del sistema.
- /FULL — esegui una [scansione completa](#) di tutti i dischi rigidi e supporti rimovibili (compresi i settori di avvio).
- /LITE — esegui una scansione iniziale del sistema con cui vengono controllati la memoria operativa e i settori di avvio di tutti i dischi, inoltre esegui una verifica della presenza di rootkit.

Parametri — opzioni della riga di comando che configurano le impostazioni del programma. Se non sono presenti, la scansione viene eseguita con le impostazioni salvate in precedenza (o con le impostazioni predefinite, se non sono state modificate). Le opzioni iniziano con il carattere "/" e, come gli altri parametri della riga di comando, vengono separate da spazi.

### 6.4. Scanner console

La lista dei componenti Dr.Web include anche Scanner console che consente di eseguire le scansioni in modalità a riga di comando, e inoltre fornisce ampie possibilità di configurazione.



I file in cui si sospetta la presenza di oggetti malevoli vengono messi da Scanner console in Quarantena.

Per avviare Scanner console, utilizzare il seguente comando:

```
[<percorso_del_programma>] dwscancl [<opzioni>] [<oggetti>]
```



Un'opzione inizia con il carattere "/", più opzioni vengono separate da spazi. La lista degli oggetti di scansione può essere vuota o contenere diversi elementi separati da spazi.

La lista delle opzioni di Scanner console è contenuta in [Allegato A](#).

Codici di output:

0 — la scansione è stata completata con successo, nessun oggetto infetto è stato trovato

1 — la scansione è stata completata con successo, sono stati trovati degli oggetti infetti

10 — sono impostate delle opzioni non valide

11 — il file della chiave non è stato trovato oppure non supporta Scanner console

12 — Scanning Engine non è in esecuzione

255 — la scansione è stata interrotta dall'utente

## 6.5. Avvio della scansione secondo il calendario

Quando Dr.Web viene installato, in Utilità di pianificazione standard di Windows viene creato automaticamente un task di scansione antivirus (di default è disattivato).

Per visualizzare i parametri del task, aprire **Pannello di controllo** (visualizzazione avanzata) → **Amministrazione** → **Utilità di pianificazione**.

Nella lista dei task selezionare il task di scansione antivirus. È possibile attivare il task, nonché configurare l'ora di avvio della scansione e impostare i parametri richiesti.

Nella parte inferiore della finestra nella scheda **Generali** vengono indicate informazioni generali sul task e le impostazioni di sicurezza. Nelle schede **Trigger** e **Condizioni** vengono indicate diverse condizioni in cui il task viene avviato. Si può visualizzare la cronologia degli eventi nella scheda **Log**.



Inoltre, si possono creare dei task di scansione antivirus personalizzati. Per maggiori informazioni sull'utilizzo del calendario di sistema consultare la guida e la documentazione del sistema operativo Windows.



Se tra i componenti installati c'è Firewall, dopo l'installazione del programma Dr.Web e il primo riavvio il servizio dell'utilità di pianificazione verrà bloccato da Firewall. Il componente **Attività pianificate** sarà operativo solo dopo il secondo riavvio in quanto a quel punto una relativa regola sarà già creata.



## 7. Impostazioni

Per accedere alle impostazioni, aprire il menu Dr.Web  e avviare le **Impostazioni**  in [modalità amministratore](#).

### Protezione con password

Per limitare l'accesso alle impostazioni Dr.Web sul computer, attivare l'opzione **Proteggi da password le impostazioni Dr.Web**. Nella finestra che si è aperta impostare una password che verrà richiesta quando si accede alle impostazioni Dr.Web, confermare la password e premere il pulsante **OK**.



Se si è dimenticata la password delle impostazioni del prodotto, rivolgersi all'amministratore della rete antivirus.





## 8. Impostazioni principali

Il centro unico di gestione delle impostazioni consente di impostare i parametri di funzionamento generali dell'complesso antivirus.

Per accedere alle impostazioni principali di Dr.Web, aprire il menu , avviare **Impostazioni**  in [modalità amministratore](#) e selezionare la sezione **Principali**.



La modifica delle impostazioni principali è possibile se è stata autorizzata dall'amministratore del server di protezione centralizzata a cui si connette Dr.Web.

Per l'accesso alle impostazioni principali di Dr.Web viene richiesta la password se nella sezione [Impostazioni](#) è stata attivata l'opzione **Proteggi da password le impostazioni Dr.Web**.

Per configurare la visualizzazione degli avvisi sullo schermo, selezionare la sezione [Avvisi](#).

Per configurare i parametri di sicurezza aggiuntivi, selezionare la sezione [Auto-protezione](#).

Per limitare l'accesso a determinate classe di dispositivi o bus, selezionare la sezione [Dispositivi](#).


Per modificare la lingua dell'interfaccia, nonché i parametri del log e della quarantena, selezionare [Avanzate](#).

Per configurare i parametri di connessione al server di protezione centralizzata, selezionare [Server](#).

### 8.1. Avvisi

In questa sezione è possibile configurare la ricezione degli avvisi sul funzionamento di Agent Dr.Web.

#### Avvisi visualizzati sullo schermo

Attivare l'opzione corrispondente per ricevere i suggerimenti-avvisi sotto forma di una finestra pop-up sopra l'icona Dr.Web  nell'area di notifica di Windows.

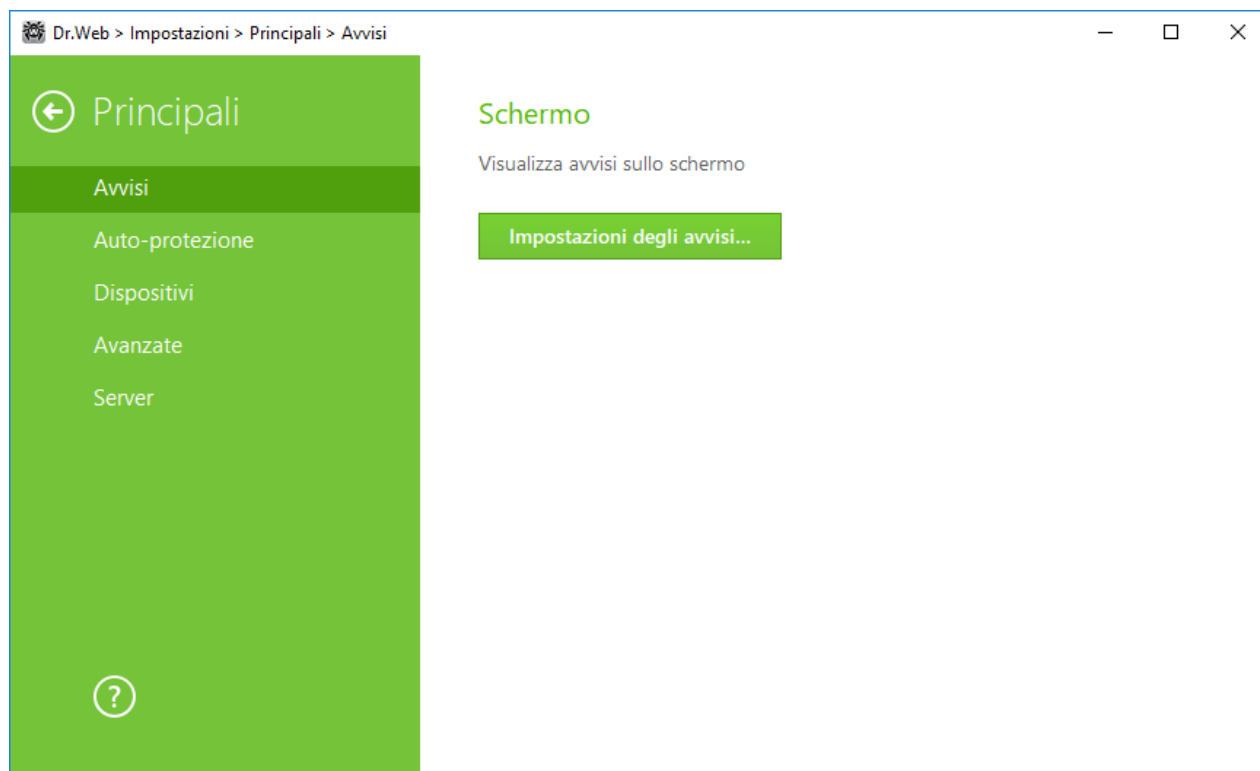


Immagine 12. Impostazioni di avvisi

### Impostazioni degli avvisi

1. Premere il pulsante **Impostazioni degli avvisi**.
2. Selezionare gli avvisi che si desidera ricevere. Per visualizzare gli avvisi, spuntare i flag di fronte ai tipi di avvisi richiesti. Se non si desidera ricevere gli avvisi di eventi, deselezionare i flag.

| Tipo di avviso                | Descrizione  |
|-------------------------------|--|
| È stata rilevata una minaccia | Avvisi sulle minacce rilevate dai componenti SpIDer Guard e SpIDer Gate.<br>Di default gli avvisi sono attivati.   |
| Avvisi critici                | Avvisi critici sui seguenti eventi: <ul style="list-style-type: none"><li>• sono state rilevate connessioni che aspettano una risposta di Firewall;</li><li>• il login e la password sono già utilizzati per la connessione al server di protezione centralizzata.</li></ul> Di default gli avvisi sono attivati.                                  |
| Avvisi importanti             | Avvisi importanti sui seguenti eventi: <ul style="list-style-type: none"><li>• il tempo di utilizzo del computer è scaduto;</li><li>• il dispositivo è bloccato;</li><li>• è stato impedito un tentativo di modifica della data e dell'ora di sistema;</li><li>• l'accesso all'oggetto protetto è bloccato dalla Protezione preventiva.;</li></ul> |



| Tipo di avviso   | Descrizione  |
|------------------|--|
|                  | <ul style="list-style-type: none"><li>• i database dei virus sono obsoleti (quando si lavora in Modalità mobile).</li></ul> Di default gli avvisi sono attivati.   |
| Avvisi secondari | Avvisi secondari sui seguenti eventi: <ul style="list-style-type: none"><li>• un aggiornamento riuscito;</li><li>• errore di aggiornamento;</li><li>• il tempo di utilizzo del web è scaduto;</li><li>• URL bloccato dal modulo Office control;</li><li>• URL bloccato da SpIDer Gate;</li><li>• l'accesso all'oggetto protetto è bloccato dal modulo Office control;</li><li>• l'amministratore della rete antivirus ha avviato il processo di scansione del computer;</li><li>• il processo di scansione del computer è stato avviato secondo il calendario;</li><li>• la scansione del computer è completata.</li></ul> Di default gli avvisi sono disattivati. |

3. Se necessario, impostare i parametri aggiuntivi di visualizzazione degli avvisi sullo schermo:

| Flag  | Descrizione  |
|---|--|
| Non visualizzare avvisi in modalità a schermo intero                                    | Avvisi durante l'utilizzo di applicazioni in modalità a schermo intero (visualizzazione di film, immagini ecc.).<br>Deselezionare questo flag per ricevere avvisi sempre.  |
| Visualizza gli avvisi del Firewall su uno schermo separato in modalità a schermo intero | Visualizzazione degli avvisi da Firewall su un desktop separato durante il funzionamento di applicazioni in modalità a schermo intero (giochi, video).<br>Deselezionare questo flag affinché gli avvisi vengano visualizzati sullo stesso desktop su cui è in esecuzione un'applicazione in modalità a schermo intero. |



Gli avvisi circa alcuni eventi non rientrano nei gruppi sopraelencati e vengono sempre visualizzati all'utente:

- installazione degli aggiornamenti critici per cui è necessario riavviare il computer;
- riavvio del computer per completare la neutralizzazione delle minacce;
- riavvio del computer per attivare/disattivare l'hypervisor;
- una richiesta per consentire a un processo di modificare un oggetto;
- un messaggio inviato dall'amministratore del server di protezione centralizzata.



## 8.2. Auto-protezione

In questa sezione è possibile configurare la protezione attraverso cui Dr.Web protegge sé stesso da influenze non autorizzate, per esempio da parte dei programmi la cui attività malevola è mirata ai programmi antivirus, nonché da danneggiamenti accidentali.

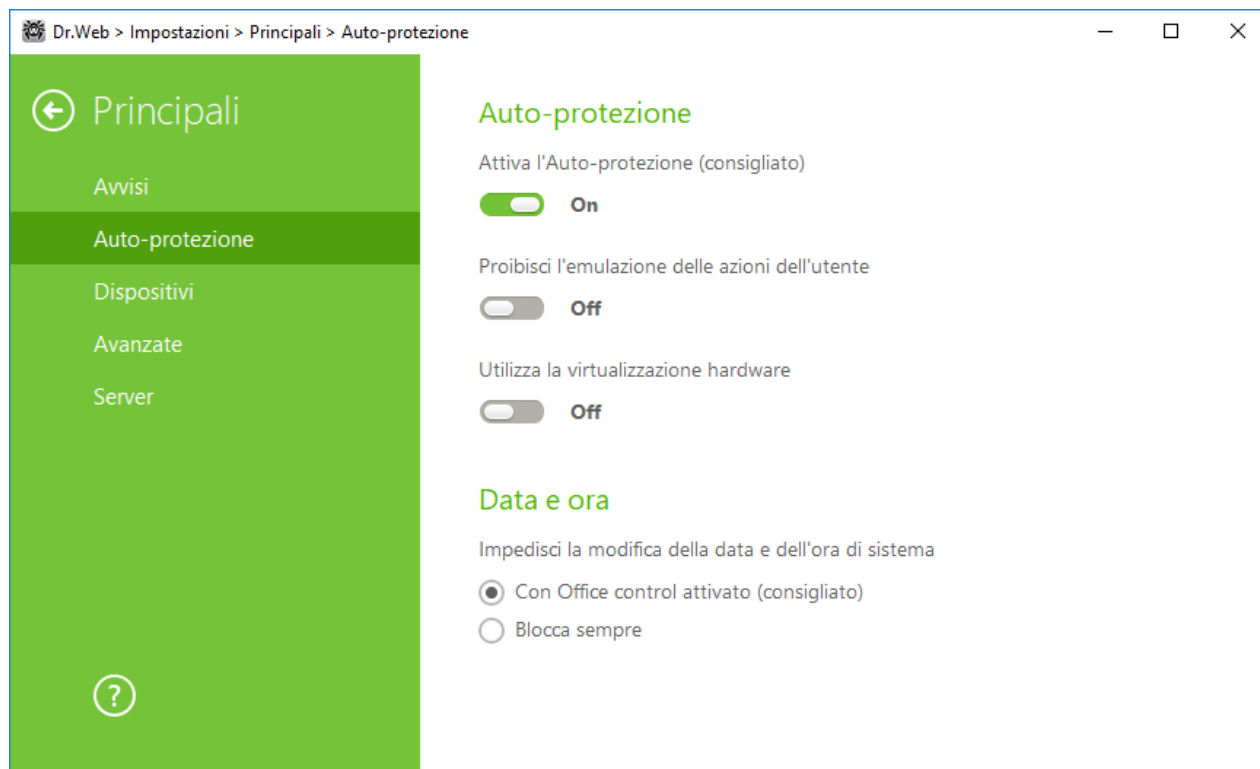


Immagine 13. Parametri di protezione Dr.Web

### Auto-protezione

L'impostazione **Attiva l'Auto-protezione (consigliato)** consente di proteggere i file e processi di Dr.Web da accessi non autorizzati. Non è consigliabile disattivare l'auto-protezione.



In caso di problemi con l'uso dei programmi di deframmentazione, è consigliabile disattivare temporaneamente il modulo di Auto-protezione.

Per eseguire un ritorno a un punto di ripristino di sistema, è necessario disattivare il modulo di Auto-protezione.

L'impostazione **Proibisci l'emulazione delle azioni dell'utente** consente di prevenire le modifiche nelle impostazioni Dr.Web, eseguite dai software di terze parti. Tra le altre cose, sarà proibita l'esecuzione degli script che emulano il funzionamento della tastiera e del mouse nelle finestre Dr.Web (per esempio script per la modifica delle impostazioni Dr.Web, per la rimozione della licenza e per le altre operazioni finalizzate a modificare il funzionamento di Dr.Web).



L'impostazione **Utilizza la virtualizzazione hardware** consente di utilizzare più possibilità del computer per il rilevamento e la cura delle minacce, nonché per rafforzare l'auto-protezione di Dr.Web. Affinché venga attivata questa opzione, sarà necessario un riavvio del computer.



La virtualizzazione hardware funziona solo se le caratteristiche hardware del computer e il sistema operativo supportano la virtualizzazione hardware.

L'attivazione di questa opzione può causare un conflitto di compatibilità con software di terze parti.

In caso di problemi, disattivare questa opzione.

---

La virtualizzazione hardware non è supportata nei sistemi operativi a 32 bit.

## Data e ora

Alcuni programmi malevoli modificano deliberatamente la data e l'ora di sistema. In questo caso, i database dei virus del programma antivirus non vengono aggiornati secondo il calendario impostato, la licenza può essere identificata come scaduta, e i componenti di protezione verranno disabilitati.

L'impostazione **Impedisci la modifica della data e dell'ora di sistema** consente di bloccare la modifica manuale e automatica della data e dell'ora di sistema, nonché del fuso orario. Questa limitazione viene impostata per tutti gli utenti del sistema. Questa impostazione rende più precisa [la funzione di limitazione di tempo](#) nel modulo Office control. Se nel modulo Office control sono impostate delle limitazioni al tempo di utilizzo del computer o della rete Internet, questa impostazione si attiva automaticamente. Si può configurare la [ricezione degli avvisi](#) per il caso in cui viene fatto un tentativo di modifica dell'ora di sistema.

## 8.3. Dispositivi

In questa sezione è possibile limitare l'accesso a determinati dispositivi o bus di dispositivo e configurare la black list e white list.



Le impostazioni di accesso ai dispositivi vengono applicate a tutti gli account di Windows.

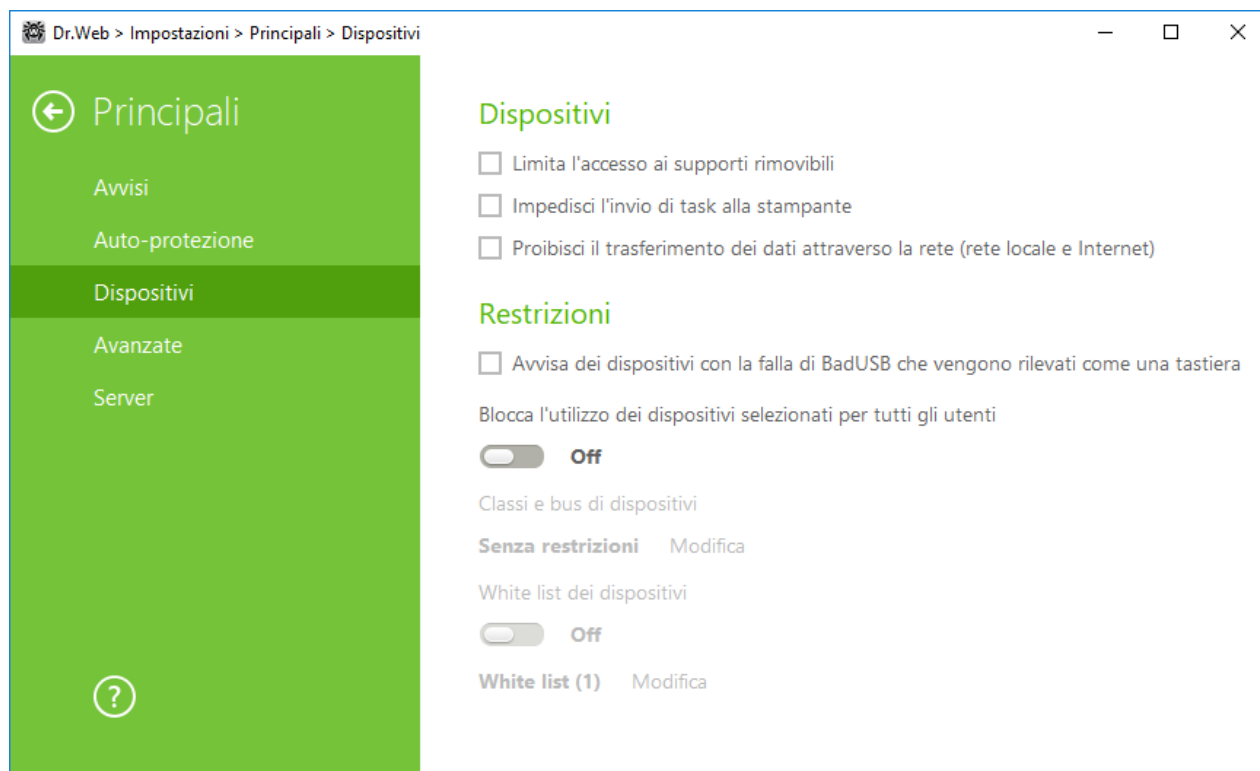


Immagine 14. Impostazioni di blocco dei dispositivi

## Dispositivi

Per bloccare l'accesso ai dati sui supporti rimovibili (chiavi USB, dischetti, unità CD/DVD, dischi ZIP ecc.), attivare l'opzione corrispondente. Per vietare di trasmettere task di stampa, attivare l'opzione **Impedisci l'invio di task alla stampante**. Di default l'opzione è disattivata. Inoltre, è possibile vietare la trasmissione di dati attraverso reti locali e Internet.

Alcuni dispositivi USB infetti possono essere riconosciuti dal computer come una tastiera. Affinché Dr.Web verifichi se un dispositivo collegato è veramente una tastiera, attivare l'opzione **Avvisa dei dispositivi con la falla di BadUSB che vengono rilevati come una tastiera**.



## Classi e bus di dispositivi

Questa funzione permette di bloccare una o più classi di dispositivi su tutti i bus e inoltre di bloccare tutti i dispositivi collegati a uno o più bus. Le classi di dispositivi sono dispositivi che svolgono funzioni uguali (per esempio, i dispositivi per la stampa). I bus sono sottosistemi di trasmissione di dati tra i blocchi funzionali del computer (per esempio, il bus USB).




Per bloccare l'accesso alle classi e ai bus di dispositivi selezionati, attivare l'opzione corrispondente. Creare una lista di tali oggetti, premendo il pulsante **Modifica**. Nella finestra che si è aperta è possibile selezionare le classi e i bus di dispositivi, l'accesso a cui si vuole bloccare.



### Creazione della lista delle classi di dispositivi bloccate

1. Per bloccare completamente una classe di dispositivi, nella colonna **Classi da bloccare** premere il pulsante .
2. Nella lista che si è aperta selezionare le classi richieste e premere **OK**. Le classi di dispositivi selezionate verranno bloccate su tutti i bus. Nella lista di selezione delle classi di dispositivi vengono visualizzate solo le classe non bloccate.
3. Per sbloccare una classe di dispositivi, nella finestra **Classi e bus di dispositivi** selezionare la classe richiesta e premere il pulsante .

### Creazione della lista dei bus di dispositivi bloccati

1. Per bloccare un bus completamente o per bloccare alcuni dispositivi sul bus, nella colonna **Bus da bloccare** premere il pulsante .
2. Nella finestra che si è aperta selezionare le classi di dispositivi richieste. Per bloccare l'intero bus selezionare tutte le classi dalla lista. Premere **OK**.
3. Per sbloccare un bus, nella finestra **Classi e bus di dispositivi** selezionare il bus richiesto e premere il pulsante .
4. Per modificare una lista delle classi bloccate su uno specifico bus, premere il pulsante .




Quando viene attivato il blocco di un dispositivo già collegato, è necessario o collegare il dispositivo nuovamente, o riavviare il computer. Il blocco funziona solo per i dispositivi che vengono collegati dopo l'attivazione della funzione.





### White list dei dispositivi

Se è stato limitato l'accesso a qualche classe o bus di dispositivi, è possibile consentire separatamente l'accesso a determinati dispositivi aggiungendoli alla white list. Inoltre, è possibile aggiungere alla white list uno specifico dispositivo in modo da non verificare su di esso la presenza della vulnerabilità BadUSB.

### Aggiunta di un dispositivo alla white list

1. Attivare l'opzione **White list dei dispositivi** (questa opzione diventa attiva se sono state impostate delle restrizioni).
2. Per creare una lista dei dispositivi, premere il pulsante **Modifica**.
3. Assicurarsi che il dispositivo sia collegato al computer.
4. Premere il pulsante . Nella finestra che si è aperta premere il pulsante **Sfoglia** e selezionare il dispositivo richiesto. Utilizzare un filtro affinché nella tabella vengano visualizzati solo i dispositivi collegati o solo quelli scollegati. Premere il pulsante **OK**.



5. Per i dispositivi con un file system è possibile configurare regole di accesso. Per farlo, nella colonna **Regola** selezionare una delle modalità: **Consenti tutto** o **Sola lettura**. Per aggiungere una nuova regola per uno specifico utente, premere il pulsante . Per eliminare una regola, premere .
6. Per salvare le modifiche, premere **OK**. Per uscire dalla finestra senza salvare le modifiche, premere **Annulla** Si ritorna alla white list dei dispositivi.
7. Per modificare un set di regole per un dispositivo, selezionarlo nella lista e premere .
8. Per eliminare un set di regole per un dispositivo, selezionarlo nella lista e premere .

## 8.4. Avanzate

In questa sezione si configurano la lingua del programma, i parametri del log e della Quarantena.

È possibile selezionare la lingua del programma da una lista a cascata. La lista delle lingue si integra automaticamente e contiene tutte le localizzazioni, disponibili al momento, dell'interfaccia grafica di Dr.Web.

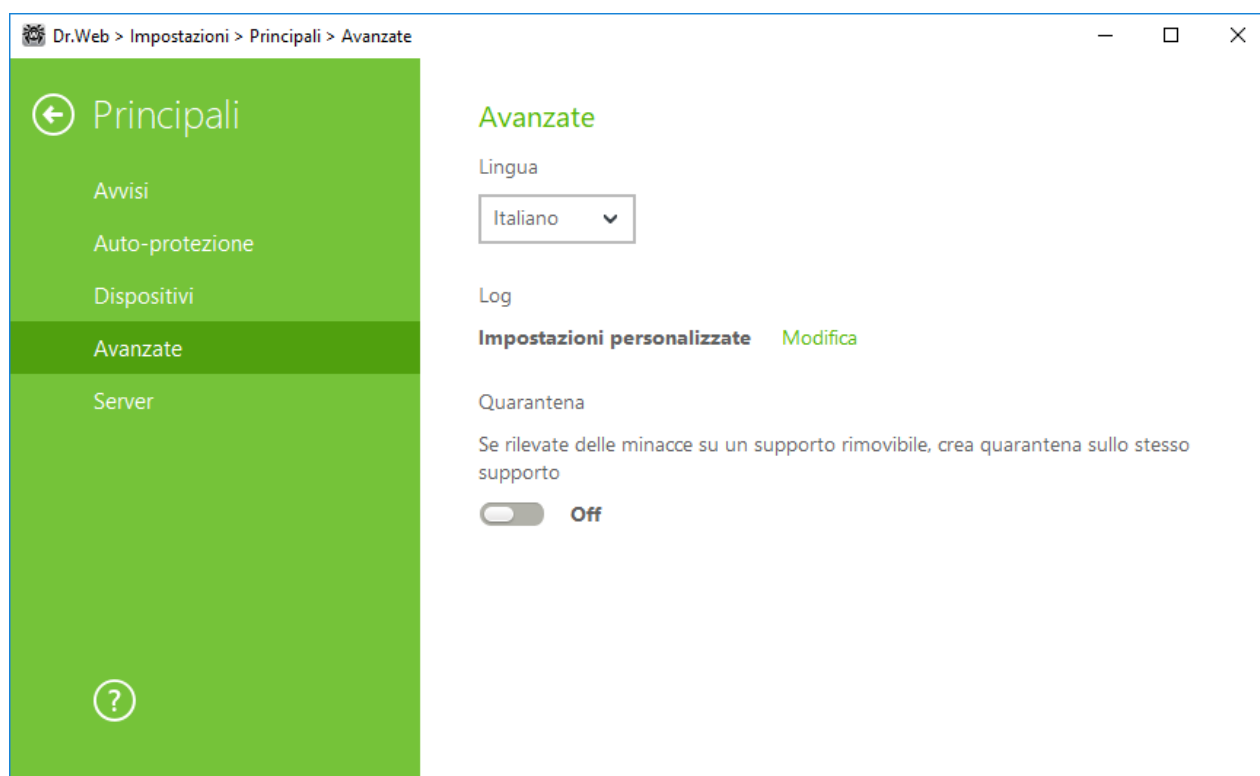


Immagine 15. Impostazioni avanzate

### Impostazioni del Log

Per gestire le impostazioni del log, premere il relativo pulsante **Modifica**.





Non è possibile modificare le impostazioni di log se l'amministratore del server di protezione centralizzata a cui si connette Dr.Web non ha autorizzato l'uso di tali operazioni.

Di default i file di log hanno una dimensione limitata pari a 10 MB (per il componente SplDer Guard — 100 MB). Se eccede la dimensione massima, il file di log viene troncato fino alla:

- dimensione impostata se le informazioni registrate durante la sessione non eccedono la dimensione consentita;
- dimensione della sessione corrente se le informazioni registrate durante la sessione eccedono la dimensione consentita.

Di default per tutti i componenti di Dr.Web il log viene registrato in modalità standard in cui vengono registrate le seguenti informazioni:

| Componente   | Informazione  |
|--------------|---|
| SplDer Guard | <p>Aggiornamenti, avvio e arresto del monitor SplDer Guard, eventi di virus, dati sui file controllati, sui nomi dei packer e sui contenuti degli oggetti composti (archivi compressi, file di email o container di file).</p> <p>È consigliabile utilizzare questa modalità per determinare gli oggetti che il monitor SplDer Guard controlla più spesso. Se necessario, si possono aggiungere tali oggetti alla lista delle <a href="#">eccezioni</a>, il che può ridurre il carico di lavoro del computer.</p> |
| SplDer Mail  | <p>Aggiornamenti, avvio e arresto del monitor di posta SplDer Mail, eventi di virus, parametri di intercettazione delle connessioni, nonché dati sui file controllati, sui nomi dei packer e sui contenuti degli archivi compressi.</p> <p>È consigliabile utilizzare questa modalità per controllare le impostazioni di intercettazione delle connessioni con i server di posta.</p>   |
| SplDer Gate  | <p>Aggiornamenti, avvio e arresto del monitoraggio HTTP SplDer Gate, eventi di virus, parametri di intercettazione delle connessioni, nonché dati sui file controllati, sui nomi dei packer e sui contenuti degli archivi compressi.</p> <p>È consigliabile utilizzare questa modalità per ottenere le informazioni più dettagliate sugli oggetti controllati e sul funzionamento del monitoraggio HTTP.</p>  |
| Scanner      | <p>In questa modalità nel log vengono registrati eventi come gli aggiornamenti, l'avvio e l'arresto di Scanner Dr.Web, le minacce rilevate, nonché i dati sui nomi di packer e sui contenuti di archivi compressi controllati.</p>  |



|                      |   |
|----------------------|---|
| Firewall             | In modalità standard Firewall non registra il file di log. Quando viene attivata la modalità di log dettagliato, vengono raccolti i dati sui pacchetti di rete (i log pcap).  |
| Aggiornamento Dr.Web | Lista dei file Dr.Web aggiornati e il loro status di download, informazioni sul funzionamento degli script ausiliari, data e ora di un aggiornamento, informazioni sul riavvio dei componenti Dr.Web dopo un aggiornamento. |
| Servizio Dr.Web      | Informazioni sui componenti Dr.Web, modifica delle impostazioni dei componenti, attivazione e disattivazione dei componenti, eventi della protezione preventiva, connessione al server di protezione centralizzata.         |

### Creazione dei memory dump

L'impostazione **Crea memory dump in caso di errori di scansione** consente di salvare le informazioni utili sul funzionamento di alcuni componenti di Dr.Web, il che consentirà successivamente agli specialisti Doctor Web di fare un'analisi più completa del problema e di proporre una soluzione. È consigliabile attivare questa impostazione a richiesta dei collaboratori del supporto tecnico Doctor Web o quando si verificano degli errori di scansione di file o di neutralizzazione di minacce. Un memory dump viene salvato nella forma di un file con l'estensione .dmp nella cartella %PROGRAMFILES%\Common Files\Doctor Web\Scanning Engine\.

### Log dettagliato



Nel log dettagliato viene registrata la quantità massima di informazioni sul funzionamento dei componenti Dr.Web. Questo porta alla disattivazione del limite alla dimensione dei file di log e alla riduzione delle prestazioni di Dr.Web e del sistema operativo. Questa modalità dovrebbe essere utilizzata solo se si verificano problemi nel funzionamento dei componenti o a richiesta dell'amministratore della rete antivirus.

1. Per attivare la modalità di log dettagliato per uno dei componenti di Dr.Web, spuntare il flag corrispondente.
2. Salvare le modifiche.

### Impostazioni della quarantena

Si può attivare un'opzione che definisce la modalità di isolamento degli oggetti infetti che vengono rilevati su supporti rimovibili. Se viene attivata questa opzione, tali minacce vengono messe in una cartella di quarantena sullo stesso supporto e non vengono cifrate. In tale caso la cartella di quarantena viene creata soltanto se il supporto è scrivibile. L'utilizzo delle cartelle separate e la rinuncia alla cifratura su supporti rimovibili consente di prevenire l'eventuale perdita di dati. Se l'opzione è disattivata, una minaccia rilevata viene spostata in quarantena sul disco locale.



## 8.5. Server

In questa sezione si possono visualizzare e modificare i parametri di interazione di Dr.Web con il server di protezione centralizzata, nonché configurare le impostazioni di Modalità mobile Dr.Web. L'amministratore della rete antivirus può vietare di modificare i parametri di interazione con il server, in tale caso i pulsanti e i flag saranno non disponibili per la gestione.

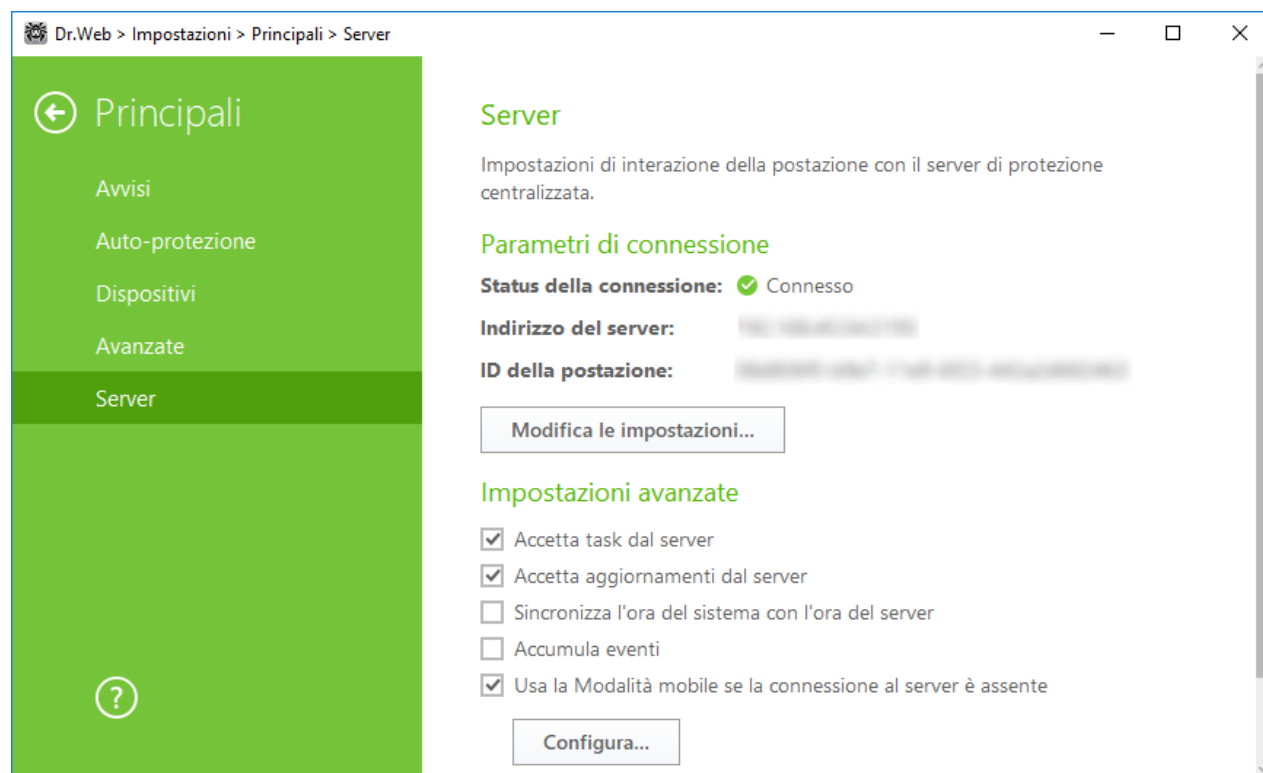


Immagine 16. Impostazioni della connessione al server

### Parametri di connessione

Nel gruppo **Parametri di connessione** vengono visualizzati:

- **Status della connessione** — stato della connessione della postazione al server di protezione centralizzata;
- **Indirizzo del server** — indirizzo del server di protezione centralizzata a cui è connessa la postazione;
- **ID della postazione** — identificatore della postazione per la connessione al server.

È possibile visualizzare e gestire le impostazioni della connessione al server, se l'amministratore della rete ha concesso tali permessi.





Le impostazioni della connessione al server di protezione centralizzata possono essere modificate solo in coordinamento con l'amministratore della rete antivirus, altrimenti il computer verrà disconnesso dalla rete antivirus.



Per modificare le impostazioni della connessione al server corrente o per aggiungere un altro server, premere **Modifica le impostazioni**. Si apre la finestra **Impostazioni di connessione** del server.


## Impostazioni di connessione

Nella tabella viene visualizzata la lista di tutti i server a cui la postazione può essere connessa. È possibile cancellare server dalla tabella e aggiungere nuovi server. Per cancellare una riga, premere il pulsante . Per configurare la connessione a un altro server, premere il pulsante . Nella finestra che si è aperta è necessario indicare l'indirizzo del server di protezione centralizzata, fornito dall'amministratore.

### Aggiunta del certificato

Un prerequisito per la connessione di una postazione al server di protezione centralizzata è la disponibilità di un certificato valido. Il certificato può essere univoco per ciascun server specifico o adatto per più server. È possibile aggiungere più certificati per la connessione a più server.

Di default è indicato il certificato che è stato utilizzato durante l'installazione del programma, se sul server non veniva effettuata una sostituzione delle chiavi di cifratura programmata. Se una sostituzione delle chiavi è stata effettuata, verrà indicato l'ultimo dei certificati generati. Per visualizzare la lista dei certificati disponibili o aggiungere un altro certificato, andare al link **Lista dei certificati**.

Per aggiungere un nuovo certificato, premere il pulsante  e nella finestra che si è aperta selezionare il file richiesto.

Per cancellare un certificato non utilizzato, premere il pulsante .

### Parametri di connessione della postazione

Per modificare i parametri di connessione della postazione:

1. Nella finestra **Parametri di connessione della postazione** indicare l'identificatore della postazione e la password per la connessione al server. Questi dati vengono forniti dall'amministratore del server.
2. Premere **OK** per salvare le modifiche.

Per resettare i parametri di connessione e connettersi come un nuovo arrivo al server di protezione centralizzata:

1. Nella finestra **Parametri di connessione della postazione** premere **Resetta i parametri e connettiti come un nuovo arrivo**.
2. Nella finestra che si è aperta confermare di voler resettare i parametri di connessione della postazione e connettersi come un nuovo arrivo. Notare che questa azione è irreversibile.



3. Dopo la conferma della registrazione della postazione sul server di protezione centralizzata Dr.Web otterrà i nuovi identificatore e password. Essi verranno utilizzati per la connessione al server.

## Impostazioni avanzate

Nel gruppo **Impostazioni avanzate** si possono selezionare le seguenti opzioni:

- **Accetta task dal server** — per ottenere periodicamente task dall'amministratore.
- **Accetta aggiornamenti dal server** — per ottenere a cadenze regolari gli aggiornamenti dei componenti di Dr.Web e dei database dei virus dal server di protezione centralizzata. Gli aggiornamenti avvengono in base alle impostazioni configurate sul server.
- **Sincronizza l'ora del sistema con l'ora del server** — per sincronizzare l'ora di sistema sul computer con quella del server di protezione centralizzata. In questa modalità Dr.Web imposta periodicamente l'ora di sistema sul computer in conformità all'ora del server.
- **Accumula eventi** — per salvare i dati degli eventi accaduti in modo da inviarli successivamente sul server di protezione centralizzata. Se l'opzione è attivata, le informazioni non vengono trasmesse sul server. Se il flag non è selezionato, e non c'è connessione al server, le informazioni importanti (per esempio circa le minacce rilevate e le statistiche) andranno perse.
- **Usa la Modalità mobile se la connessione al server è assente** — per ottenere tempestivamente gli aggiornamenti dei database dei virus.

Se il computer non avrà la connessione al server di protezione centralizzata per un lungo tempo, per ottenere tempestivamente gli aggiornamenti dai server Doctor Web, si consiglia di impostare la modalità mobile di funzionamento di Dr.Web. A questo scopo spuntare il flag **Usa la Modalità mobile se la connessione al server è assente**.



Il flag **Usa la Modalità mobile se la connessione al server è assente** sarà disponibile a condizione che sul server di protezione centralizzata nei permessi della postazione sia consentita la **Modifica della configurazione di Agent Dr.Web**.

In Modalità mobile Dr.Web tenta di connettersi al server di protezione centralizzata, fa tre tentativi e se non sono riusciti, aggiorna i database dei virus dai server Doctor Web. I tentativi di rilevamento del server di protezione centralizzata si susseguono continuamente a intervalli di circa un minuto.

Per configurare le impostazioni di Modalità di funzionamento mobile, premere il pulsante **Configura**. Si apre la finestra **Modalità mobile**.

Dalla lista a cascata **Periodicità degli aggiornamenti** si può selezionare la periodicità con cui verrà controllata la disponibilità degli aggiornamenti sui server Doctor Web.



Se nella lista **Periodicità degli aggiornamenti** viene selezionata l'opzione **Manualmente**, gli aggiornamenti automatici non verranno eseguiti. Sarà possibile avviare l'aggiornamento nel menu Dr.Web.



Se si usa un server proxy, impostare il flag corrispondente. In questo caso saranno attivi i campi:

| Impostazione           | Descrizione   |
|------------------------|---|
| Indirizzo              | Indicare l'indirizzo del server proxy.  |
| Porta                  | Indicare la porta del server proxy.   |
| Utente                 | Indicare il nome dell'account per la connessione al server proxy.                   |
| Password               | Indicare la password dell'account utilizzato per la connessione al server proxy.    |
| Tipo di autenticazione | Selezionare il tipo di autenticazione richiesto per la connessione al server proxy. |

Dopo aver finito di modificare, premere il pulsante **OK** per salvare le modifiche apportate o il pulsante **Annulla** per uscire dalla finestra senza salvare le modifiche. Per modificare le impostazioni della connessione al server proxy, premere nuovamente il pulsante **Modifica**.



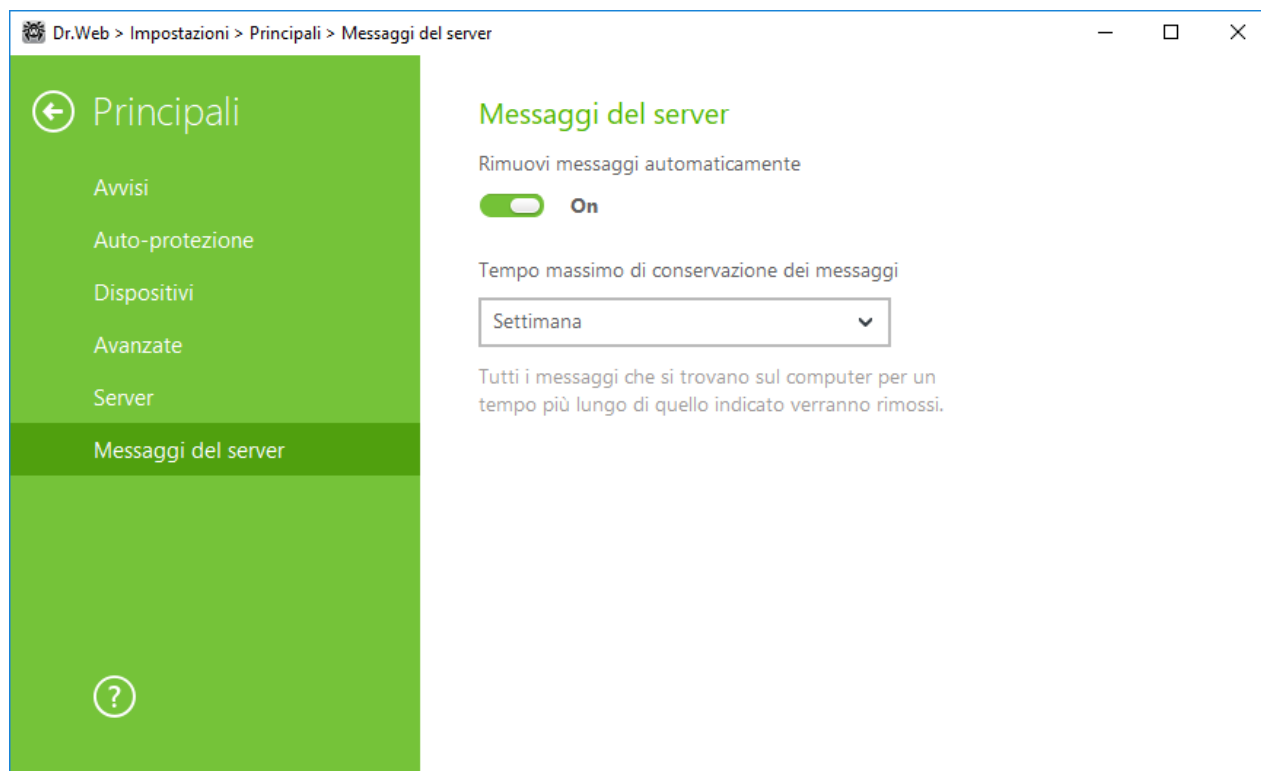
In modalità mobile solo i database dei virus vengono aggiornati.

Se il flag **Usa la Modalità mobile se la connessione al server è assente** viene deselezionato prima che riprenda la comunicazione con il server di protezione centralizzata, i database dei virus non verranno più aggiornati, ma la ricerca del server continuerà.

Tutte le modifiche che vengono impostate per la postazione sul server di protezione centralizzata entreranno in vigore non appena riprenderà la comunicazione di Dr.Web con il server.

## 8.6. Messaggi del server

Per la comodità di gestione degli avvisi sul server di protezione centralizzata l'amministratore della rete ha la possibilità di attivare l'invio dei messaggi sulla postazione. In questo caso nella finestra **Principali** comparirà la sezione **Messaggi del server**.



### Immagine 17. Impostazioni di rimozione automatica dei messaggi del server

È possibile configurare le impostazioni di rimozione automatica dei messaggi. A questo scopo attivare l'opzione **Rimuovi messaggi automaticamente** e nella voce **Tempo massimo di conservazione dei messaggi** nella lista a cascata selezionare il periodo di tempo richiesto. I messaggi verranno rimossi dopo questo periodo.



## 9. Office control

Tramite il modulo Office control è possibile controllare l'accesso degli utenti a siti, file e cartelle, e inoltre il tempo di utilizzo della rete Internet e del computer per ciascun account di Windows.

Per configurare Office control, aprire il menu , avviare **Impostazioni**  in [modalità amministratore](#) e selezionare la sezione **Office control**.

La limitazione dell'accesso a risorse del file system locale consente di salvaguardare l'integrità e la riservatezza dei dati importanti e di proteggere i file da un'infezione. C'è la possibilità di proteggere sia file singoli che cartelle per intero che si trovano sia su dischi locali che su supporti di memoria rimovibili.

Il controllo dell'accesso a risorse Internet consente sia di proteggere gli utenti dalla visualizzazione di siti indesiderati (siti dedicati alla violenza, al gioco d'azzardo ecc.) che di concedere a un utente l'accesso solo ai siti definiti dalle impostazioni del modulo Office control.

### 9.1. Configurazione del modulo Office control



La modifica delle impostazioni del componente è possibile se è stata autorizzata dall'amministratore del server di protezione centralizzata a cui Dr.Web si connette.

Per l'accesso alle impostazioni del modulo Office control viene richiesta la password se nella sezione [Impostazioni](#) è stata attivata l'opzione **Proteggi da password le impostazioni Dr.Web**.





Immagine 18. Impostazioni del modulo Office control

### Configurazione dei parametri del modulo Office control per diversi utenti

Selezionare nel pannello a sinistra il nome dell'utente per cui si desidera configurare le restrizioni di accesso. Nella parte principale della finestra vengono visualizzate le impostazioni definite per questo utente. Di default per tutti gli utenti del computer è consentito un accesso illimitato alle risorse Internet e alle risorse locali e non ci sono limitazioni al tempo di utilizzo. Per modificare le impostazioni, premere **Modifica** di fronte all'opzione desiderata.



Nuovi utenti vengono visualizzati nella lista solo dopo che eseguono il primo accesso al loro account.



È possibile [configurare](#) che gli avvisi sulle attività del modulo Office control vengano visualizzati sullo schermo.

#### 9.1.1. Internet

Di default per tutti gli utenti è impostata la modalità **Senza restrizioni**. Per modificare le impostazioni, dalla lista a cascata selezionare un'altra modalità.

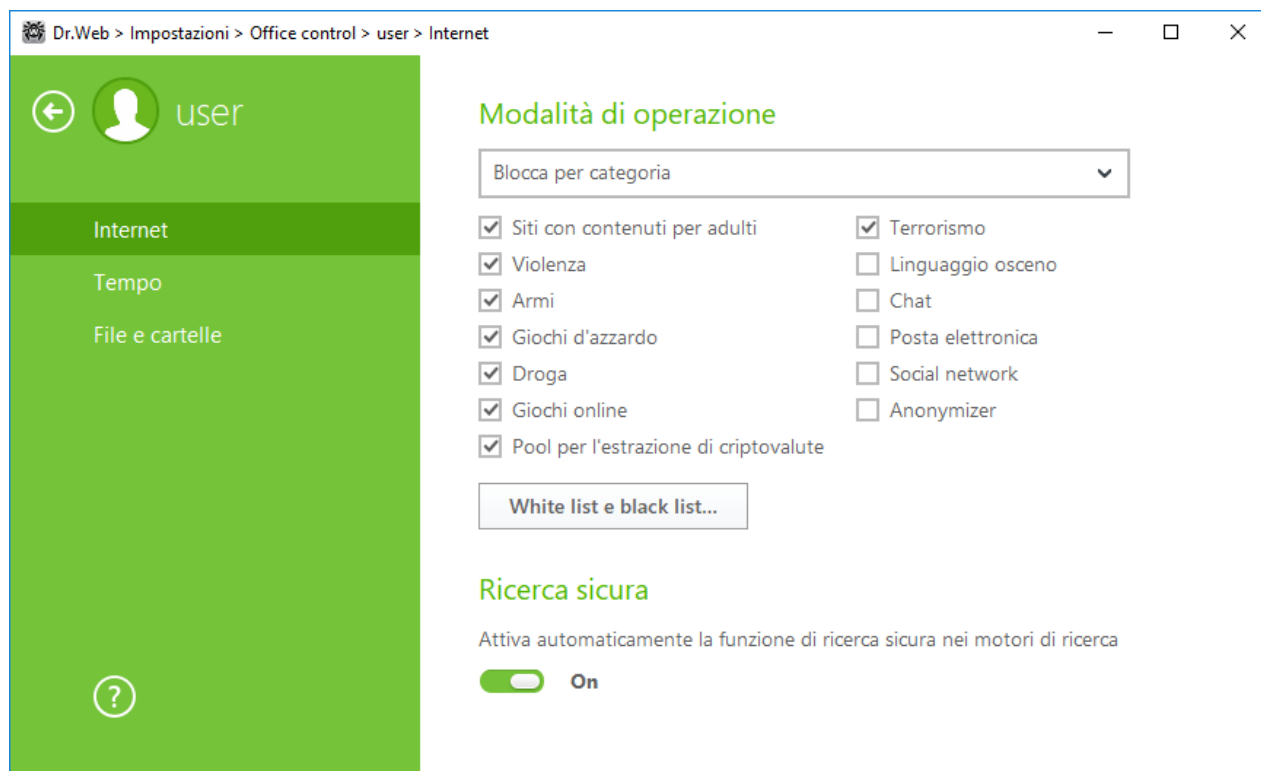


## Blocca per categoria

Lo stesso sito può essere classificato in più categorie diverse. In questo caso, il modulo Office control blocca l'accesso al sito se rientra in almeno una delle categorie attivate per il divieto di accesso.

In questa modalità è possibile indicare le categorie di risorse l'accesso a cui si vuole limitare:

| <b>Categoria</b>                      | <b>Descrizione</b>  |
|---------------------------------------|---|
| Siti con contenuti per adulti         | Siti contenenti materiali di carattere pornografico o erotico, siti di incontri, ecc.   |
| Violenza                              | Siti contenenti richiami alla violenza, materiali su vari incidenti con perdita di vite umane ecc.  |
| Armi                                  | Siti dedicati alle armi e agli esplosivi, nonché materiali che descrivono la loro fabbricazione ecc.  |
| Giochi d'azzardo                      | Siti che ospitano giochi online per soldi, casinò online, aste, e inoltre siti di scommesse ecc.  |
| Droga                                 | Siti che promuovono l'uso, la fabbricazione o la distribuzione di sostanze stupefacenti ecc.  |
| Giochi online                         | Siti che ospitano giochi che utilizzano una connessione Internet permanente.  |
| Terrorismo                            | Siti contenenti materiali di carattere propagandistico e aggressivo, descrizioni di attentati ecc.  |
| Linguaggio volgare                    | Siti che contengono linguaggio volgare (nei titoli di sezioni, articoli e così via).  |
| Chat                                  | Siti per lo scambio di messaggi in tempo reale.   |
| Posta elettronica                     | Siti che forniscono la possibilità di registrazione gratuita di caselle email.  |
| Social network                        | Social network di carattere generale, social network d'affari, aziendali, dedicati a un determinato argomento, nonché siti di incontri dedicati a un determinato argomento. |
| Anonymizer                            | Siti che consentono all'utente di nascondere le proprie informazioni personali e forniscono accesso a siti bloccati.  |
| Pool per l'estrazione di criptovalute | Siti che forniscono l'accesso ai servizi che riuniscono gli utenti con lo scopo di estrazione (mining) di criptovalute.   |



### Immagine 19. Configurazione dell'accesso a Internet in base alle categorie di siti

Per vietare l'accesso alle risorse della categoria richiesta, spuntare il flag corrispondente.

Inoltre, in questa modalità è possibile indicare in autonomo i siti l'accesso a cui verrà vietato o consentito a prescindere dalle altre restrizioni:

- Per bloccare l'accesso a un sito che non appartiene a nessuna delle categorie indicate, deve essere incluso nella black list personalizzata.
- Per consentire forzatamente l'accesso a un sito nonostante il fatto che appartenga a una delle categorie indesiderate, tale sito deve essere incluso nella white list personalizzata.

### Blocca tutti eccetto i siti inclusi nella white list

In questa modalità viene vietato l'accesso a tutte le risorse web eccetto quelle indicate nella white list di siti.

### Ricerca sicura

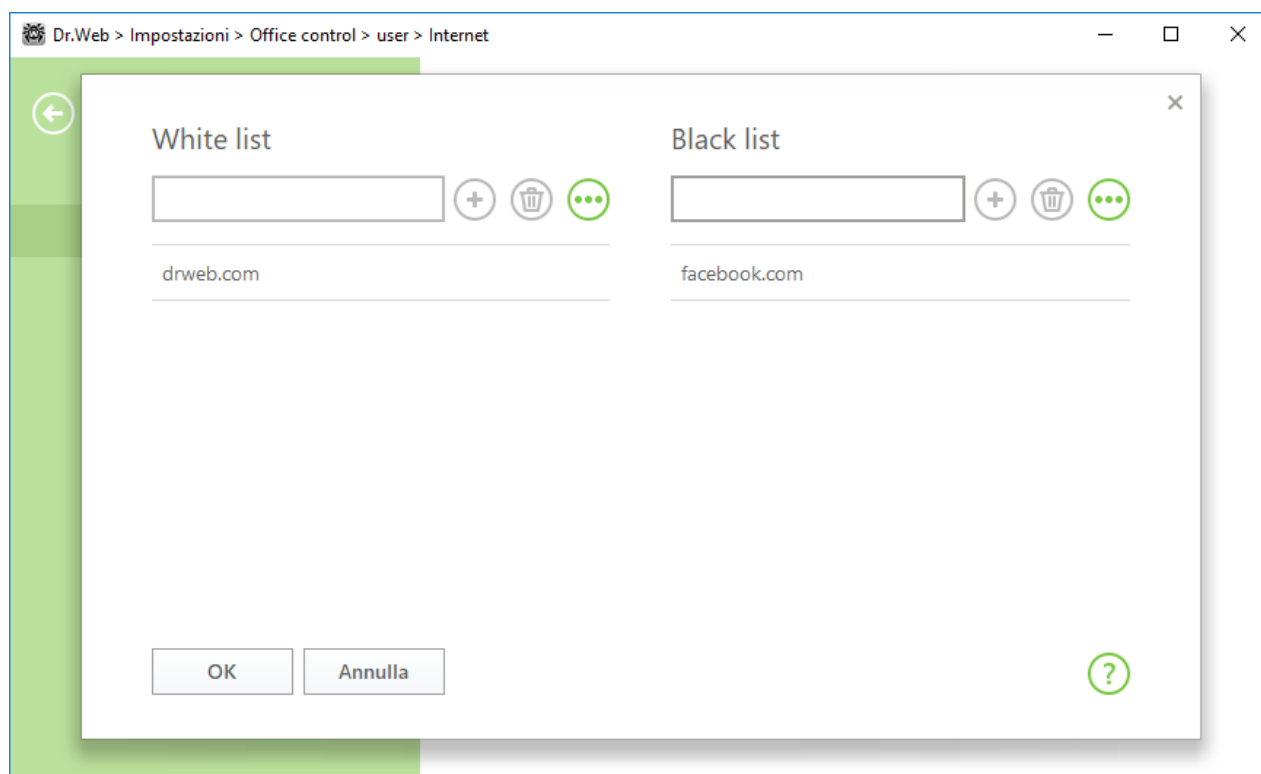
In qualsiasi delle modalità, eccetto la modalità **Senza restrizioni**, può essere attivata l'opzione **Ricerca sicura** che influisce sull'output dei risultati dei motori di ricerca. Questa funzione consente di escludere risorse indesiderate dai risultati di una ricerca, utilizzando le funzionalità dei motori di ricerca.

Per attivare la funzione **Ricerca sicura**, impostare l'interruttore su **On**.

## White list e black list dei siti

In questa finestra vengono impostate le liste dei siti l'accesso a cui viene consentito o bloccato a prescindere dalle altre impostazioni del modulo Office control.

Per gestire la white list e la black list, premere il pulsante **White list e black list**.



**Immagine 20. Creazione della white list e della black list**

Di default le liste sono vuote. Se necessario, è possibile aggiungere indirizzi di siti alla white o black list.

### Gestione di una lista degli indirizzi a dominio

1. Immettere il nome a dominio o una parte del nome a dominio di un sito nel campo **White list** o **Black list** a seconda di quello se si vuole consentire o vietare rispettivamente l'accesso a tale sito:
  - per aggiungere alla lista un determinato sito, immettere il suo indirizzo (per esempio `www.example.com`). L'accesso a tutte le risorse situate su questo sito verrà determinato da questo record;
  - per consentire l'accesso ai siti nei cui indirizzi è contenuto un determinato testo, immettere questo testo nel campo. Esempio: se si immette il testo `example`, l'accesso agli indirizzi `example.com`, `example.test.com`, `test.com/example`, `test.example222.it` e così via verrà determinato da questo record;
  - per consentire l'accesso a un determinato dominio, indicare il nome del dominio con il carattere ".". In tale caso l'accesso a tutte le risorse situate in questo dominio verrà



determinato da questo record. Se per indicare il dominio si usa il carattere "/", la parte della sottostringa a sinistra del carattere "/" sarà considerata nome a dominio e le parti a destra del carattere — parte dell'indirizzo consentito in questo dominio. Esempio: se si immette il testo `example.com/test`, verranno elaborati gli indirizzi come `example.com/test11`, `template.example.com/test22` e così via;

- per aggiungere alle eccezioni determinati siti, immettere nel campo di immissione una maschera che li definisce. Le maschere vengono aggiunte nel formato: `mask://...`



La maschera imposta la parte generale del nome di un oggetto, notare in particolare che:

- il carattere "\*" sostituisce qualsiasi sequenza di caratteri, anche una vuota;
- il carattere "?" sostituisce qualsiasi carattere, anche uno vuoto, ma uno solo.

Esempi:

- `mask://*.it/ o .it` — si apriranno tutti i siti nella zona .it;
- `mask://mail` — si apriranno tutti i siti in cui è contenuta la parola "mail";
- `mask://???..it/ o .it` — si apriranno tutti i siti della zona .it, i cui nomi sono composti da tre caratteri o meno.

Una stringa al momento dell'aggiunta alla lista può essere trasformata in una forma universale. Esempio: l'indirizzo `http://www.example.com` verrà trasformato in un record `www.example.com`.

2. Premere il pulsante  per aggiungere l'indirizzo alla lista.
3. Per cancellare un indirizzo dalla lista, selezionarlo nella lista e premere il pulsante .
4. Se necessario, ripetere i passi 1 e 2 per aggiungere altre risorse.

## 9.1.2. Tempo

In questa sezione vengono configurate le limitazioni al tempo dell'utilizzo del computer e della rete Internet da parte degli utenti.

Di default agli utenti è consentito utilizzare il computer e la rete Internet per un tempo illimitato.

È possibile limitare il tempo di utilizzo per gli utenti utilizzando una tabella con quadrati di tempo.

### Limitazione del tempo di accesso in modalità di tabella


1. Selezionare i giorni della settimana e le ore in cui si desidera vietare all'utente di accedere a Internet ed evidenziare i quadrati di tempo corrispondenti in blue:
  - per selezionare un quadrato, farci clic una volta con il pulsante sinistro del mouse;
  - per selezionare contemporaneamente diversi quadrati situati uno accanto agli altri, fare clic una volta con il pulsante sinistro del mouse sul primo quadrato e tenendo premuto il pulsante selezionare il periodo richiesto.
2. Selezionare i giorni della settimana e le ore in cui si desidera vietare all'utente di usare il computer ed evidenziare i quadrati di tempo corrispondenti in rosso:
  - per selezionare un quadrato, farci clic due volte con il pulsante sinistro del mouse;

- per selezionare contemporaneamente diversi quadrati situati uno accanto agli altri, fare clic due volte con il pulsante sinistro del mouse sul primo quadrato e tenendo premuto il pulsante selezionare il periodo richiesto.

Inoltre è possibile creare varie impostazioni per lo stesso utente salvandole in profili. Questa opzione sarà conveniente se occorrerà cambiare periodicamente le impostazioni in altri valori memorizzati (per esempio impostare diverse limitazioni per il tempo dell'anno scolastico e per il tempo delle vacanze).

### Creazione e modifica di un profilo delle impostazioni

È possibile modificare un profilo impostazioni personalizzato o crearne uno nuovo.

1. Per creare un nuovo profilo, premere il pulsante  e impostare il nome del profilo. Premere **OK**.
2. Per modificare un profilo personalizzato, selezionarlo dalla lista.
3. Quindi apportare le modifiche necessarie alla tabella.

Se viene selezionato il profilo **Senza restrizioni** e se vengono apportate modifiche alla tabella, il profilo verrà automaticamente sostituito con uno personalizzato.

## 9.1.3. File e cartelle

Di default non ci sono limitazioni all'accesso a file e cartelle. Per impostare limitazioni, attivare la relativa opzione e premere il pulsante **Oggetti**.

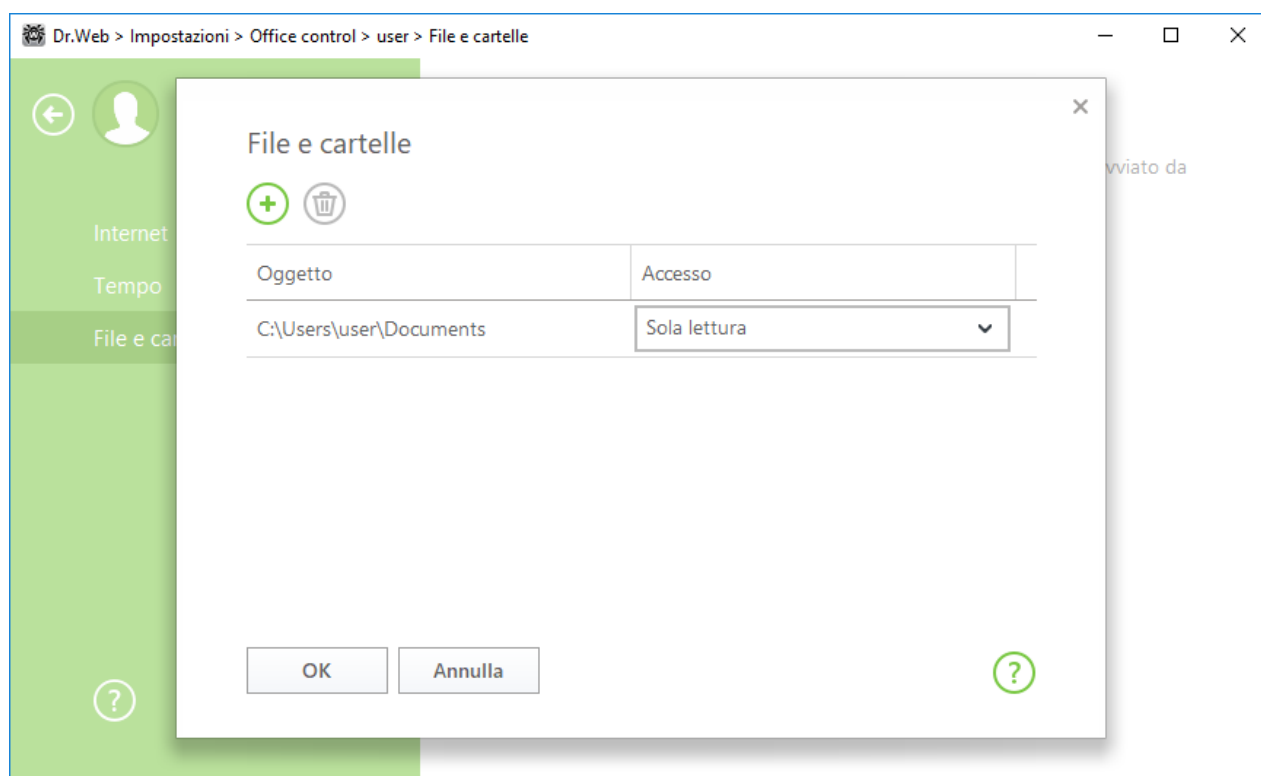



Immagine 21. Gestione dell'accesso a file e cartelle



Per aggiungere un oggetto alla lista, premere il pulsante  e selezionare il file o la cartella desiderata. Con l'impostazione predefinita l'oggetto aggiunto sarà disponibile all'utente per sola lettura.

Per bloccare completamente l'accesso all'oggetto selezionato, premere la limitazione impostata e dalla lista a cascata selezionare **Bloccati**.


Per eliminare un oggetto, selezionarlo dalla lista e premere il pulsante .

Notare che la limitazione di accesso non è garantita se il computer viene avviato da supporti rimovibili o se si accede agli oggetti impostati da altri sistemi operativi installati sul computer.



## 10. Eccezioni

In questa sezione è possibile configurare le eccezioni alle verifiche tramite i componenti SpIDer Guard, SpIDer Gate, SpIDer Mail e Scanner, e inoltre aggiungere indirizzi di mittenti alla black list o alla white list per non eseguire la verifica antispam delle relative email.

Per configurare le eccezioni, aprire il menu , avviare **Impostazioni**  in [modalità amministratore](#) e selezionare la sezione **Eccezioni**.



Notare che le modifiche in questa sezione possono essere bloccate da parte dell'amministratore della rete antivirus.

Per configurare l'accesso ai siti non raccomandati dall'azienda Doctor Web, selezionare la sezione [Siti web](#).

Per escludere determinati file e cartelle dalla scansione, selezionare la sezione [File e cartelle](#).

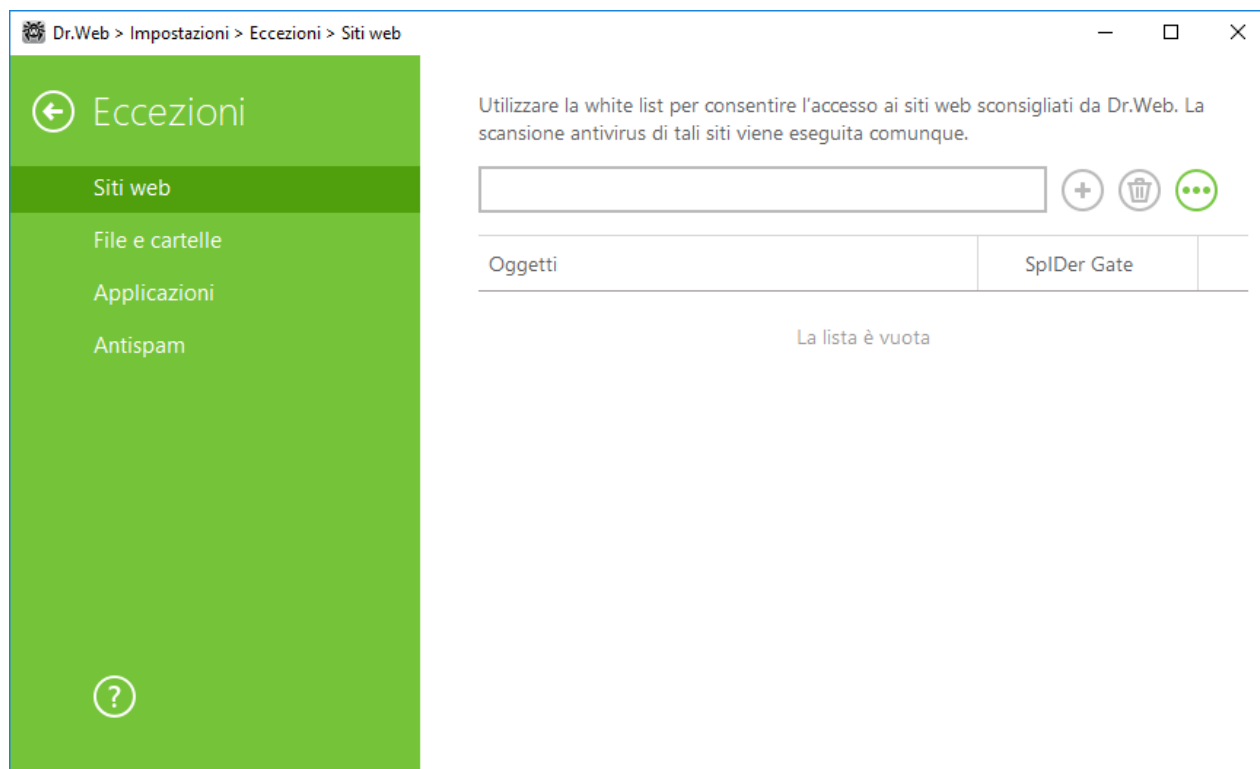
Per escludere determinati processi dalla scansione tramite i componenti Dr.Web, selezionare la sezione [Applicazioni](#).

Per configurare la scansione antispam delle email tramite il componente SpIDer Mail, selezionare la sezione [Antispam](#).

### 10.1. Siti

Se si vuole accedere ai siti sconsigliati per la visita dall'azienda Doctor Web, aggiungerli alle eccezioni. L'accesso ai siti dalla lista sarà consentito, ma la scansione antivirus di questi siti si mantiene. Di default la lista è vuota. Se l'indirizzo di un sito è aggiunto alla white list, l'accesso ad esso verrà concesso a prescindere dalle altre impostazioni di SpIDer Gate. Notare che se tale sito è aggiunto contemporaneamente alla black list del modulo Office control e alle eccezioni, l'accesso ad esso verrà bloccato.





**Immagine 22. Aggiunta di siti alle eccezioni**

### Gestione di una lista degli indirizzi a dominio



1. Nel campo di immissione indicare il nome a dominio o una parte del nome a dominio di un sito, l'accesso a cui si vuole consentire a prescindere dalle altre restrizioni:
  - per aggiungere alla lista un determinato sito, immettere il suo indirizzo (per esempio `www.example.com`). Sarà consentito l'accesso a tutte le risorse situate su questo sito;
  - per consentire l'accesso ai siti nei cui indirizzi è contenuto un determinato testo, immettere questo testo nel campo. Esempio: se si immette il testo `example`, sarà consentito l'accesso agli indirizzi `example.com`, `example.test.com`, `test.com/example`, `test.example222.it` e così via;
  - per consentire l'accesso a un determinato dominio, indicare il nome del dominio con il carattere ".". In tale caso sarà consentito l'accesso a tutte le risorse situate in questo dominio. Se per indicare il dominio si usa il carattere "/", allora la parte della sottostringa a sinistra del carattere "/" verrà considerata il nome a dominio e le parti a destra del carattere verranno considerate la parte dell'indirizzo consentito in questo dominio. Esempio: se si immette il testo `example.com/test`, saranno consentiti gli indirizzi `example.com/test11`, `template.example.com/test22` e così via;
  - per aggiungere alle eccezioni determinati siti, immettere nel campo di immissione una maschera che li definisce. Le maschere vengono aggiunte nel formato: `mask://...`  
La maschera imposta la parte generale del nome di un oggetto, notare in particolare che:
    - il carattere "\*" sostituisce qualsiasi sequenza di caratteri, anche una vuota;
    - il carattere "?" sostituisce qualsiasi carattere, anche uno vuoto, ma uno solo.



Esempi:

- `mask://*.it` — si apriranno tutti i siti nella zona .it;
- `mask://mail` — si apriranno tutti i siti in cui è contenuta la parola "mail";
- `mask://???.it` — si apriranno tutti i siti della zona .it, di cui i nomi sono costituiti da tre caratteri o meno.

Una stringa al momento dell'aggiunta alla lista può essere trasformata in una forma universale. Esempio: l'indirizzo `http://www.example.com` verrà trasformato in un record `www.example.com`.

2. Premere il pulsante . L'indirizzo indicato apparirà nella lista.
3. Se necessario, ripetere i passi 1 e 2 per aggiungere altri indirizzi. Per cancellare un indirizzo dalla white list, selezionare l'elemento corrispondente nella lista e premere il pulsante .

### Gestione degli oggetti nella lista

Attraverso il pulsante  sono disponibili le seguenti azioni:

- **Esportazione** — questa opzione consente di salvare la lista delle eccezioni creata per utilizzarla su un altro computer su cui è installato Dr.Web.
- **Importazione** — questa opzione consente di utilizzare una lista delle eccezioni creata su un altro computer.
- **Pulisci tutto** — questa opzione consente di cancellare tutti gli oggetti dalla lista delle eccezioni.

## 10.2. File e cartelle

In questa sezione si configura una lista delle cartelle e dei file che vengono esclusi dalla scansione tramite i componenti SpIDer Guard e Scanner. Come tali possono essere le cartelle di quarantena dell'antivirus, le cartelle di lavoro di alcuni programmi, file temporanei (file di swap) ecc.

Di default la lista è vuota. Aggiungere alle eccezioni cartelle e file specifici o utilizzare maschere per vietare la scansione di un determinato gruppo di file. Ciascun oggetto che viene aggiunto può essere escluso dalla scansione eseguita tramite entrambi i componenti o tramite ciascun componente separatamente.

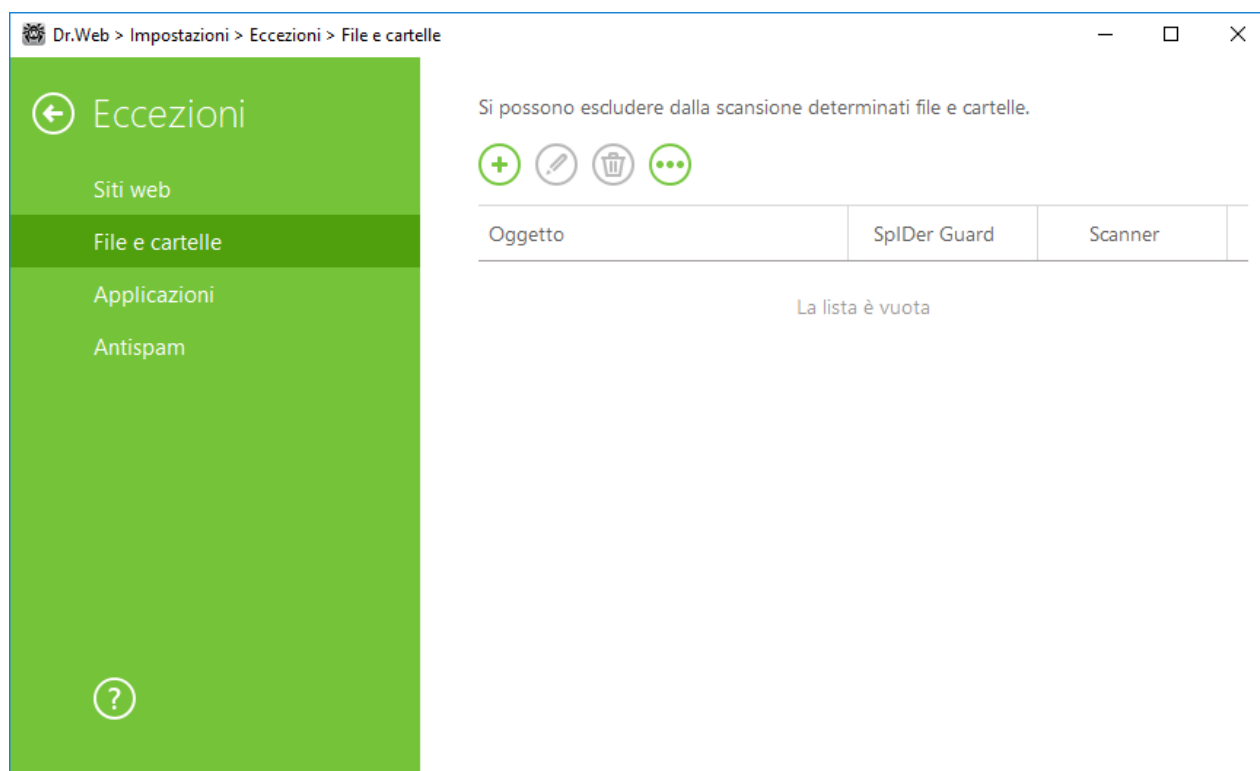



Immagine 23. Eccezioni alla verifica dei file e cartelle

### Gestione di una lista delle eccezioni

1. Per aggiungere una cartella o un file alla lista delle eccezioni, eseguire una delle seguenti azioni:

- per indicare un file o una cartella specifica esistente, premere il pulsante . Nella finestra che si è aperta premere il pulsante **Sfoglia** e selezionare una cartella o un file nella finestra standard di apertura di file. È possibile immettere manualmente il percorso completo del file o della cartella nel campo di immissione, nonché modificare la stringa nel campo di immissione prima di aggiungerla alla lista. Per esempio:
  - `C:\folder\file.txt` — si esclude dalla scansione il file.txt nella cartella C:\folder.
  - `C:\folder` — si escludono dalla scansione tutte le sottocartelle e i file nella cartella C:\folder.
- per escludere dalla scansione un file con un determinato nome, immettere il nome del file con l'estensione nel campo di immissione. In questo caso non è necessario specificare il percorso del file. Esempio:
  - `file.txt` — si escludono dalla scansione tutti i file con il nome file e l'estensione .txt in tutte le cartelle.
  - `file` — si escludono dalla scansione tutti i file con il nome di file senza estensione in tutte le cartelle.
- per escludere dalla scansione un determinato tipo di file o cartelle, immettere nel campo di immissione una maschera che lo definisce.



La maschera imposta la parte generale del nome di un oggetto, notare in particolare che:




- il carattere "\*" sostituisce qualsiasi sequenza di caratteri, anche una vuota;
- il carattere "?" sostituisce qualsiasi carattere, ma uno solo;

Esempi:

- resoconto\*.doc — una maschera che imposta tutti i documenti Microsoft Word di cui il nome inizia con la sottostringa "resoconto", per esempio i file resoconto-febbraio.doc, resoconto121209.doc e così via;
- \*.exe — una maschera che imposta tutti i file eseguibili con l'estensione EXE, per esempio setup.exe, iTunes.exe e così via;
- photo????09.jpg — una maschera che imposta tutti i file delle immagini del formato JPG di cui il nome inizia con la sottostringa "photo" e finisce con la sottostringa "09" e tra queste due sottostringhe nel nome di file ci sono esattamente quattro caratteri casuali, per esempio photo121209.jpg, photopapà09.jpg o photo----09.jpg.
- file\* — si escludono dalla scansione tutti i file con qualsiasi estensione di cui il nome inizia con file in tutte le cartelle.
- file.\* — si escludono dalla scansione tutti i file con il nome file e qualsiasi estensione in tutte le cartelle.
- C:\folder\\*\* — si escludono dalla scansione tutte le sottocartelle e file nella cartella C:\folder. I file nelle sottocartelle verranno scansionati.
- C:\folder\\* — si escludono dalla scansione tutti i file nella cartella C:\folder e in tutte le sottocartelle a ogni livello di nidificazione.
- C:\folder\\*.txt — si escludono dalla scansione i file \*.txt nella cartella C:\folder. I file \*.txt nelle sottocartelle verranno scansionati.
- C:\folder\\*\\*.txt — si escludono dalla scansione i file \*.txt solo nelle sottocartelle del primo livello di nidificazione della cartella C:\folder.
- C:\folder\\*\*\\*.txt — si escludono dalla scansione i file \*.txt nelle sottocartelle di ogni livello di nidificazione della cartella C:\folder. Nella cartella stessa C:\folder i file \*.txt verranno scansionati.

2. Nella finestra di configurazione indicare i componenti che non devono eseguire la scansione del file selezionato.
3. Premere il pulsante **OK**. Il file o la cartella selezionata apparirà nella lista.
4. Per modificare un'eccezione, selezionare l'elemento desiderato nella lista e premere .
5. Se necessario, ripetere i passi 1 e 2 per aggiungere altri file o cartelle. Per cancellare un file o una cartella dalla lista delle eccezioni, selezionare l'elemento corrispondente nella lista e premere il pulsante .

### Gestione degli oggetti nella lista

Attraverso il pulsante  sono disponibili le seguenti azioni:



- **Esportazione** — questa opzione consente di salvare la lista delle eccezioni creata per utilizzarla su un altro computer su cui è installato Dr.Web.
- **Importazione** — questa opzione consente di utilizzare una lista delle eccezioni creata su un altro computer.
- **Pulisci tutto** — questa opzione consente di cancellare tutti gli oggetti dalla lista delle eccezioni.

## 10.3. Applicazioni

In questa sezione si configura la lista dei programmi e processi che vengono esclusi dalla scansione tramite i componenti SpIDer Guard, SpIDer Gate e SpIDer Mail.

Di default la lista è vuota.

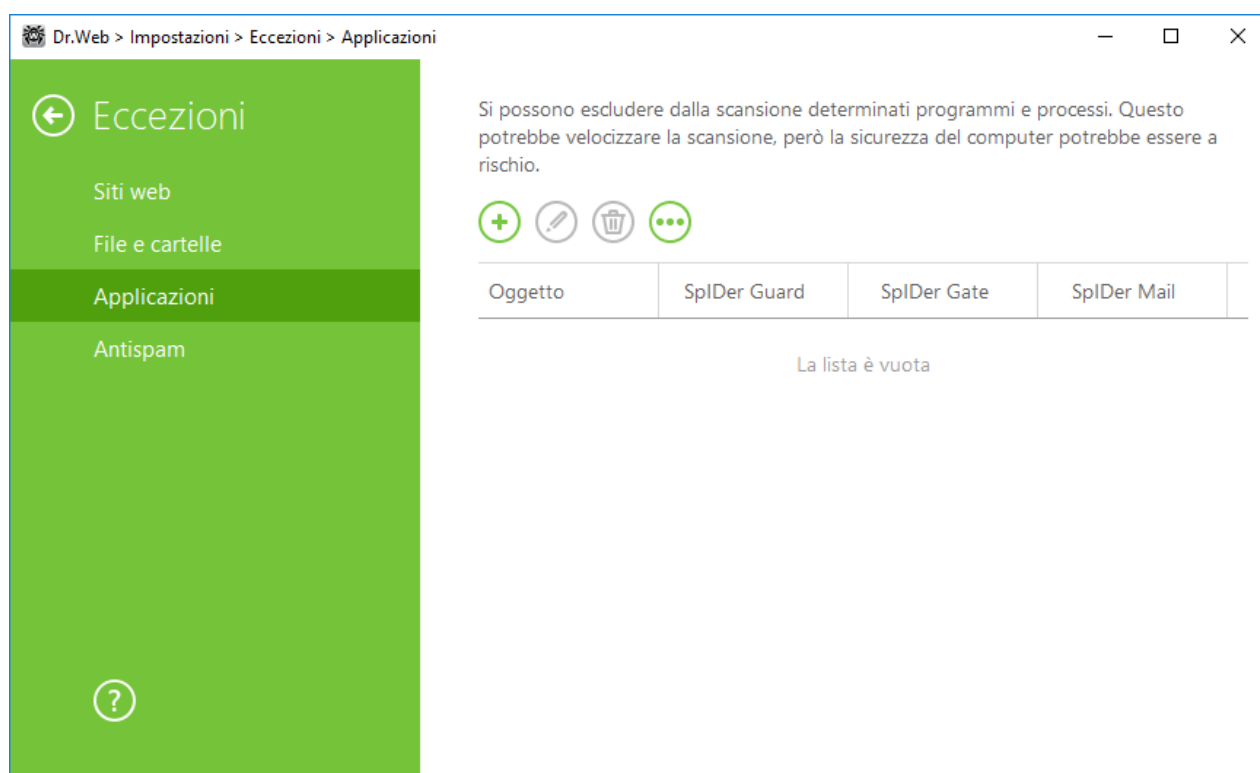



Immagine 24. Lista di applicazioni escluse

### Gestione di una lista delle eccezioni

1. Per aggiungere un programma o processo alla lista delle eccezioni, premere . Eseguire una delle seguenti azioni:
  - nella finestra che si è aperta premere il pulsante **Sfoglia** e selezionare un'applicazione nella finestra standard di apertura di file. È possibile immettere manualmente il percorso completo dell'applicazione nel campo di immissione. Per esempio:  
`C:\Program Files\folder\example.exe`
  - per escludere un'applicazione dalla scansione, immettere il suo nome nel campo di immissione. Non è necessario specificare il percorso completo dell'applicazione. Per esempio:



example.exe

- per escludere dalla scansione un determinato tipo di applicazioni, immettere nel campo di immissione una maschera che lo definisce.

La maschera imposta la parte generale del nome di un oggetto, notare in particolare che:

- il carattere "\*" sostituisce qualsiasi sequenza di caratteri, anche una vuota;
- il carattere "?" sostituisce qualsiasi carattere, ma uno solo;

Esempio di come si impostano le eccezioni:

- C:\Program Files\folder\\*.exe — esclude dalla scansione le applicazioni nella cartella C:\Program Files\folder. Nelle sottocartelle le applicazioni verranno scansionate.
- C:\Program Files\\*\\*.exe — esclude dalla scansione le applicazioni solo nelle sottocartelle del primo livello di nidificazione della cartella C:\Program Files.
- C:\Program Files\\*\*\\*.exe — esclude dalla scansione le applicazioni nelle sottocartelle di ogni livello di nidificazione della cartella C:\Program Files. Nella cartella stessa C:\Program Files le applicazioni verranno scansionate.
- C:\Program Files\folder\exam\*.exe — esclude dalla scansione ogni applicazione nella cartella C:\Program Files\folder, il cui nome inizia con "exam". Nelle sottocartelle tali applicazioni verranno scansionate.
- example.exe — esclude dalla scansione tutte le applicazioni con il nome example e l'estensione .exe in tutte le cartelle.
- example\* — esclude dalla scansione qualsiasi tipo di applicazioni di cui i nomi iniziano con example in tutte le cartelle.
- example.\* — esclude dalla scansione tutte le applicazioni con il nome example e qualsiasi estensione in tutte le cartelle.
- è possibile escludere dalla scansione un'applicazione in base al nome di una variabile, se il nome e il valore di questa variabile sono specificati nelle impostazioni delle variabili di sistema. Per esempio:
  - %EXAMPLE\_PATH%\example.exe — esclude dalla scansione un'applicazione in base al nome di una variabile di sistema. Il nome e il valore della variabile di sistema possono essere definiti nelle impostazioni del sistema operativo.

In caso del sistema operativo Windows 7 e superiori: **Pannello di controllo** → **Sistema** → **Impostazioni di sistema avanzate** → **Avanzate** → **Variabili d'ambiente** → **Variabili di sistema**.

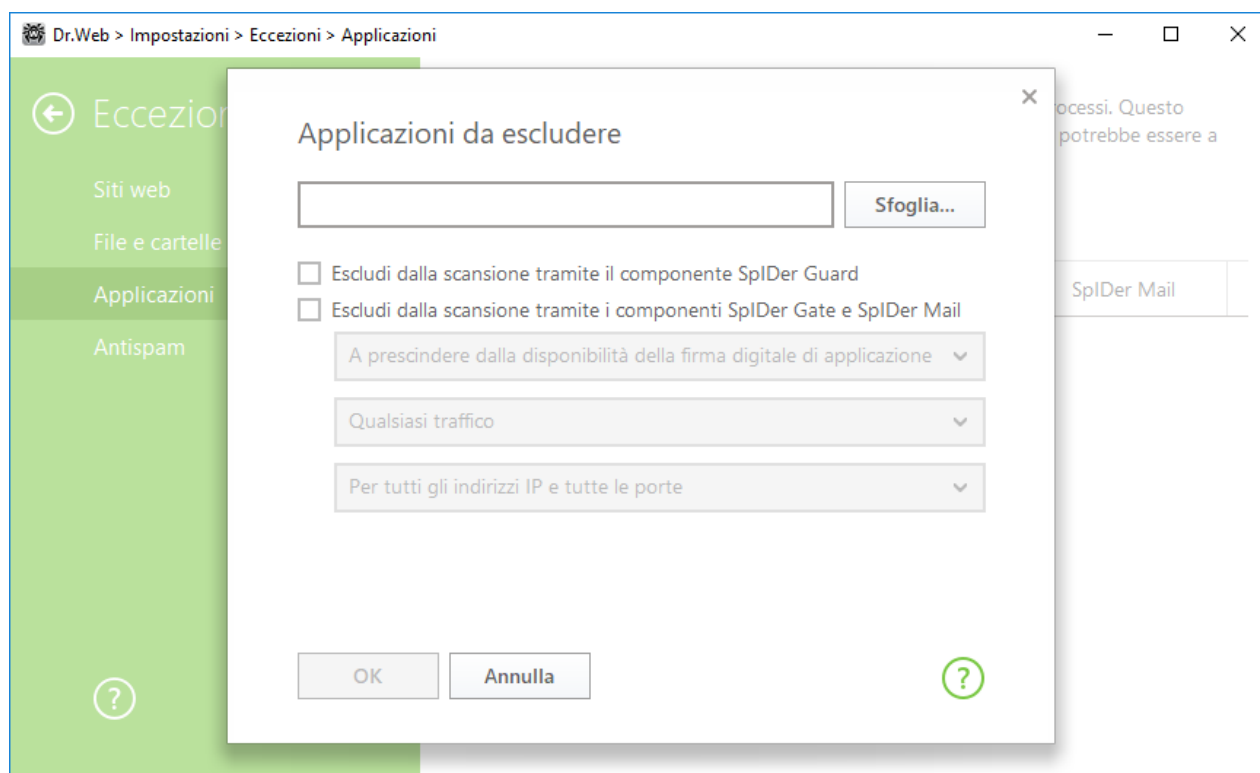
Il nome della variabile nell'esempio: EXAMPLE\_PATH.

Il valore della variabile nell'esempio: C:\Program Files\folder.

2. Nella finestra di configurazione indicare quali componenti non devono eseguire la scansione dell'applicazione selezionata. Nel caso di oggetti che vengono esclusi dalla scansione tramite i componenti SpIDer Gate e SpIDer Mail, indicare le condizioni aggiuntive.





| Parametro  | Descrizione  |
|--|--|
| A prescindere dalla disponibilità della firma digitale di applicazione | Selezionare questa opzione se l'applicazione deve essere esclusa dalla scansione a prescindere dalla disponibilità di una firma digitale valida.   |
| Se è disponibile la firma digitale di applicazione                     | Selezionare questa opzione se l'applicazione deve essere esclusa dalla scansione soltanto se ha una firma digitale valida. Altrimenti l'applicazione verrà controllata dai componenti.   |
| Qualsiasi traffico   | Selezionare questa opzione per escludere dalla scansione sia il traffico cifrato dell'applicazione che quello non cifrato.   |
| Traffico cifrato   | Selezionare questa opzione per escludere dalla scansione soltanto il traffico cifrato dell'applicazione.   |
| Per tutti gli indirizzi IP e tutte le porte                            | Selezionare questa opzione per escludere dalla scansione il traffico trasmesso su qualsiasi indirizzo IP e porta.  |
| Per gli indirizzi IP e le porte indicate                               | Selezionare questa opzione per indicare gli indirizzi IP o le porte in modo da escludere dalla scansione il traffico che ne viene trasmesso. Il traffico trasmesso da altri indirizzi IP o porte verrà controllato (se non è escluso dalle altre impostazioni).  |
| Impostazione di indirizzi e porte                                      | Per la messa a punto delle eccezioni, utilizzare i seguenti suggerimenti: <ul style="list-style-type: none"><li>• per escludere dalla scansione un determinato dominio su una determinata porta, indicare, per esempio <code>site.com:80</code>;</li><li>• per escludere dalla scansione il traffico su una porta non standard (per esempio 1111), è necessario indicare: <code>*:1111</code>;</li><li>• per escludere dalla scansione il traffico da un dominio su qualsiasi porta, indicare: <code>site:*</code></li></ul> |




**Immagine 25. Aggiunta di applicazioni alle eccezioni**

3. Premere il pulsante **OK**. L'applicazione selezionata apparirà nella lista.
4. Se necessario, ripetere le azioni per aggiungere altri programmi.

### Gestione degli oggetti nella lista

Per modificare un'eccezione, selezionare l'elemento richiesto nella lista e premere . Per cancellare un'applicazione dalla lista delle eccezioni, selezionare l'elemento corrispondente nella lista e premere .

Attraverso il pulsante  sono disponibili le seguenti azioni:

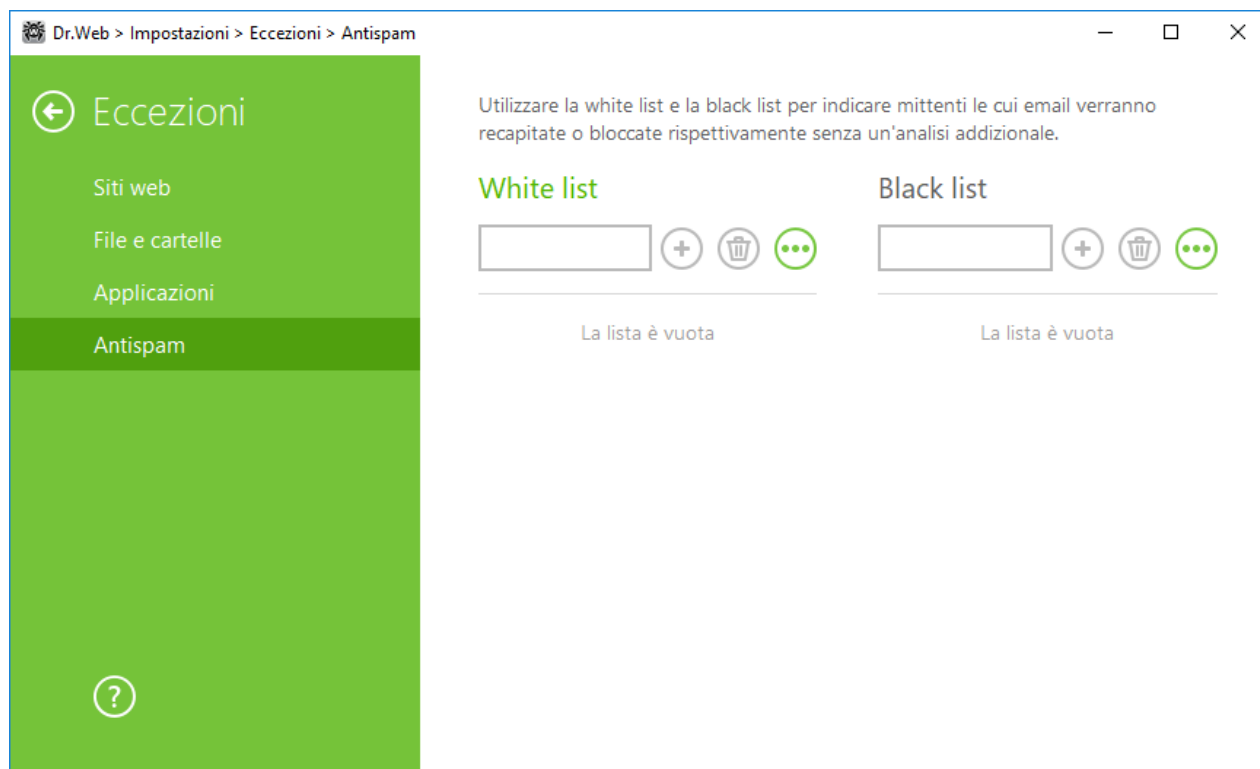
- **Esportazione** — questa opzione consente di salvare la lista delle eccezioni creata per utilizzarla su un altro computer su cui è installato Dr.Web.
- **Importazione** — questa opzione consente di utilizzare una lista delle eccezioni creata su un altro computer.
- **Pulisci tutto** — questa opzione consente di cancellare tutti gli oggetti dalla lista delle eccezioni.

## 10.4. Antispam

In questa finestra si configurano le liste dei mittenti le cui email saranno escluse dalla scansione antispam. Il componente SplDer Mail lascia passare o riconosce come spam le simili email senza eseguire l'analisi.




Se l'indirizzo di un mittente è aggiunto alla white list, l'email non viene analizzata dal punto di vista del contenuto di spam. Se l'indirizzo di un mittente è aggiunto alla black list, lo status di spam viene attribuito alla relativa email senza ulteriori analisi. Di default entrambe le liste sono vuote.




**Immagine 26. Aggiunta di indirizzi email alle eccezioni**


### Impostazione delle liste dell'antispam

1. Immettere nel rispettivo campo di immissione l'indirizzo email del mittente o una maschera che definisce gli indirizzi email dei mittenti di cui le email si vogliono processare automaticamente senza analisi. Metodi di immissione:
  - per aggiungere alla lista un determinato mittente, immettere il suo indirizzo email completo (per esempio `name@pochta.ru`). Tutte le email ricevute da questo indirizzo verranno processate senza analisi;
  - per aggiungere alla lista mittenti che utilizzano indirizzi email simili, utilizzare i caratteri "\*" e "?" per sostituire la parte differente dell'indirizzo. In particolare, il carattere "\*" sostituisce qualsiasi sequenza di caratteri, e il carattere "?" sostituisce un carattere (qualsiasi). Esempio: se si inserisce l'indirizzo `name*@pochta.ru`, le email dai mittenti con gli indirizzi come `name@pochta.ru`, `name1@pochta.ru`, `name_moj@pochta.ru` ecc. verranno processate senza analisi;
  - per assicurarsi di ricevere o bloccare le email dagli indirizzi email in uno specifico dominio, utilizzare il carattere "\*" invece del nome utente. Esempio: per impostare tutte le email dai mittenti dal dominio `pochta.ru`, immettere `*@pochta.ru`.
2. Per aggiungere alla lista l'indirizzo immesso, premere il pulsante .



3. Se necessario, ripetere i passi 1 e 2 per aggiungere altri indirizzi. Per cancellare un indirizzo dalla lista, selezionare l'elemento corrispondente nella lista e premere il pulsante .

### Gestione degli oggetti nella lista



Attraverso il pulsante  sono disponibili le seguenti azioni:

- **Esportazione** — questa opzione consente di salvare la lista delle eccezioni creata per utilizzarla su un altro computer su cui è installato Dr.Web.
- **Importazione** — questa opzione consente di utilizzare una lista delle eccezioni creata su un altro computer.
- **Pulisci tutto** — questa opzione consente di cancellare tutti gli oggetti dalla lista delle eccezioni.



## 11. Componenti di protezione

I componenti di protezione eseguono la scansione del sistema, la verifica della presenza di minacce e spam nelle email, il controllo delle connessioni di rete e del traffico HTTP.

Per configurare i componenti di protezione, aprire il menu , avviare **Impostazioni**  in [modalità amministratore](#) e selezionare la sezione **Componenti di protezione**.



Le impostazioni dei componenti di protezione sono disponibili solo a un avvio con i [permessi di amministratore](#).

Per configurare la verifica dei file che vengono aperti o dei processi che vengono avviati, selezionare [SplDer Guard](#).

Per configurare la verifica del traffico HTTP, selezionare [SplDer Gate](#).

Per configurare la verifica della presenza di minacce nella posta, selezionare [SplDer Mail](#).

Per controllare le connessioni e la trasmissione di dati attraverso Internet e inoltre per bloccare le connessioni sospette a livello di pacchetto e di applicazione, selezionare [Firewall](#).

Per modificare i parametri generali di controllo di file e oggetti vari, la reazione al rilevamento di file infetti o sospetti e di programmi malevoli, selezionare [Scanner](#).

Per controllare il comportamento delle applicazioni di terze parte, selezionare la sezione [Protezione preventiva](#).

### 11.1. SplDer Guard

SplDer Guard — monitor antivirus che risiede nella memoria operativa ed esegue la verifica dei file e della memoria al volo e inoltre rileva manifestazioni di attività di virus.

Con le impostazioni predefinite il monitor antivirus controlla solo i file che vengono creati o modificati sul disco rigido e tutti i file sui supporti rimovibili. Inoltre, il monitor antivirus cerca costantemente le azioni dei processi in esecuzione che sono proprie dei virus, e se rileva tali azioni, blocca tali processi. Al rilevamento di oggetti infetti, il monitor antivirus SplDer Guard applica ad essi le azioni secondo le impostazioni definite.

Non vengono controllati i file all'interno degli archivi e le caselle di posta. Se un file in archivio o in allegato a un'email è infetto, l'oggetto malevolo verrà rilevato dal monitor al momento dell'estrazione del file prima che possa comparire la possibilità di infezione del computer. Per prevenire l'infiltrazione sul computer degli oggetti malevoli che vengono diffusi attraverso la posta elettronica, [utilizzare](#) il monitor di posta SplDer Mail.



Quando rileva oggetti infetti, il monitor SpliDer Guard ci applica le azioni che corrispondono alle [impostazioni stabilite](#). Modificando le impostazioni in modo desiderato, si può modificare la reazione automatica del monitor agli eventi di virus.



È possibile l'incompatibilità del programma Dr.Web con MS Exchange Server. In caso di problemi, aggiungere i database e il registro delle transazioni di MS Exchange Server alla lista delle eccezioni di SpliDer Guard.

Di default SpliDer Guard si avvia automaticamente a ogni caricamento del sistema operativo e il monitor avviato SpliDer Guard non può essere scaricato dalla memoria durante la sessione di funzionamento corrente del sistema operativo.

### 11.1.1. Configurazione di SpliDer Guard



La modifica delle impostazioni del componente è possibile se è stata autorizzata dall'amministratore del server di protezione centralizzata a cui Dr.Web si connette.

---

Per l'accesso alle impostazioni di monitor SpliDer Guard viene richiesta la password se nella sezione [Impostazioni](#) è stata attivata l'opzione **Proteggi da password le impostazioni Dr.Web**.

Le impostazioni predefinite del programma sono ottimali per la maggior parte degli usi, non è consigliabile modificarle senza necessità.

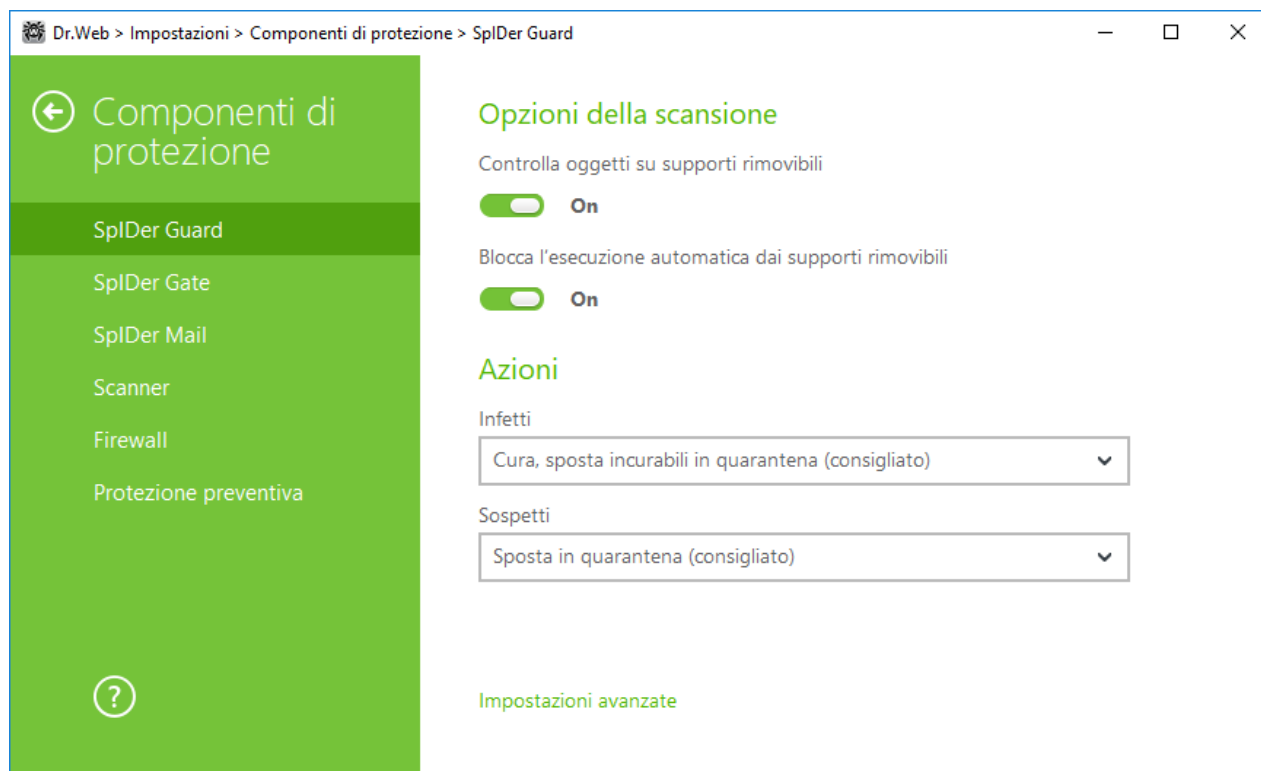


Immagine 27. Configurazione di SplDer Guard

## Opzioni della scansione

SplDer Guard di default verifica i file che vengono aperti, modificati ed eseguiti sui supporti di memorizzazione rimovibili (dischi CD/DVD, unità flash ecc.) e inoltre blocca l'avvio automatico del loro contenuto attivo. L'utilizzo di queste impostazioni aiuta a prevenire l'infezione del computer attraverso i supporti rimovibili. Se queste opzioni vengono disattivate, gli oggetti sui supporti rimovibili non verranno controllati.



In caso di problemi con l'installazione dei programmi che utilizzano il file autorun.inf, è consigliabile disattivare temporaneamente l'opzione **Blocca l'esecuzione automatica dai supporti rimovibili**.

## Azioni

In questa sezione viene configurata la reazione di SplDer Guard al rilevamento di file infetti o sospetti e di programmi malevoli.

La reazione viene configurata separatamente per ciascuna categoria di oggetti:

- **Infetti** — oggetti infettati da un virus conosciuto e (presumibilmente) curabile;
- **Sospetti** — oggetti presumibilmente infettati da un virus o contenenti un oggetto malevolo;
- vari oggetti potenzialmente pericolosi. Per espandere l'intera lista di oggetti, premere il link **Impostazioni avanzate**.



È possibile modificare la reazione del monitor SpIDer Guard al rilevamento di ciascun tipo di oggetti separatamente. Le reazioni possibili dipendono dal tipo di minaccia.

Di default il monitor di file SpIDer Guard cerca di curare i file infettati da un virus conosciuto e potenzialmente curabile e mette in [Quarantena](#) gli altri oggetti più pericolosi. Di default vengono ignorati i programmi joke, gli hacktool e gli oggetti inaffidabili. Le reazioni del monitor di file SpIDer Guard sono analoghe alle rispettive reazioni di Scanner Dr.Web.

Esistono le seguenti azioni applicabili agli oggetti rilevati:

| Azione  | Descrizione  |
|---|--|
| Cura, sposta in quarantena oggetti incurabili | <p>Per ripristinare l'oggetto allo stato precedente all'infezione. Se il virus è incurabile o se il tentativo di trattamento non è riuscito, l'oggetto verrà spostato in quarantena.</p> <p>Questa azione è disponibile solo per gli oggetti infettati da un virus conosciuto curabile, esclusi i trojan e i file infetti all'interno degli oggetti composti (archivi compressi, file di email o container di file).</p> |
| Cura, rimuovi oggetti incurabili              | <p>Per ripristinare l'oggetto allo stato precedente all'infezione. Se il virus è incurabile o se il tentativo di trattamento non è riuscito, l'oggetto verrà rimosso.</p> <p>Questa azione è disponibile solo per gli oggetti infettati da un virus conosciuto curabile, esclusi i trojan e i file infetti all'interno degli oggetti composti (archivi compressi, file di email o container di file).</p>                |
| Rimuovi                                       | <p>Per rimuovere l'oggetto.</p> <p>Nessun'azione verrà eseguita in caso dei settori di avvio.</p>  |
| Sposta in quarantena                          | <p>Per spostare l'oggetto nella cartella speciale <a href="#">Quarantena</a>.</p> <p>Nessun'azione verrà eseguita in caso dei settori di avvio.</p>  |
| Ignora  | <p>Per saltare l'oggetto senza eseguire alcun'azione e per non visualizzare avvisi.</p> <p>Questa azione è possibile solo per i programmi malevoli: adware, dialer, joke, riskware e hacktool.</p>   |
| Informa                                       | <p>Per visualizzare un avviso e saltare l'oggetto senza eseguire alcun'azione.</p> <p>Questa azione è possibile solo per gli oggetti sospetti e i programmi malevoli.</p>  |



Il monitor SpIDer Guard non verifica gli oggetti composti (archivi compressi, file di email o container di file) quindi non viene applicata alcun'azione a tali oggetti o ai file inclusi in tali oggetti.



I backup degli oggetti processati vengono conservati in [Quarantena](#).

## Modalità di controllo

In questo gruppo di impostazioni viene indicato in caso di quali azioni su un oggetto quest'ultimo deve essere controllato da SpIDer Guard.

| Impostazione           | Descrizione  |
|------------------------|--|
| Ottimale (consigliato) | Si usa di default.<br><br>In questa modalità la verifica viene eseguita solo nei seguenti casi: <ul style="list-style-type: none"><li>• per oggetti sui dischi rigidi — all'avvio o creazione dei file, nonché al tentativo di scrittura nei file esistenti o nei settori di avvio;</li><li>• per oggetti sui supporti rimovibili — a qualsiasi accesso ai file o ai settori di avvio (lettura, scrittura, avvio).</li></ul> |
| Paranoicale            | In questa modalità in caso di qualsiasi accesso (creazione, lettura, scrittura, avvio) vengono controllati tutti i file e settori di avvio sui dischi rigidi e di rete, nonché sui supporti rimovibili.  |



Quando funziona in modalità ottimale, SpIDer Guard non interrompe l'avvio del [file di test EICAR](#) e non determina questa operazione come pericolosa poiché questo file non rappresenta alcuna minaccia al computer. Tuttavia, quando tale file viene copiato o creato sul computer, SpIDer Guard elabora automaticamente il file come un programma malevolo e di default lo mette in Quarantena.

## Chiarimenti e suggerimenti

È consigliabile utilizzare la modalità **Ottimale** dopo aver eseguito una [scansione](#) di tutti i dischi rigidi tramite Scanner Dr.Web. In tale caso verrà esclusa l'infiltrazione sul computer dei nuovi virus o altri programmi malevoli attraverso i supporti rimovibili, ma non verranno ricontrollati gli oggetti puliti già controllati.

La modalità **Paranoicale** fornisce il massimo livello di protezione, ma aumenta notevolmente il carico di lavoro del computer.

In ogni modalità gli oggetti su unità di rete o supporti rimovibili vengono controllati solo se sono attivate le opzioni corrispondenti nel gruppo di impostazioni **Opzioni della scansione**.



Alcuni supporti rimovibili (in particolare hard disk portatili con interfaccia USB) possono essere rappresentati nel sistema come dischi rigidi. Pertanto tali dispositivi dovrebbero



essere utilizzati con molta cautela e al momento della connessione al computer dovrebbero essere scansionati tramite Scanner Dr.Web.

Di default non vengono controllati i file all'interno degli archivi e le caselle di posta. L'assenza della scansione degli archivi e della posta elettronica nel funzionamento continuo di SpIDer Guard non porta all'infiltrazione dei virus sul computer, ma semplicemente rinvia il momento del loro rilevamento. Se un archivio contaminato viene decompresso o un'email contaminata viene aperta, il sistema operativo tenta di registrare sul disco l'oggetto infetto e in questo momento SpIDer Guard rileva inevitabilmente l'oggetto malevolo.

## Impostazioni avanzate

Questo gruppo di impostazioni consente di configurare i parametri di scansione al volo che verranno utilizzati a prescindere dalla modalità di SpIDer Guard selezionata. È possibile attivare:

- l'uso dell'analisi euristica;
- la verifica dei programmi e moduli che vengono caricati;
- la verifica dei file di installazione;
- la verifica dei file su unità di rete (non consigliato);
- la verifica della presenza di rootkit sul computer (consigliato);
- la verifica degli script che vengono eseguiti da Windows Script Host e Power Shell (in Windows 10).

### Analisi euristica

Di default SpIDer Guard esegue la scansione utilizzando l'[analisi euristica](#). Se l'opzione è disattivata, la scansione si basa soltanto sulle firme dei virus conosciuti.

### Controllo in background della presenza di infezioni

Antirookit incluso in Dr.Web permette di monitorare in background la presenza nel sistema operativo di minacce composte, e se necessario, esegue la cura di un'infezione attiva.

Quando questa impostazione è attiva, Antirookit Dr.Web risiede nella memoria. A differenza della scansione dei file al volo, eseguita dal monitor SpIDer Guard, la ricerca dei rootkit (programmi malevoli studiati per nascondere le modifiche nel sistema operativo, quale il funzionamento di determinati processi, la modifica delle chiavi di registro, di cartelle o file) viene effettuata nel BIOS di sistema del computer e nelle aree critiche di Windows, quali gli oggetti in esecuzione automatica, i processi e moduli in esecuzione, la memoria operativa, i MBR/VBR dei dischi ecc.

Uno dei principali criteri di Antirookit Dr.Web è che funziona, risparmiando le risorse del sistema operativo (tempo di CPU, RAM libera ecc.), nonché tenendo conto delle prestazioni dell'hardware.





Quando scopre minacce, Antirootkit Dr.Web avvisa l'utente della minaccia e neutralizza gli effetti pericolosi.



Durante la verifica in background della presenza di rootkit vengono esclusi dalla verifica i file e le cartelle indicate nella [scheda corrispondente](#).

La verifica in background della presenza di rootkit è attivata di default.



La disattivazione di SpIDer Guard non influisce sulla scansione in background. Se l'impostazione è attivata, la scansione in background viene eseguita a prescindere da quello se è attivato o disattivato SpIDer Guard.

## 11.2. SpIDer Gate

SpIDer Gate — modulo di scansione antivirus del traffico HTTP. Con le impostazioni predefinite SpIDer Gate controlla automaticamente il traffico HTTP in arrivo e blocca la trasmissione di oggetti che contengono programmi malevoli. Attraverso il protocollo HTTP funzionano i web browser, i gestori di download e molte altre applicazioni che si scambiano dati con web server, cioè utilizzano la rete Internet.

Tramite la [modifica delle impostazioni](#) SpIDer Gate è possibile disattivare la scansione del traffico in arrivo o aggiungere alla scansione anche il traffico in uscita, nonché creare una lista delle applicazioni di cui il traffico HTTP verrà controllato in ogni caso e per intero. Inoltre, c'è la possibilità di escludere dalla scansione il traffico di singole applicazioni.

Con le impostazioni di base SpIDer Gate blocca gli oggetti ricevuti attraverso la rete che contengono programmi malevoli. Inoltre, di default è attivato il filtraggio URL dei siti sconsigliati e dei siti conosciuti come fonti di diffusione dei virus.

SpIDer Gate non supporta il controllo di connessioni sicure, cioè non controlla dati trasmessi attraverso protocolli crittografici.

Il programma risiede nella memoria operativa del computer e si riavvia automaticamente a caricamento di Windows.

### 11.2.1. Configurazione di SpIDer Gate



La modifica delle impostazioni del componente è possibile se è stata autorizzata dall'amministratore del server di protezione centralizzata a cui Dr.Web si connette.

Per l'accesso alle impostazioni di monitoraggio HTTP SpIDer Gate viene richiesta la password se nella sezione [Impostazioni](#) è stata attivata l'opzione **Proteggi da password le impostazioni Dr.Web**.

Le impostazioni predefinite del programma sono ottimali per la maggior parte degli usi, non è consigliabile modificarle senza necessità.



Immagine 28. Configurazione di SpIDer Gate

## Controllo del traffico dei client di messaggistica istantanea

Nel gruppo **Opzioni della scansione** è possibile attivare la scansione dei link e dati trasmessi dai client dei sistemi di messaggistica istantanea (Agent Mail.ru, ICQ e dai client che utilizzano il protocollo Jabber). Viene controllato solo il traffico in arrivo. Di default l'opzione è attivata.

I link trasmessi nei messaggi vengono controllati in base alle impostazioni di SpIDer Gate: i link di siti conosciuti come fonti di diffusione dei virus vengono automaticamente bloccati, i link di siti sconsigliati e gli URL aggiunti su richiesta di un titolare del diritto vengono bloccati se sono attive le relative impostazioni nella sezione **Parametri di blocco**. Il controllo tiene in considerazione la [white list di siti](#) e [le applicazioni escluse dalla scansione](#).

Vengono inoltre controllati i file trasmessi dai client dei sistemi di messaggistica istantanea. Se viene rilevata una minaccia, la trasmissione di tale file viene bloccata, se è attivata la relativa impostazione nella sezione **Blocca programmi**. I virus vengono automaticamente bloccati se l'opzione **Controlla dati in trasferimento e URL in client IM** è attivata.



## Parametri di blocco

Nel gruppo **Parametri di blocco** è possibile impostare il blocco automatico dell'accesso agli URL aggiunti al database su richiesta di un titolare del diritto (per farlo attivare l'opzione corrispondente) e anche ai siti sconsigliati, conosciuti come non attendibili (per farlo attivare l'opzione **Blocca l'accesso ai siti sconsigliati**). Nella sezione **Eccezioni** si possono [indicare i siti](#) l'accesso a cui deve essere consentito nonostante le limitazioni impostate.



SpIDer Gate di default blocca l'accesso ai siti noti come fonti di virus o di altri tipi di programmi malevoli. Il controllo tiene conto delle applicazioni [escluse dalla scansione](#).

## Blocco dei programmi

Il monitoraggio HTTP SpIDer Gate può bloccare i seguenti programmi malevoli:

- sospetti;
- riskware;
- dialer;
- hacktool;
- adware;
- joke.

Di default vengono bloccati i programmi sospetti e gli adware, nonché i dialer.

## Blocco degli oggetti

SpIDer Gate può bloccare oggetti non controllati o danneggiati. Di default queste opzioni sono disattivate.

## Impostazioni avanzate

È possibile configurare la scansione di archivi e di pacchetti di installazione. Di default l'opzione di scansione di archivi e pacchetti di installazione è disattivata.

Inoltre, è possibile configurare **Priorità di scansione** — l'allocazione delle risorse in base alla priorità di scansione del traffico. Con una priorità di scansione inferiore la velocità di lavoro con la rete Internet diminuisce poiché il monitoraggio HTTP SpIDer Gate deve aspettare più a lungo il caricamento dei dati e controllare una quantità di informazioni più grande. Con l'aumento della priorità la scansione viene eseguita più di frequente, il che permette al monitoraggio HTTP di fornire dati più velocemente, aumentando in questo modo la velocità di lavoro con la rete. Tuttavia, con le scansioni più frequenti aumenta il carico di lavoro del processore.



Inoltre, si può selezionare il tipo di traffico HTTP da controllare. Di default viene controllato solo il traffico in arrivo. Il controllo tiene in considerazione le azioni impostate, la [white list di siti](#) e le [applicazioni escluse dalla scansione](#).

## 11.3. SpIDer Mail

Il monitor di posta SpIDer Mail viene incluso di default tra i componenti installati, risiede nella memoria e si avvia automaticamente al caricamento del sistema operativo.

SpIDer Mail non supporta il controllo del traffico email crittografato.

### Processamento delle email

Il monitor di posta SpIDer Mail riceve tutte le email in ingresso invece del client di posta elettronica e le sottopone a una scansione antivirus con il massimo grado di dettaglio. Se non ci sono virus od oggetti sospetti, passa l'email al programma di posta in un modo "trasparente" – come se fosse arrivata direttamente dal server. In modo simile controlla le email in uscita prima di inviarle sul server.

[La reazione](#) del monitor di posta SpIDer Mail al rilevamento delle email infette e sospette, nonché delle email che non hanno superato il controllo (per esempio le email con una struttura troppo complessa) di default è la seguente:

- informazioni dannose vengono eliminate dalle email infette (quest'azione si chiama la *cura* dell'email), quindi le email vengono consegnate in modo normale;
- le email contenenti oggetti sospetti vengono spostate in [Quarantena](#) come file separati, al programma di posta viene spedita una relativa notifica (questa azione si chiama lo *spostamento* dell'email). Le email spostate vengono eliminate dal server POP3 o IMAP4;
- le email non infette e le email che non hanno superato il controllo vengono trasmesse senza modifiche (*vengono consentite*).

Le email in uscita infette o sospette non vengono trasmesse sul server, l'utente viene notificato del rifiuto di invio del messaggio (di regola, in tale caso il programma di posta salva l'email).

Le impostazioni predefinite del monitor di posta SpIDer Mail sono ottimali per un utente principiante e assicurano il massimo livello di protezione con il minimo intervento dell'utente. Tuttavia, in questo caso vengono bloccate alcune funzioni dei programmi di posta (per esempio l'invio di un'email su molteplici indirizzi può essere percepito come il mailing di massa, non viene riconosciuto lo spam ricevuto), nonché viene persa la possibilità di ottenere informazioni utili dalle email automaticamente distrutte (dalla parte di testo non infetta). Gli utenti più esperti possono [modificare](#) le impostazioni di verifica della posta e le impostazioni di reazione di SpIDer Mail a vari eventi.



## Controllo di email tramite altri strumenti

Scanner Dr.Web può rilevare virus nelle caselle di posta di alcuni formati, però il monitor di posta SpIDer Mail ha rispetto ad esso una serie di vantaggi:

- non tutti i formati delle caselle di posta dei programmi popolari sono supportati da Scanner Dr.Web; se viene utilizzato il monitor di posta SpIDer Mail, le email infette non arrivano nemmeno fino alle caselle di posta;
- Scanner Dr.Web controlla le caselle di posta solo on demand, e non al momento della ricezione della posta, e questa operazione è impegnativa e richiede un tempo notevole.

Dunque, con le impostazioni predefinite di tutti i componenti di Dr.Web, il monitor di posta SpIDer Mail rileva per primo e non lascia passare sul computer i virus e gli oggetti malevoli che si diffondono via email. Il suo funzionamento è molto economico in termini di consumo di risorse di calcolo; gli altri componenti possono non essere utilizzati per il controllo dei file di posta.

### 11.3.1. Configurazione di SpIDer Mail



La modifica delle impostazioni del componente è possibile se è stata autorizzata dall'amministratore del server di protezione centralizzata a cui Dr.Web si connette.

Per l'accesso alle impostazioni di monitor di posta SpIDer Mail viene richiesta la password se nella sezione [Impostazioni](#) è stata attivata l'opzione **Proteggi da password le impostazioni Dr.Web**.

Le impostazioni predefinite del programma sono ottimali per la maggior parte degli usi, non è consigliabile modificarle senza necessità.

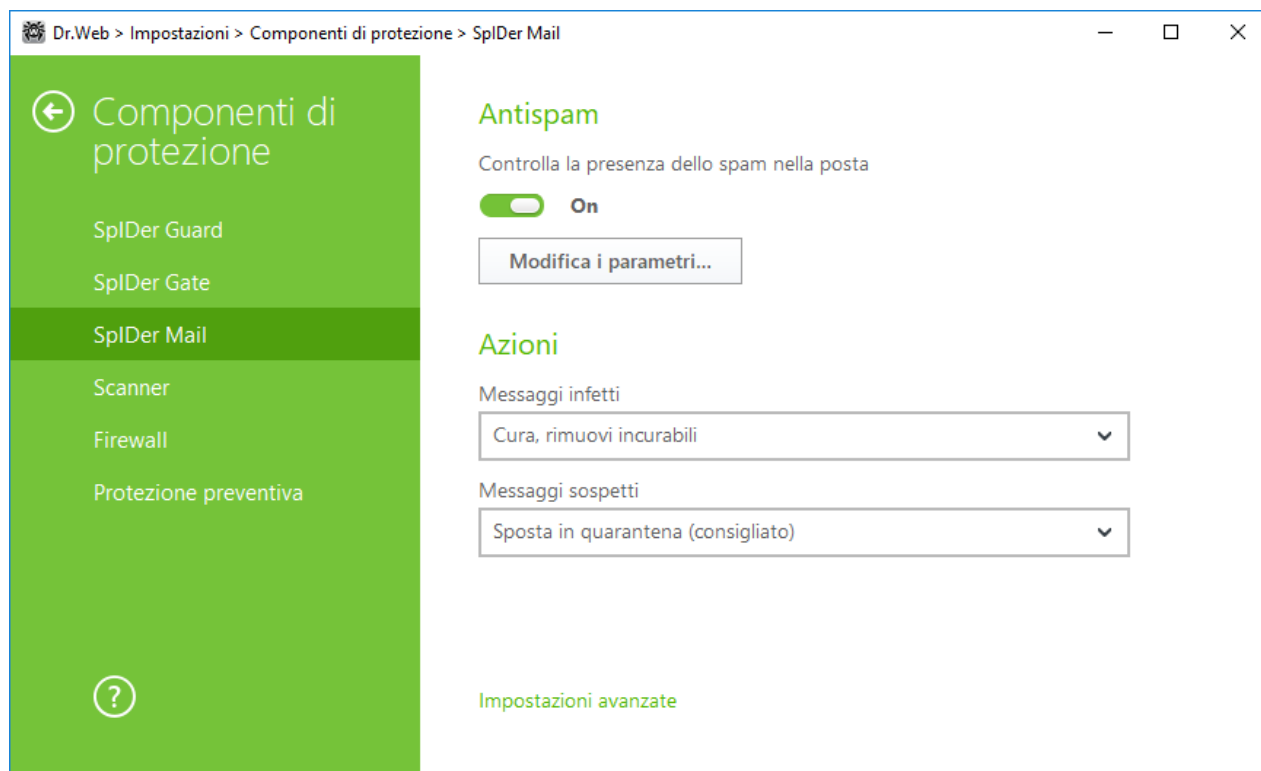


Immagine 29. Configurazione di SpIDer Mail

## Antispam

Di default, SpIDer Mail controlla la presenza dello spam nelle email. È possibile disattivare questa opzione tramite l'interruttore corrispondente o modificare i parametri di scansione, premendo il pulsante **Modifica i parametri**. Le tecnologie del filtro antispam e le impostazioni configurabili sono descritte in dettaglio nella sezione [Antispam](#).

## Azioni

Di default il monitor di posta SpIDer Mail cerca di curare le email infettate da un virus conosciuto e potenzialmente curabile. Le email incurabili e sospette, nonché gli adware e i dialer vengono messi in [Quarantena](#). Le altre email vengono trasmesse dal monitor di posta senza modifica (*le lascia passare*).

Le reazioni del monitor di posta SpIDer Mail sono analoghe alle rispettive reazioni di Scanner Dr.Web.

È possibile prescrivere al monitor di posta SpIDer Mail le seguenti reazioni:

| Azione                     | Descrizione   |
|----------------------------|---|
| Cura, sposta in quarantena | Per ripristinare l'email allo stato precedente all'infezione. Se il virus è incurabile o se il tentativo di trattamento non è riuscito, l'oggetto verrà spostato in |



| Azione                           | Descrizione  |
|----------------------------------|--|
| oggetti incurabili               | quarantena.<br><br>Questa azione è possibile solo per le email infettate da un virus conosciuto curabile, esclusi i trojan i quali vengono rimossi al rilevamento. La cura di file in archivi non è possibile a prescindere dal tipo di virus. |
| Cura, rimuovi oggetti incurabili | Per ripristinare l'email allo stato precedente all'infezione. Se il virus è incurabile o se il tentativo di trattamento non è riuscito, l'oggetto verrà eliminato.   |
| Rimuovi                          | Per eliminare l'email. In questo caso l'email non viene inoltrata al destinatario, invece al programma di posta viene trasmessa una notifica di operazione eseguita.   |
| Sposta in quarantena             | Per spostare l'email nella cartella speciale <a href="#">Quarantena</a> . In questo caso l'email non viene inoltrata al destinatario, invece al programma di posta viene trasmessa una notifica di operazione eseguita.                        |
| Ignora                           | Per trasmettere l'email senza applicare ad essa alcune azioni.   |

Nel caso di rilevamento di oggetti malevoli nella posta, se è impostata qualsiasi delle azione citate, tranne l'azione **Ignora**, la trasmissione dell'email sarà negata.

È possibile aumentare l'affidabilità della protezione antivirus rispetto al livello predefinito, selezionando nella lista **Non controllati** la voce **Sposta in quarantena**. In questo caso è consigliabile controllare successivamente tramite Scanner Dr.Web i file con i messaggi spostati.



La protezione dalle email sospette può essere disattiva solo se il computer è protetto additionally tramite il monitor SpIDer Guard permanentemente residente nella memoria.

## Azioni eseguite sulle email

In questo gruppo di impostazioni vengono indicate le azioni aggiuntive applicabili alle email processate dal monitor di posta SpIDer Mail.

| Impostazione                                      | Descrizione  |
|---|--|
| Aggiungi l'intestazione 'X-AntiVirus' ai messaggi | È un'impostazione predefinita.<br><br>Se viene utilizzata questa impostazione, alle intestazioni di tutte le email processate dal monitor di posta SpIDer Mail vengono aggiunte informazioni circa la scansione di questa email e la versione di Dr.Web. Non è possibile modificare il formato dell'intestazione che viene aggiunta. |



| Impostazione                        | Descrizione  |
|-------------------------------------|--|
| Rimuovi email modificate sul server | Se viene utilizzata questa impostazione, le email in ingresso eliminate o spostate in quarantena dal monitor di posta SplDer Mail vengono eliminate sul server di posta a prescindere dalle impostazioni del programma di posta. |

## Ottimizzazione della scansione

È possibile impostare una condizione al verificarsi della quale le email con una struttura complessa di cui la scansione consuma troppe risorse vengono riconosciute come non controllate. A tale scopo attivare l'opzione **Timeout della scansione di un'email** e impostare il tempo massimo entro cui viene controllata un'email. Dopo il tempo indicato il monitor di posta SplDer Mail interrompe la scansione dell'email. Di default sono impostati 250 secondi.

## Scansione degli archivi compressi

Attivare l'opzione **Controlla archivi** affinché SplDer Mail controlli il contenuto degli archivi compressi trasmessi via email. In questo caso saranno disponibili le seguenti impostazioni:

- **Dimensione massima di un file che viene decompresso.** Se l'archivio decompresso eccederà la dimensione indicata, il monitor di posta SplDer Mail non lo decomprimerà e non lo controllerà. Di default è impostato il valore di 30720 KB;
- **Rapporto di compressione massimo di un archivio.** Se il rapporto di compressione eccede il valore indicato, il monitor di posta SplDer Mail non decomprimerà e non controllerà l'archivio. Di default è impostato il valore 0;
- **Livello di nidificazione massimo in un archivio.** Se il livello di nidificazione eccede il valore impostato, il monitor di posta SplDer Mail controllerà l'archivio solo fino al livello indicato. Di default è impostato il valore 64.

Per attivare uno o più parametri di ottimizzazione, spuntare i flag corrispondenti.



Un parametro non ha limitazioni, se è impostato il valore 0.

## Impostazioni avanzate

Questo gruppo di impostazioni permette di configurare i parametri aggiuntivi di scansione della posta elettronica:

- uso dell'analisi euristica — in questa modalità vengono utilizzati i [meccanismi speciali](#) che permettono di scoprire nella posta elettronica oggetti sospetti che con grande probabilità sono infettati dai virus ancora sconosciuti. Per disattivare l'analisi euristica, deselezionare il flag **Usa l'analisi euristica (consigliato)**;
- controllo di pacchetti di installazione. Di default questa impostazione è disattivata.





## 11.3.2. Antispam

Le tecnologie del filtro antispam Dr.Web sono composte da diverse migliaia di regole che condizionalmente possono essere divise in alcuni gruppi:

- **l'analisi euristica** — una tecnologia molto complessa intelligente dell'analisi empirica di tutte le parti dell'email: del campo dell'intestazione, del corpo, del contenuto dell'allegato;
- **il filtraggio della controazione** — consiste nel riconoscimento degli espedienti utilizzati dagli spammer per aggirare filtri antispam;
- **l'analisi basata sulle firme HTML** — i messaggi che includono il codice HTML vengono confrontati con i campioni della libreria delle firme HTML dell'antispam. Tale confronto, in combinazione con i dati sulle dimensioni delle immagini di solito utilizzate dai mittenti dello spam protegge gli utenti dai messaggi di spam contenenti link di pagine web;
- **l'analisi semantica** — un confronto delle parole ed espressioni del messaggio con le parole e locuzioni tipiche dello spam, che viene effettuato in base a un dizionario speciale. Vengono sottoposte all'analisi sia le parole, espressioni e i caratteri visibili che quelli visivamente nascosti tramite espedienti tecnici speciali;
- **la tecnologia anti-scaming** — ai messaggi scamming e pharming appartengono le cosiddette "truffe alla nigeriana", i messaggi su vincite alla lotteria, al casinò, false email di banche. Per filtrare tali email, viene impiegato un modulo specifico;
- **il filtraggio dello spam tecnico** — i cosiddetti messaggi bounce nascono come una reazione ai virus o come una manifestazione dell'attività dei virus. Un modulo speciale dell'antispam identifica tali messaggi come indesiderati.

È possibile configurare i seguenti parametri di funzionamento di Antispam:

| Impostazione  | Descrizione  |
|---|--|
| Consenti testo in cirillico                             | È un'impostazione predefinita.<br><br>Questa impostazione comanda al monitor di posta SpIDer Mail di non classificare come spam senza una preliminare analisi le email scritte in una codifica cirillica stabilita. Se questo flag è deselezionato, il filtro con grande probabilità contrassegnerà tali email come lo spam.               |
| Consenti testo asiatico                                 | È un'impostazione predefinita.<br><br>Questa impostazione comanda al monitor di posta SpIDer Mail di non classificare come spam senza una preliminare analisi le email scritte nelle codifiche delle lingue asiatiche più comuni. Se questo flag è deselezionato, il filtro con grande probabilità contrassegnerà tali email come lo spam. |
| Aggiungi prefisso all'intestazione dei messaggi di spam | È un'impostazione predefinita. All'inizio dell'oggetto dei messaggi di spam viene aggiunta la sottostringa "[SPAM]".   |



| Impostazione | Descrizione  |
|--------------|--|
|              | <p>Questa impostazione comanda al monitor di posta SpIDer Mail di aggiungere il prefisso indicato agli oggetti delle email riconosciute come lo spam.</p> <p>L'aggiunta del prefisso aiuterà l'utente a creare le regole per il filtraggio delle email contrassegnate come spam in quei client di posta (per esempio, MS Outlook Express) in cui non è possibile configurare filtri per intestazione dell'email.</p> |

## Elaborazione delle email da parte del filtro antispam

Il monitor di posta SpIDer Mail aggiunge a tutte le email controllate le seguenti intestazioni:

- `X-DrWeb-SpamState`: `<valore>` dove `<valore>` indica se l'email è spam (`Yes`) secondo l'opinione del monitor di posta SpIDer Mail o se non lo è (`No`);
- `X-DrWeb-SpamVersion`: `<versione>` dove `<versione>` — la versione della libreria di Antispam Dr.Web;
- `X-DrWeb-SpamReason`: `<punteggio di spam>` dove `<punteggio di spam>` — l'elenco dei punteggi attribuiti all'email secondo le varie categorie di appartenenza allo spam.

Utilizzare queste intestazioni e il prefisso nell'oggetto dell'email (se il flag relativo è selezionato) per configurare il filtraggio dello spam da parte del programma di posta in uso.



Se per la ricezione delle email si usano i protocolli IMAP/NNTP, configurare il programma di posta in uso in modo che le email vengano caricate dal server di posta per intero, senza l'anteprima delle intestazioni. Questo è necessario per il corretto funzionamento del filtro antispam.

Per aumentare la qualità di funzionamento del filtro antispam, è possibile segnalare errori di riconoscimento dello spam.



Il filtro antispam processa messaggi di posta redatti in conformità con lo standard MIME RFC 822.

### Correzione di errori di riconoscimento

1. Quando si scopre un errore nel funzionamento del filtro antispam, creare una nuova email e allegarci il messaggio riconosciuto nel modo sbagliato. Le email inviate nel testo dell'email non verranno analizzate.
2. Inviare l'email con l'allegato all'amministratore della rete antivirus.

## 11.4. Scanner



La modifica delle impostazioni del componente è possibile se è stata autorizzata dall'amministratore del server di protezione centralizzata a cui Dr.Web si connette.

Per l'accesso alle impostazioni di Scanner viene richiesta la password se nella sezione [Impostazioni](#) è stata attivata l'opzione **Proteggi da password le impostazioni Dr.Web**.

Le impostazioni predefinite del programma sono ottimali per la maggior parte degli usi, non è consigliabile modificarle senza necessità.

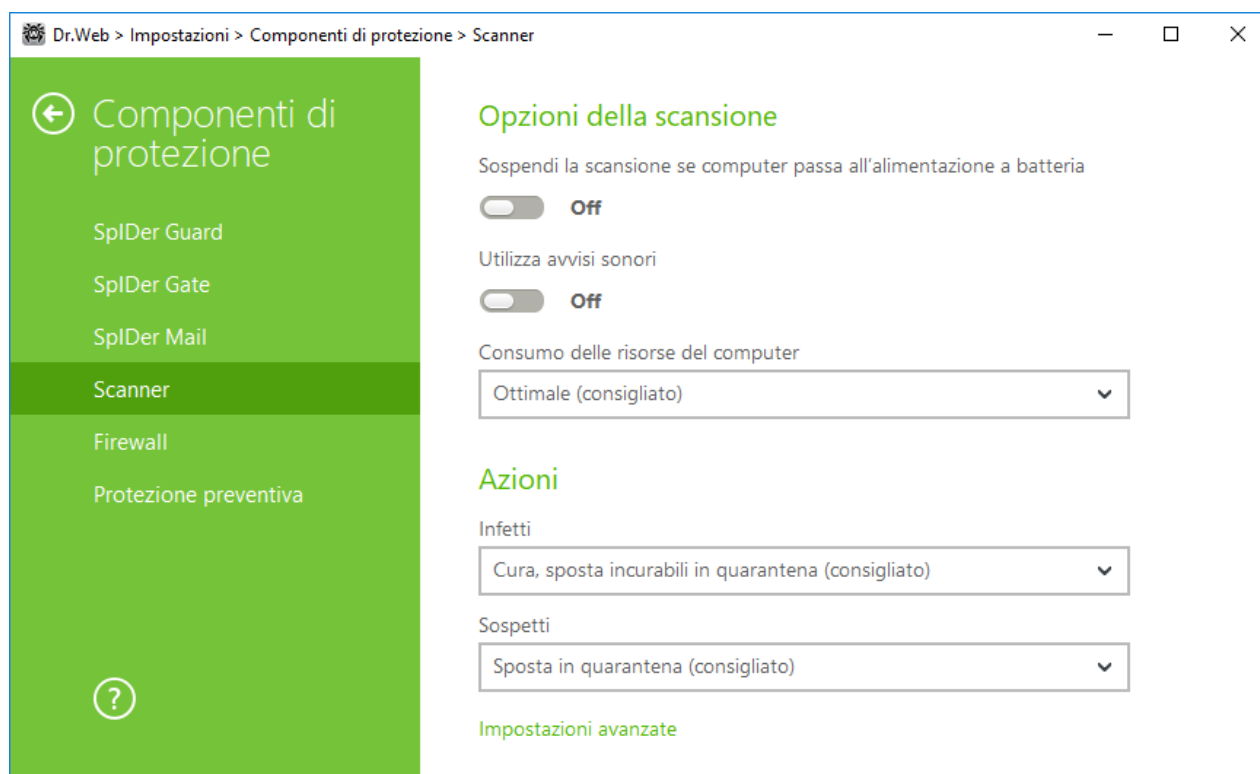


Immagine 30. Configurazione di Scanner

### Opzioni della scansione

In questo gruppo sono disponibili le impostazioni generali di funzionamento di Scanner Dr.Web:

- **Sospendi la scansione se computer passa all'alimentazione a batteria.** Attivare questa opzione affinché la scansione venga sospesa se il computer passa all'alimentazione a batteria. Di default l'opzione è disattivata.
- **Utilizza avvisi sonori.** Attivare questa opzione affinché Scanner Dr.Web accompagni ogni evento con un segnale sonoro. Di default l'opzione è disattivata.
- **Consumo delle risorse del computer.** Questa opzione imposta le restrizioni sul consumo delle risorse del computer da parte di Scanner Dr.Web. Di default, è impostato il valore ottimale.



## Azioni

In questa sezione viene configurata la reazione di Scanner al rilevamento dei file infetti o sospetti e dei programmi malevoli.

La reazione viene configurata separatamente per ciascuna categoria di oggetti:

- **Infetti** — oggetti infettati da un virus conosciuto e (presumibilmente) curabile;
- **Sospetti** — oggetti presumibilmente infettati da un virus o contenenti un oggetto malevolo;
- vari oggetti potenzialmente pericolosi.

È possibile modificare la reazione di Scanner al rilevamento di ciascun tipo di oggetti separatamente. Le reazioni possibili dipendono dal tipo di minaccia.

Di default Scanner cerca di curare i file infettati da un virus conosciuto e potenzialmente curabile e mette in [Quarantena](#) gli altri oggetti più pericolosi.

Esistono le seguenti azioni applicabili agli oggetti rilevati:

| Azione   | Descrizione   |
|--|---|
| Cura, sposta in quarantena<br>oggetti incurabili | Per ripristinare l'oggetto allo stato precedente all'infezione. Se il virus è incurabile o se il tentativo di trattamento non è riuscito, l'oggetto verrà spostato in quarantena.<br><br>Questa azione è disponibile solo per gli oggetti infettati da un virus conosciuto curabile, esclusi i trojan e i file infetti all'interno degli oggetti composti (archivi compressi, file di email o container di file). |
| Cura, rimuovi<br>oggetti incurabili              | Per ripristinare l'oggetto allo stato precedente all'infezione. Se il virus è incurabile o se il tentativo di trattamento non è riuscito, l'oggetto verrà rimosso.<br><br>Questa azione è disponibile solo per gli oggetti infettati da un virus conosciuto curabile, esclusi i trojan e i file infetti all'interno degli oggetti composti (archivi compressi, file di email o container di file).                |
| Rimuovi  | Per rimuovere l'oggetto.<br><br>Nessun'azione verrà eseguita in caso dei settori di avvio.  |
| Sposta in<br>quarantena                          | Per spostare l'oggetto nella cartella speciale <a href="#">Quarantena</a> .<br><br>Nessun'azione verrà eseguita in caso dei settori di avvio.   |
| Ignora   | Per saltare l'oggetto senza eseguire alcun'azione e per non visualizzare avvisi.<br><br>Questa azione è possibile solo per i programmi malevoli: adware, dialer, joke, riskware e hacktool.   |



| Azione  | Descrizione  |
|---------|--|
| Segnala | Per visualizzare un avviso e saltare l'oggetto senza eseguire alcun'azione.<br><br>Questa azione è possibile solo per gli oggetti sospetti e i programmi malevoli. |



Se il programma rileva un virus o un codice sospetto all'interno degli oggetti composti (archivi compressi, file di email o container di file), le azioni applicabili alle minacce all'interno di tali oggetti vengono eseguite con l'intero oggetto e non soltanto con la sua parte infetta.

## Impostazioni avanzate

Si può disattivare la scansione dei pacchetti di installazione, degli archivi compressi e dei file di email. Di default, la scansione di tali oggetti è attivata.

Si può inoltre configurare il comportamento di Scanner dopo la fine della scansione:

1. **Non applicare azione.** Scanner visualizzerà una tabella con la lista delle minacce rilevate.
2. **Neutralizza le minacce rilevate.** Scanner applicherà automaticamente le azioni alle minacce rilevate.
3. **Neutralizza le minacce rilevate e spegnerà il computer.** Scanner applicherà automaticamente le azioni alle minacce rilevate e quindi spegnerà il computer.

## 11.5. Firewall

Firewall Dr.Web è progettato per la protezione del computer da accessi non autorizzati dall'esterno e per la prevenzione della fuga di dati importanti via rete. Questo componente consente di controllare la connessione e il trasferimento di dati attraverso Internet e di bloccare le connessioni sospette a livello di pacchetto e applicazione.

Firewall fornisce i seguenti vantaggi:

- scansione e filtraggio di tutto il traffico in arrivo e in uscita;
- controllo delle connessioni a livello di applicazione;
- filtraggio dei pacchetti a livello di rete;
- un passaggio rapido da un set di regole a un altro;
- registrazione degli eventi.

### 11.5.1. Addestramento di Firewall

Dopo l'installazione di Firewall il programma viene addestrato per qualche tempo nel processo di utilizzo del computer. La modalità di training è disponibile per le seguenti modalità di



funzionamento di Firewall (per maggiori informazioni sulle modalità di funzionamento di Firewall vedi sezione [Configurazione di firewall](#)):

- **Consenti connessioni per le applicazioni affidabili** (impostata di default);
- **Modalità interattiva.**

In modalità **Consenti connessioni per le applicazioni affidabili** al rilevamento di un tentativo di connessione alla rete da parte del sistema o delle applicazioni, Firewall controlla se queste applicazioni sono affidabili e se le regole di filtraggio sono impostate per esse. Se non ci sono regole, Dr.Web visualizza un avviso corrispondente in cui è possibile impostare una regola. Per le applicazioni affidabili non vengono create regole. La connessione alla rete è consentita per tali applicazioni.

Alle applicazioni affidabili appartengono: le applicazioni di sistema o quelle che hanno il certificato Microsoft, nonché le applicazioni dalla lista delle applicazioni affidabili Dr.Web.

In modalità **Modalità interattiva**, quando Firewall rileva un tentativo da parte del sistema o di applicazioni di connettersi alla rete, Firewall controlla se le regole di filtraggio sono impostate per questi programmi. Se non ci sono regole, viene visualizzato un avviso corrispondente in cui è possibile impostare una regola. In seguito tali connessioni verranno elaborate in base a questa regola.



Se viene utilizzato un account limitato (Ospite), Firewall Dr.Web non visualizza avvisi di tentativi di accesso alla rete. Gli avvisi vengono visualizzati sotto l'account amministratore, se tale sessione è attiva allo stesso tempo della sessione ospite.

## Regole per le applicazioni

1. Quando si scopre un tentativo di connessione alla rete da parte di un'applicazione, leggere le seguenti informazioni:

| Campo                      | Descrizione  |
|----------------------------|--|
| Applicazione               | Il nome del programma. Assicurarsi che il percorso indicato nel campo <b>Percorso dell'applicazione</b> corrisponda alla posizione corretta del programma. |
| Percorso dell'applicazione | Il percorso completo del file eseguibile dell'applicazione e il suo nome.  |
| Firma digitale             | La firma digitale dell'applicazione.   |
| Indirizzo                  | Il protocollo e l'indirizzo dell'host a cui l'applicazione tenta di connettersi.   |
| Porta                      | La porta su cui l'applicazione tenta di connettersi.   |
| Direzione                  | La direzione della connessione.  |



2. Decidere sull'operazione adatta in questo caso e selezionare l'azione corrispondente nella parte inferiore della finestra:
  - per bloccare questa connessione una volta, selezionare l'azione **Vieta una volta**;
  - per consentire all'applicazione questa connessione una volta, selezionare l'azione **Consenti una volta**;
  - per andare al modulo di creazione della regola di filtraggio, selezionare l'azione **Crea regola**. Si apre una finestra in cui si può selezionare una regola predefinita o [creare manualmente una regola per le applicazioni](#).
3. Premere il pulsante **OK**. Firewall eseguirà l'operazione impostata e la finestra di avviso si chiuderà.



In alcuni casi, il sistema operativo Windows non consente di identificare in modo univoco un servizio che funziona come un processo di sistema. Quando Firewall scopre un tentativo di connessione da parte di un processo di sistema, notare la porta indicata nelle informazioni sulla connessione. Se si utilizza un'applicazione che può accedere alla porta indicata, consentire questa connessione.

Se il programma che tenta di stabilire una connessione è già conosciuta da Firewall (cioè sono impostate le relative regole di filtraggio), ma viene avviato da un'altra applicazione sconosciuta (processo padre), Firewall mostra un avviso corrispondente.

### Regole per i processi padre

1. Quando Firewall scopre un tentativo di connessione alla rete da parte di un'applicazione avviata da un programma sconosciuto da Firewall, leggere le informazioni sul file eseguibile del programma padre.
2. Quando si deciderà sull'operazione adatta in questo caso, eseguire una delle seguenti azioni:
  - per bloccare una volta solo la connessione dell'applicazione alla rete, premere il pulsante **Vieta**;
  - per consentire una volta solo all'applicazione di connettersi alla rete, premere il pulsante **Consenti**;
  - per creare una regola, premere **Crea regola** e nella finestra che si è aperta configurare le opportune [impostazioni per il processo padre](#).
3. Premere il pulsante **OK**. Firewall eseguirà l'operazione impostata e la finestra di avviso si chiuderà.

Inoltre, è possibile una situazione in cui un'applicazione sconosciuta viene avviata da un'altra applicazione sconosciuta, in tale caso l'avviso includerà le informazioni corrispondenti e in caso di selezione di **Crea regola** si aprirà una finestra in cui è possibile configurare le regole sia per le applicazioni che per i processi padre.

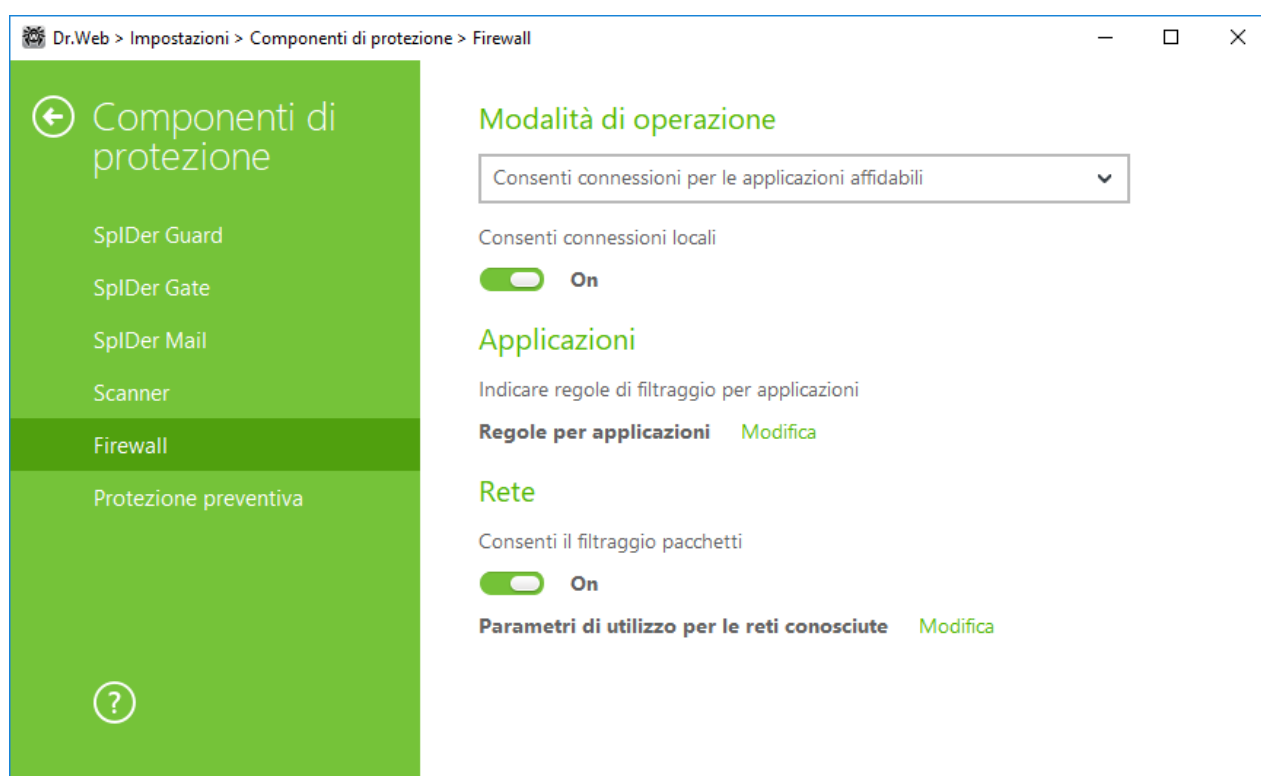
## 11.5.2. Configurazione di Firewall

In questa sezione è possibile configurare i seguenti parametri di funzionamento di Firewall:

- selezionare la modalità di funzionamento del programma;
- [configurare la lista](#) delle applicazioni autorizzate;
- configurare i parametri per le reti conosciute.



Per l'accesso alle impostazioni di Firewall viene richiesta la password se nella sezione [Impostazioni](#) è stata attivata l'opzione **Proteggi da password le impostazioni Dr.Web**.



**Immagine 31. Impostazioni principali di Firewall**

Di default Firewall non crea regole per le applicazioni conosciute. A prescindere dalla modalità di funzionamento si effettua la registrazione degli eventi.

Le impostazioni predefinite del programma sono ottimali per la maggior parte degli usi, non è consigliabile modificarle senza necessità.

L'impostazione **Consenti connessioni locali** permette a tutte le applicazioni di stabilire liberamente le connessioni locali (dall'interfaccia o all'interfaccia 127.0.0.1 (localhost)) sul computer. Questa opzione viene utilizzata dopo la verifica della conformità delle connessioni alle regole impostate. Disattivare questa opzione affinché le regole di filtraggio vengano utilizzate a prescindere da quello se una connessione avviene attraverso la rete o all'interno del computer.





## Selezione della modalità di funzionamento

Selezionare una delle seguenti modalità di funzionamento:

- **Consenti connessioni per le applicazioni affidabili** — una modalità in cui a tutte le applicazioni affidabili viene concesso l'accesso alle risorse di rete (si usa di default), nel caso di tutte le altre applicazioni viene visualizzato un avviso in cui è possibile impostare una regola (vedi sezione [Addestramento di Firewall](#));
- **Consenti connessioni sconosciute** — una modalità in cui a tutte le applicazioni sconosciute viene concesso l'accesso alle risorse di rete;
- **Modalità interattiva** — una [modalità di training](#) in cui all'utente viene concesso il completo controllo della reazione di Firewall;
- **Blocca connessioni sconosciute** — una modalità in cui vengono bloccate automaticamente tutte le connessioni sconosciute. Le connessioni conosciute vengono processate da Firewall sulla base delle regole di filtraggio impostate.

### Consenti connessioni per le applicazioni affidabili

Questa modalità si usa di default.

In questa modalità a tutte le applicazioni affidabili è consentito l'accesso alle risorse di rete, incluso Internet. Alle applicazioni affidabili appartengono: le applicazioni di sistema o quelle che hanno il certificato Microsoft, nonché le applicazioni dalla lista delle applicazioni affidabili Dr.Web. Le regole per le simili applicazioni non vengono visualizzate nella lista delle regole. Nel caso di altre applicazioni, Firewall fornisce la possibilità di proibire o consentire manualmente una connessione sconosciuta, e inoltre di creare per essa una regola.

Quando scopre un tentativo di accesso alle risorse di rete da parte del sistema operativo o di un'applicazione dell'utente, Firewall controlla se le regole di filtraggio sono impostate per questi programmi. Se non ci sono regole, viene mostrato un avviso corrispondente in cui è possibile selezionare una soluzione provvisoria o creare una regola secondo cui successivamente verranno processate tali connessioni.

### Consenti connessioni sconosciute

In questa modalità l'accesso alle risorse di rete, compreso Internet, viene concesso a tutte le applicazioni sconosciute per cui non sono impostate le regole di filtraggio. Quando scopre un tentativo di connessione, Firewall non mostra alcun avviso.

### Modalità interattiva

In questa modalità l'utente può controllare completamente la reazione di Firewall al rilevamento di una connessione sconosciuta e così addestrare il programma nel corso dell'utilizzo del computer.



Quando scopre un tentativo di accesso alle risorse di rete da parte del sistema operativo o di un'applicazione dell'utente, Firewall controlla se le regole di filtraggio sono impostate per questi programmi. Se non ci sono regole, viene mostrato un avviso corrispondente in cui è possibile selezionare una soluzione provvisoria o creare una regola secondo cui successivamente verranno processate tali connessioni.

### Blocca connessioni sconosciute

In questa modalità vengono bloccate automaticamente tutte le connessioni sconosciute alle risorse di rete, compreso Internet.

Quando scopre un tentativo di accesso alle risorse di rete da parte del sistema operativo o di un'applicazione dell'utente, Firewall controlla se le regole di filtraggio sono impostate per questi programmi. Se non ci sono regole di filtraggio, Firewall blocca automaticamente l'accesso alla rete e non visualizza alcun avviso. Se sono impostate le regole di filtraggio per questa connessione, vengono eseguite le azioni indicate nelle regole.

## Parametri per le applicazioni



Per ciascun programma non può esserci più di un set di regole di filtraggio.

Tramite il filtraggio a livello di applicazione è possibile controllare l'accesso di specifici programmi e processi alle risorse di rete, nonché consentire o proibire a queste applicazioni di avviare altri processi. È possibile impostare regole sia per le applicazioni dell'utente che per quelle di sistema.

In questa sezione è possibile gestire i [set di regole di filtraggio](#), creando nuove regole, modificando quelle esistenti o eliminando regole non richieste. Un'applicazione viene identificata in modo univoco dal percorso completo del file eseguibile. Per indicare il kernel del sistema operativo Microsoft Windows (il processo system per cui non c'è il file eseguibile corrispondente) si usa il nome `SYSTEM`.





Se si è creata una regola di blocco per un processo o si è impostata la modalità Blocca connessioni sconosciute e quindi si è disattivata la regola di blocco o si è modificata la modalità di funzionamento, il blocco rimarrà attivo fino al prossimo tentativo di connessione dopo il riavvio del processo.

Per le applicazioni che sono già rimosse dal computer le regole non vengono rimosse automaticamente. È possibile rimuovere tali regole, selezionando la voce **Rimuovi le regole non utilizzate** nel menu contestuale della lista.



## Regole per le applicazioni

Nella finestra **Nuovo set di regole per l'applicazione** (o **Modifica del set di regole**) è possibile configurare l'accesso di un'applicazione alle risorse di rete e inoltre proibire o consentire l'avvio di altre applicazioni.

Per accedere a questa finestra, nelle [impostazioni](#) di Firewall nella voce **Regole per le applicazioni** premere **Modifica** e nella finestra comparsa premere il pulsante  o selezionare un'applicazione e premere il pulsante .

Quando Firewall funziona in [modalità di training](#), è possibile cominciare a creare una regola direttamente dalla finestra dell'avviso che informa di un tentativo di una connessione non autorizzata.

## Avvio di altre applicazioni

Per consentire o proibire a un'applicazione di avviare altre applicazioni, dalla lista a cascata **Avvio delle applicazioni di rete** selezionare:

- **Consenti** per consentire all'applicazione di avviare processi;
- **Proibisci** per proibire all'applicazione di avviare processi;
- **Non impostato**. In questo caso a questa applicazione vengono applicate le impostazioni della [modalità di funzionamento](#) di Firewall selezionata.

## Accesso alle risorse di rete

1. Selezionare la modalità di accesso alle risorse di rete:

- **Consenti tutto** — tutte le connessioni dell'applicazione saranno consentite;
- **Blocca tutto** — tutte le connessioni dell'applicazione sono proibite;
- **Non impostato**. In questo caso a questa applicazione vengono applicate le impostazioni della [modalità di funzionamento](#) di Firewall selezionata.
- **Personalizzato** — in questa modalità è possibile creare un set di regole che autorizzano o proibiscono alcune connessioni dell'applicazione.

2. Se è selezionata la modalità di accesso alle risorse di rete **Personalizzato**, più in basso viene visualizzata una tabella con le informazioni sul set di regole per questa applicazione.

| Parametro | Descrizione   |
|-----------|---|
| Attivato  | Stato della regola.   |
| Azione    | Indica l'azione eseguita da Firewall quando un programma tenta di connettersi a Internet: <ul style="list-style-type: none"><li>• <b>Blocca pacchetti</b> — blocca il tentativo di connessione;</li></ul> |



| Parametro           | Descrizione  |
|---------------------|--|
|                     | <ul style="list-style-type: none"><li>• <b>Consenti pacchetti</b> — consenti la connessione.</li></ul>   |
| Nome regola         | Il nome della regola.  |
| Tipo di connessione | La direzione della connessione: <ul style="list-style-type: none"><li>• <b>In arrivo</b> — la regola si applica se una connessione viene avviata dalla rete a un programma sul computer;</li><li>• <b>In uscita</b> — la regola si applica se una connessione viene avviata da un programma sul computer;</li><li>• <b>Qualsiasi</b> — la regola si applica a prescindere dalla direzione della connessione.</li></ul> |
| Descrizione         | Una descrizione della regola da parte dell'utente.   |



3. Se necessario, modificare un set di regole predefinito o creare un nuovo set di regole per l'applicazione.
4. Se si è scelta la creazione di una nuova regola o la modifica di una regola esistente, [configurarne i parametri](#) nella finestra che si è aperta.
5. Dopo aver finito di modificare un set di regole, premere il pulsante **OK** per salvare le modifiche apportate o il pulsante **Annulla** per rifiutare le modifiche. Le modifiche apportate a un set di regole vengono salvate se si passa a un'altra modalità.

Spuntare il flag **Chiedi conferma in caso di modificazione dell'oggetto (consigliato)** se si vuole che l'accesso alle risorse di rete per un'applicazione venga nuovamente richiesto durante una modifica o un aggiornamento delle applicazioni.

## Configurazione dei parametri della regola

Le regole di filtraggio regolano la comunicazione di rete di un programma con specifici host sulla rete.

### Creazione e modifica di una regola

Per aggiungere una nuova regola, nella finestra **Modifica del set di regole** premere il pulsante . Per modificare una regola esistente, selezionare la regola desiderata e premere il pulsante . In tale caso nella voce **Accesso alle risorse di rete** deve essere selezionata la modalità **Personalizzato**.

Impostare i seguenti parametri della regola:

| Parametro       | Descrizione |
|-----------------|-------------|
| <b>Generale</b> |             |



| Parametro                        | Descrizione  |
|----------------------------------|--|
| Nome regola                      | Il nome della regola che viene creata/modificata.  |
| Descrizione                      | Una breve descrizione della regola.  |
| Azione                           | Indica l'azione eseguita da Firewall quando un programma tenta di connettersi a Internet: <ul style="list-style-type: none"><li>• <b>Blocca pacchetti</b> — blocca il tentativo di connessione;</li><li>• <b>Consenti pacchetti</b> — autorizza la connessione.</li></ul>  |
| Stato                            | Stato della regola: <ul style="list-style-type: none"><li>• <b>Attivato</b> — la regola viene applicata;</li><li>• <b>Disattivato</b> — la regola temporaneamente non viene applicata.</li></ul>   |
| Tipo di connessione              | La direzione della connessione: <ul style="list-style-type: none"><li>• <b>In arrivo</b> — la regola si applica se una connessione viene avviata dalla rete a un programma sul computer;</li><li>• <b>In uscita</b> — la regola si applica se una connessione viene avviata da un programma sul computer;</li><li>• <b>Qualsiasi</b> — la regola si applica a prescindere dalla direzione della connessione.</li></ul>   |
| Registrazione del log            | Modalità di registrazione del log: <ul style="list-style-type: none"><li>• <b>Attivato</b> — registra eventi;</li><li>• <b>Disattivato</b> — non salvare informazioni sulla regola.</li></ul>  |
| <b>Impostazioni della regola</b> |  |
| Protocollo                       | I protocolli del livello di rete e di trasporto attraverso cui avviene la connessione.<br><br>Sono supportati i seguenti protocolli del livello di rete: <ul style="list-style-type: none"><li>• IPv4;</li><li>• IPv6;</li><li>• IP all — un protocollo IP di qualsiasi versione.</li></ul> Sono supportati i seguenti protocolli del livello di trasporto: <ul style="list-style-type: none"><li>• TCP;</li><li>• UDP;</li><li>• TCP &amp; UDP — protocollo TCP o UDP;</li><li>• RAW.</li></ul> |



| Parametro                         | Descrizione   |
|-----------------------------------|---|
| Indirizzo locale/Indirizzo remoto | <p>L'indirizzo IP dell'host remoto che partecipa alla connessione. È possibile indicare sia uno specifico indirizzo (<b>Pari a</b>) che un intervallo di indirizzi (<b>Nell'intervallo</b>), nonché una maschera di una specifica sottorete (<b>Maschera</b>) o maschere di tutte le sottoreti in cui il computer ha un indirizzo di rete (<b>MY_NETWORK</b>).</p> <p>Per impostare la regola per tutti gli host, selezionare la variante <b>Qualsiasi</b>.</p> |
| Porta locale/Porta remota         | <p>La porta su cui avviene la connessione. È possibile indicare sia una specifica porta (<b>Pari a</b>) che un intervallo di porte (<b>Nell'intervallo</b>).</p> <p>Per impostare la regola per tutte le porte, selezionare la variante <b>Qualsiasi</b>.</p>   |

## Parametri per le reti

Il filtraggio a livello di pacchetto consente di controllare l'accesso alla rete a prescindere dai programmi che avviano la connessione. Le regole vengono applicate a tutti i pacchetti di rete di un determinato tipo che vengono trasmessi tramite una delle interfacce di rete del computer.

Questo tipo di filtraggio fornisce metodi di controllo generali a differenza del [filtraggio a livello di applicazione](#).

## Filtro dei pacchetti

Nella finestra **Rete** è possibile impostare un set di regole di filtraggio dei pacchetti trasmessi attraverso una specifica interfaccia.


Per accedere a questa finestra, nella finestra delle impostazioni di Firewall nella voce **Parametri di utilizzo per le reti conosciute** premere **Modifica**. Trovare nella lista l'interfaccia desiderata e correlarci il set di regole corrispondente. Se nella lista non è disponibile un set di regole adatto, creare tale set.


Firewall viene fornito con i seguenti set di regole predefiniti:

- **Default Rule** — le regole che descrivono le configurazioni di rete più comuni ed attacchi diffusi (si usa di default per tutte le nuove [interfacce](#));
- **Allow All** — tutti i pacchetti vengono consentiti;
- **Block All** — tutti i pacchetti vengono bloccati.

Per un utilizzo comodo e un passaggio veloce tra le modalità di filtraggio, si possono impostare [ulteriori set di regole](#).



Per vedere tutte le interfacce disponibili o per aggiungere alla tabella una nuova interfaccia, premere il pulsante . Nella finestra che si è aperta è possibile indicare quali interfacce devono essere sempre visualizzate nella tabella. Le interfacce attive sono automaticamente visualizzate nella tabella.

Le interfacce di rete non attive possono essere cancellate dalla tabella visualizzata, premendo il pulsante .

### Impostazioni del filtro pacchetti





Per gestire i set di regole esistenti e per aggiungerne nuovi, passare alla finestra **Impostazioni del filtro pacchetti**, premendo il pulsante **Set di regole**.

Su questa pagina è possibile:

- [gestire](#) i set di regole di filtraggio, creandone nuovi, modificando quelli esistenti o eliminando regole non richieste;
- [impostare](#) i parametri di filtraggio aggiuntivi.

### Gestione del set di regole

Per gestire un set di regole, eseguire una delle seguenti azioni:

- per creare un set di regole per un'interfaccia di rete, premere ;
- per modificare un set di regole esistente, selezionarlo dalla lista e premere ;
- per aggiungere una copia di un set di regole esistente, premere . La copia viene aggiunta sotto il set di regole selezionato;
- per eliminare un set di regole selezionato, premere .

### Impostazioni avanzate

Per configurare le impostazioni avanzate del filtraggio dei pacchetti, nella finestra **Impostazioni del filtro pacchetti** selezionare i seguenti flag:

| Flag                                    | Descrizione  |
|---|--|
| Attiva filtraggio di pacchetti dinamico | <p>Spuntare questo flag per tenere conto dello stato della connessione TCP nel filtraggio e per far passare solo i pacchetti di cui il contenuto corrisponde allo stato attuale. In tale caso vengono bloccati tutti i pacchetti che vengono trasmessi nei limiti della connessione ma non soddisfano le specifiche del protocollo. Questo meccanismo consente di proteggere meglio il computer dagli attacchi DoS (Denial of Service, Negazione del servizio), dalla scansione delle risorse, dall'introduzione di dati e da altre operazioni malevole.</p> <p>Inoltre, è consigliabile selezionare questo flag se vengono utilizzati i protocolli con algoritmi complessi di trasmissione di dati (FTP, SIP ecc.).</p> |



| Flag                             | Descrizione  |
|----------------------------------|--|
|                                  | Deselezionare questo flag per filtrare pacchetti senza tenere conto delle connessioni TCP.   |
| Elabora pacchetti IP frammentati | Spuntare questo flag per elaborare correttamente la trasmissione di grandi quantità di dati. La dimensione massima del pacchetto (MTU — Maximum Transmission Unit) può variare in diverse reti, perciò nella trasmissione alcuni pacchetti IP possono essere suddivisi in più frammenti. In caso di utilizzo di questa opzione, a tutti i pacchetti frammentati viene applicata la stessa azione prevista dalle regole di filtraggio per il pacchetto principale (il primo).<br><br>Deselezionare questo flag per elaborare tutti i pacchetti separatamente. |

Premere il pulsante **OK** per salvare le modifiche apportate o il pulsante **Annulla** per uscire dalla finestra senza salvare le modifiche.

Nella finestra **Modifica del set di regole** viene visualizzata una lista delle regole di filtraggio pacchetti, incluse in uno specifico set. Si può gestire la lista aggiungendo nuove regole o modificando quelle esistenti, nonché si può cambiare l'ordine di esecuzione delle regole. Le regole vengono applicate consecutivamente secondo l'ordine nella lista.

Per ogni regola nella lista vengono fornite le seguenti brevi informazioni:

| Parametro             | Descrizione  |
|-----------------------|--|
| Attivato              | Stato della regola.  |
| Azione                | Indica l'azione eseguita da Firewall quando elabora un pacchetto: <ul style="list-style-type: none"><li>• <b>Blocca pacchetti</b> — blocca il pacchetto;</li><li>• <b>Consenti pacchetti</b> — trasmetti il pacchetto.</li></ul>   |
| Nome regola           | Il nome della regola.  |
| Direzione             | La direzione della connessione: <ul style="list-style-type: none"><li>•  — la regola si applica se il pacchetto viene ricevuto dalla rete;</li><li>•  — la regola si applica se il pacchetto viene inviato dal computer;</li><li>•  — la regola si applica a prescindere dalla direzione della connessione.</li></ul> |
| Registrazione del log | Modalità di registrazione di eventi. Indica quali informazioni devono essere registrate nel log: <ul style="list-style-type: none"><li>• <b>Soltanto le intestazioni</b> — registra nel log soltanto le intestazioni dei pacchetti;</li><li>• <b>Pacchetto intero</b> — registra nel log il pacchetto per intero;</li><li>• <b>Disattivato</b> — non salvare informazioni sul pacchetto.</li></ul>   |





| Parametro   | Descrizione                         |
|-------------|-------------------------------------|
| Descrizione | Una breve descrizione della regola. |

### Modifica e creazione di un set di regole

1. Se necessario, impostare un nome o modificare il nome del set di regole.
2. Creare regole di filtraggio, utilizzando le seguenti opzioni:
  - per aggiungere una nuova regola, premere . La regola viene aggiunta in cima alla lista;
  - per modificare una regola selezionata, premere ;
  - per aggiungere una copia di una regola selezionata, premere il pulsante . La copia viene aggiunta davanti alla regola selezionata;
  - per eliminare una regola selezionata, premere .
3. Se si è scelta la creazione di una nuova regola o la modifica di una regola esistente, [configurarne i parametri](#).
4. Utilizzare le frecce a destra della lista per definire l'ordine di esecuzione delle regole. Le regole vengono eseguite consecutivamente secondo l'ordine nella lista.
5. Dopo aver finito di modificare la lista, premere il pulsante **OK** per salvare le modifiche apportate o il pulsante **Annulla** per rifiutare le modifiche.



I pacchetti per cui non ci sono regole nel set vengono bloccati automaticamente. Le eccezioni sono i pacchetti che vengono autorizzati dalle regole nel [Filtro delle applicazioni](#).

### Aggiunta o modifica di una regola di filtraggio

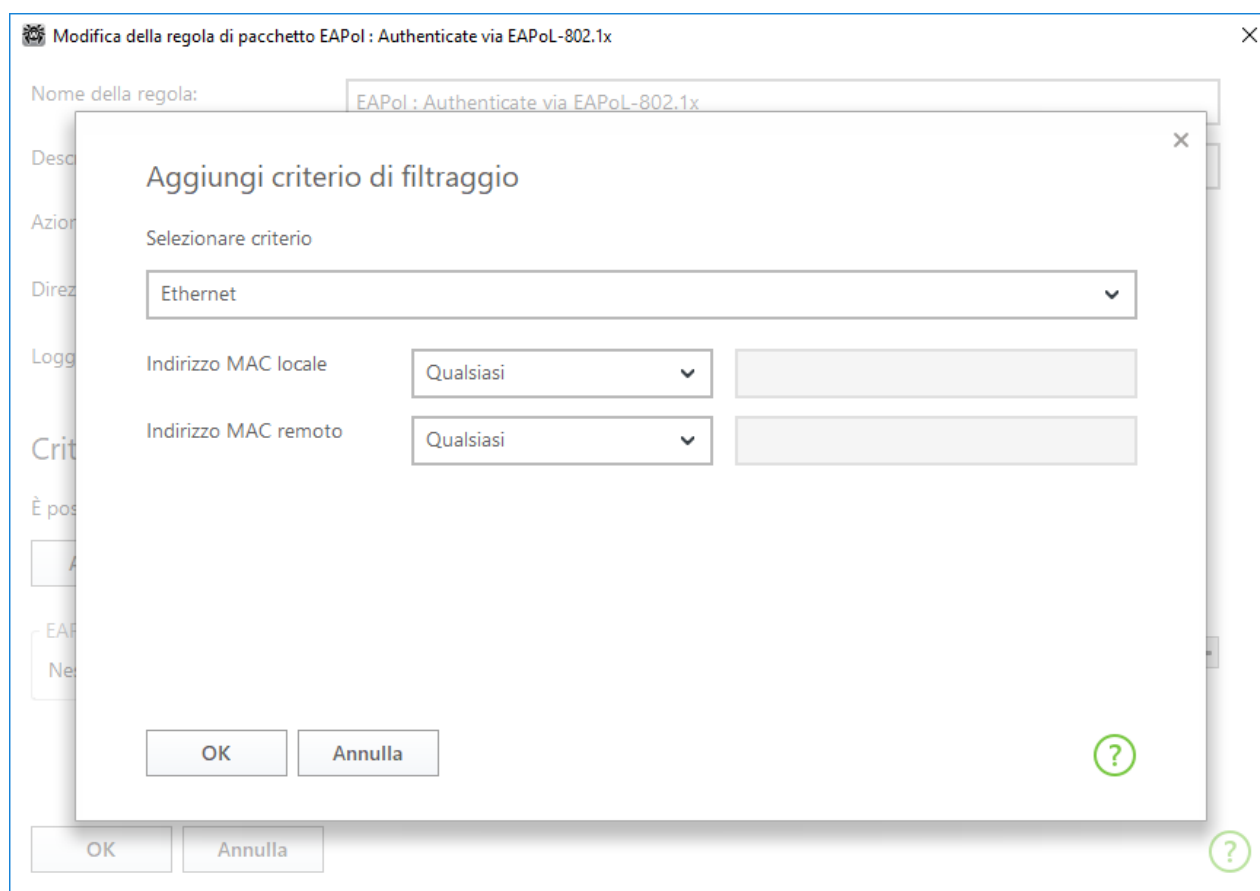
1. Nella finestra di configurazione del set di regole per il filtro dei pacchetti premere il pulsante o il pulsante . Si apre la finestra di creazione o modifica della regola di filtraggio pacchetti.
2. Impostare i seguenti parametri della regola:

| Parametro   | Descrizione  |
|-------------|--|
| Nome regola | Il nome della regola che viene creata/modificata.  |
| Descrizione | Una breve descrizione della regola.  |
| Azione      | Indica l'azione eseguita da Firewall quando elabora un pacchetto: <ul style="list-style-type: none"><li>• <b>Blocca pacchetti</b> — blocca il pacchetto;</li><li>• <b>Consenti pacchetti</b> — trasmetti il pacchetto.</li></ul> |



| Parametro             | Descrizione  |
|-----------------------|--|
| Direzione             | La direzione della connessione: <ul style="list-style-type: none"><li>• <b>In arrivo</b> — la regola si applica se il pacchetto viene ricevuto dalla rete;</li><li>• <b>In uscita</b> — la regola si applica se il pacchetto viene inviato dal computer;</li><li>• <b>Qualsiasi</b> — la regola si applica a prescindere dalla direzione della connessione.</li></ul>                              |
| Registrazione del log | Modalità di registrazione di eventi. Indica quali informazioni devono essere registrate nel log: <ul style="list-style-type: none"><li>• <b>Pacchetto intero</b> — registra nel log il pacchetto per intero;</li><li>• <b>Soltanto le intestazioni</b> — registra nel log soltanto le intestazioni dei pacchetti;</li><li>• <b>Disattivato</b> — non salvare informazioni sul pacchetto.</li></ul> |

3. Se necessario, aggiungere un criterio di filtraggio, per esempio, un protocollo di trasporto o di rete, premendo il pulsante **Aggiungi criterio**. Si aprirà la finestra **Aggiungi criterio di filtraggio**:



**Immagine 32. Aggiunta di un criterio di filtraggio**



Selezionare il criterio desiderato nella lista a cascata. Nella stessa finestra è possibile configurare i parametri per il criterio selezionato. È possibile aggiungere qualsiasi numero desiderato di criteri. In tale caso, affinché l'azione dalla regola venga applicata a un pacchetto, il pacchetto deve soddisfare tutti i criteri della regola.

Per alcune intestazioni sono disponibili criteri di filtraggio aggiuntivi. Tutti i criteri aggiunti vengono visualizzati nella finestra di modifica della regola di pacchetto e sono modificabili.

4. Dopo aver finito di modificare, premere il pulsante **OK** per salvare le modifiche apportate o il pulsante **Annulla** per uscire dalla finestra senza salvare le modifiche.



Se non è stato aggiunto alcun criterio di filtraggio, questa regola consentirà o bloccherà tutti i pacchetti (a seconda dell'impostazione nel campo **Azione**).

Se in questa regola all'interno dell'intestazione IPv4 per i parametri **Indirizzo IP locale** e **Indirizzo IP remoto** viene impostato il valore **Qualsiasi**, la regola funzionerà per qualsiasi pacchetto che contenga l'intestazione IPv4 e che sia stato inviato da un indirizzo fisico di un computer locale.

## 11.6. Dr.Web per Microsoft Outlook

### Funzioni principali del componente

Il plugin Dr.Web per Outlook svolge le seguenti funzioni:

- scansione antivirus dei file allegati alle email in arrivo;
- controllo antispam delle email;
- rilevamento e neutralizzazione di programmi malevoli;
- impiega l'analisi euristica per fornire un'ulteriore protezione contro i virus sconosciuti.

### Configurazione del plugin Dr.Web per Outlook

La configurazione dei parametri e la visualizzazione delle statistiche di funzionamento del programma sono disponibili attraverso l'applicazione di posta Microsoft Outlook sezione **Servizi** → **Impostazioni** → scheda **Antivirus Dr.Web** (in caso di Microsoft Outlook 2010 sezione **File** → **Impostazioni** → **Estensioni** selezionare il plugin Dr.Web per Outlook e premere il pulsante **Impostazioni dell'estensione**).



La scheda **Antivirus Dr.Web** nelle impostazioni dell'applicazione Microsoft Outlook è disponibile solo se l'utente ha i permessi per la modifica di queste impostazioni.

Nella scheda **Antivirus Dr.Web** viene visualizzato lo stato attuale della protezione (attivata/disattivata). Inoltre, dalla scheda si può accedere alle seguenti funzioni del programma:

- **Log** — consente di configurare la registrazione degli eventi del programma;



- [Controllo allegati](#) — consente di configurare la scansione della posta elettronica e definire le azioni del programma eseguite sugli oggetti malevoli rilevati;
- [Filtro antispam](#) — consente di definire le azioni del programma eseguite sui messaggi di spam, nonché di creare una white list e black list di indirizzi email;
- [Statistiche](#) — visualizza i dati sugli oggetti controllati e processati dal programma.

## 11.6.1. Scansione antivirus

Dr.Web per Outlook impiega diversi [metodi di rilevamento dei virus](#). Agli oggetti malevoli trovati vengono applicate le azioni definite dall'utente: il programma può curare oggetti infetti, eliminarli o spostarli in [Quarantena](#) per isolarli e conservarli in sicurezza.

Il programma Dr.Web per Outlook rileva i seguenti oggetti malevoli:

- oggetti infetti;
- file-bomba o archivi-bomba;
- adware;
- hacktool;
- dialer;
- joke;
- riskware;
- spyware;
- trojan;
- worm e virus.

### Azioni

Dr.Web per Outlook consente di configurare la reazione del programma ai file infetti o sospetti e programmi malevoli rilevati durante il controllo degli allegati della posta elettronica.

Per configurare la scansione degli allegati e definire le azioni che il programma applicherà agli oggetti malevoli rilevati, nell'applicazione di posta Microsoft Outlook selezionare **Servizi** → **Impostazioni** → scheda **Antivirus Dr.Web** (in caso di Microsoft Outlook 2010 sezione **File** → **Impostazioni** → **Estensioni** selezionare il plugin Dr.Web per Outlook e premere il pulsante **Impostazioni dell'estensione**) e premere il pulsante **Scansione allegati**.



La finestra **Scansione allegati** è disponibile solo se l'utente possiede i permessi dell'amministratore del sistema.

Nel sistema operativo Windows Vista e superiori, quando si fa clic sul pulsante **Scansione allegati**:



- Se l'UAC è attivato: all'amministratore viene visualizzata una richiesta per confermare le azioni del programma, a un utente senza i permessi di amministratore viene visualizzata una richiesta per inserire le credenziali dell'amministratore del sistema;
- Se l'UAC è disattivato: l'amministratore può modificare le impostazioni del programma, un utente non può avere l'accesso alla modifica delle impostazioni.

Nella finestra **Scansione allegati** è possibile configurare le azioni che il programma applicherà a diverse categorie di oggetti controllati, nonché le azioni per il caso di un errore di scansione. Inoltre, si può attivare o disattivare la scansione degli archivi.

### Per impostare le azioni da applicare a oggetti malevoli rilevati, si utilizzano le seguenti impostazioni:

- la lista a cascata **Infetti** imposta la reazione al rilevamento degli oggetti infettati dai virus conosciuti e (presumibilmente) curabili;
- la lista a cascata **Non curati** imposta la reazione al rilevamento degli oggetti infettati da un virus conosciuto incurabile, nonché per i casi quando il tentativo di cura non è riuscito;
- la lista a cascata **Sospetti** imposta la reazione al rilevamento degli oggetti presumibilmente infettati da un virus (rilevati tramite l'analisi euristica);
- la sezione **Programmi malevoli** imposta la reazione al rilevamento dei seguenti software indesiderati:
  - adware;
  - dialer;
  - joke;
  - hacktool;
  - riskware;
- la lista a cascata **Se la scansione va in errore** consente di configurare le azioni del programma per il caso se la scansione dell'allegato non è possibile, per esempio se l'allegato è un file corrotto o un file protetto da password;
- il flag **Controlla archivi** consente di attivare o disattivare la scansione dei file allegati che sono archivi compressi. Impostare questo flag per attivare la scansione — togliere la spunta per disattivarla.

Le reazioni disponibili dipendono dal tipo di evento di virus.

### Sono previste le seguenti azioni applicabili agli oggetti rilevati:

- **Cura** (l'azione è disponibile soltanto per gli oggetti infetti) — significa che il programma tenterà di curare l'oggetto infetto;
- **Come per non curati** (l'azione è disponibile soltanto per gli oggetti infetti) — significa che all'allegato infetto verrà applicata l'azione selezionata per gli oggetti non curati;
- **Elimina** — significa che l'oggetto verrà eliminato;



- **Sposta in quarantena** — significa che l'oggetto verrà isolato nella cartella di [Quarantena](#);
- **Salta** — significa che l'oggetto verrà saltato senza modifiche.

## 11.6.2. Controllo antispam

Dr.Web per Outlook cerca lo spam in tutti i messaggi di posta tramite Antispam Dr.Web e filtra i messaggi in base alle [impostazioni](#) definite dall'utente.

Per configurare la scansione antispam dei messaggi, nell'applicazione di posta Microsoft Outlook selezionare **Servizi** → **Impostazioni** → scheda **Antivirus Dr.Web** (in caso di Microsoft Outlook 2010 sezione **File** → **Impostazioni** → **Estensioni** selezionare il plugin Dr.Web per Outlook e premere il pulsante **Impostazioni dell'estensione**) e premere il pulsante **Filtro antispam**. Si apre la finestra di configurazione del [Filtro antispam](#).



La finestra **Filtro antispam** è disponibile solo se l'utente possiede i permessi dell'amministratore del sistema.

Nel sistema operativo Windows Vista e superiori, quando si fa clic sul pulsante **Filtro antispam**:

- se l'UAC è attivato: all'amministratore viene visualizzata una richiesta per confermare le azioni del programma, a un utente senza i permessi di amministratore viene visualizzata una richiesta per inserire le credenziali dell'amministratore del sistema;
- se l'UAC è disattivato: l'amministratore può modificare le impostazioni del programma, un utente non può avere l'accesso alla modifica delle impostazioni.

## Configurazione del filtro antispam

**Per configurare i parametri del filtro antispam:**

- Spuntare il flag **Controlla spam nelle email** per attivare il filtro antispam.
- Se si vuole aggiungere uno specifico testo all'intestazione del messaggio riconosciuto come lo spam, spuntare il flag **Aggiungi un prefisso all'oggetto dei messaggi**. Il testo da aggiungere può essere immesso nel campo di testo a destra del flag. Di default viene aggiunto il prefisso **\*\*\*SPAM\*\*\***.
- I messaggi controllati possono essere contrassegnati come letti nelle proprietà dell'email. A tale scopo è necessario impostare il flag **Segna il messaggio come già letto**. Di default, il flag **Segna il messaggio come già letto** è impostato.
- Inoltre è possibile configurare le [white list e black list](#) per eseguire il filtraggio delle email.



Se alcune email sono state riconosciute in modo sbagliato, è possibile inoltrarle all'amministratore della rete antivirus.



## White list e black list

La white list e la black list di indirizzi email vengono utilizzate per filtrare i messaggi.

Per visualizzare e modificare la white list o la black list, nelle [impostazioni del filtro antispam](#) premere rispettivamente il pulsante **White list** o **Black list**.

### Per aggiungere un indirizzo alla white list o black list:

1. Premere il pulsante **Aggiungi**.
2. Immettere l'indirizzo email nel campo appropriato.
3. Premere il pulsante **OK** nella finestra **Modifica la lista**.

### Per modificare un indirizzo nella lista:

1. Selezionare l'indirizzo nella lista, premere il **Modifica**.
2. Modificare le informazioni desiderate.
3. Premere il pulsante **OK** nella finestra **Modifica la lista**.

### Per cancellare un indirizzo dalla lista:

1. Selezionare l'indirizzo nella lista.
2. Premere il pulsante **Rimuovi**.

Nella finestra **White list e black list** premere il pulsante **OK** per salvare le modifiche apportate.

## White list

Se l'indirizzo di un mittente è aggiunto alla white list, la relativa email non viene analizzata tramite Antispam. Tuttavia, se il nome a dominio degli indirizzi del destinatario e del mittente coincidono e questo nome a dominio è inserito nella white list con l'utilizzo del carattere "\*", l'email viene controllata tramite Antispam. Metodi di immissione:

- per aggiungere alla lista un determinato mittente, immettere il suo indirizzo email completo (per esempio `mail@example.net`). Tutte le email ricevute da questo indirizzo verranno consegnate senza controllo antispam;
- ciascun elemento della lista può contenere soltanto un indirizzo email o una maschera di indirizzi email;
- per aggiungere alla lista dei mittenti un determinato tipo di indirizzi, immettere una maschera che definisce questi indirizzi. La maschera imposta un template per la determinazione dell'oggetto. Può includere caratteri normali ammissibili negli indirizzi email, nonché il carattere specifico "\*" che sostituisce qualsiasi sequenza di caratteri (anche una vuota).

Per esempio sono ammissibili le seguenti varianti:

- `mailbox@domain.com`



- `*box@domain.com`
- `mailbox@dom*`
- `*box@dom*`



Il carattere "\*" può essere messo soltanto all'inizio o alla fine di un indirizzo.

Il carattere "@" è obbligatorio.

- per assicurarsi di ricevere le email dagli indirizzi email in uno specifico dominio, utilizzare il carattere "\*" invece del nome utente. Per esempio per ricevere tutte le email dai mittenti nel dominio `example.net`, immettere `*@example.net`;
- per assicurarsi di ricevere le email dagli indirizzi email con uno specifico nome utente da qualsiasi dominio, utilizzare il carattere "\*" invece del nome a dominio. Per esempio per ricevere tutte le email dai mittenti con il nome della casella di posta "ivanov", immettere `ivanov@*`.

## Black list

Se l'indirizzo di un mittente è aggiunto alla black list, lo status di spam viene attribuito alla relativa email senza ulteriore analisi. Metodi di immissione:

- per aggiungere alla lista un determinato mittente, immettere il suo indirizzo email completo (per esempio `spam@spam.it`). Tutte le email ricevute da questo indirizzo verranno riconosciute automaticamente come lo spam;
- ciascun elemento della lista può contenere soltanto un indirizzo email o una maschera di indirizzi email;
- per aggiungere alla lista dei mittenti un determinato tipo di indirizzi, immettere una maschera che definisce questi indirizzi. La maschera imposta un template per la determinazione dell'oggetto. Può includere caratteri normali ammissibili negli indirizzi email, nonché il carattere specifico "\*" che sostituisce qualsiasi sequenza di caratteri (anche una vuota).

Per esempio sono ammissibili le seguenti varianti:

- `mailbox@domain.com`
- `*box@domain.com`
- `mailbox@dom*`
- `*box@dom*`



Il carattere "\*" può essere messo soltanto all'inizio o alla fine di un indirizzo.

Il carattere "@" è obbligatorio.

- per assicurarsi di contrassegnare come lo spam le email dagli indirizzi email in uno specifico dominio, utilizzare il carattere "\*" invece del nome utente. Per esempio per contrassegnare come lo spam tutte le email dai mittenti nel dominio `spam.it`, immettere `*@spam.it`;





- per assicurarsi di contrassegnare come lo spam le email dagli indirizzi email con uno specifico nome utente da qualsiasi dominio, utilizzare il carattere "\*" invece del nome a dominio. Per esempio per contrassegnare come lo spam tutte le email dai mittenti con il nome della casella di posta "ivanov", immettere `ivanov@*`;
- gli indirizzi dal dominio del destinatario non vengono processati. Per esempio se la casella di posta del destinatario (cioè dell'utente) si trova nel dominio mail.it, le email inviate dal dominio mail.it non verranno processate dal filtro antispam.

### 11.6.3. Registrazione degli eventi

Dr.Web per Outlook registra errori ed eventi nei seguenti log:

- [log di registrazione degli eventi del sistema operativo](#) (Event Log);
- [log di testo di debug](#).

#### Log del sistema operativo

Nel log di registrazione degli eventi del sistema operativo (Event Log) vengono registrate le seguenti informazioni:

- messaggi sull'avvio e arresto del programma;
- impostazioni dei moduli del software: dello scanner, del motore, dei database dei virus (le informazioni vengono registrate ad avvio del programma e ad aggiornamento dei moduli);
- messaggi sul rilevamento dei virus.

#### Per visualizzare il log di registrazione degli eventi del sistema operativo:

1. Aprire il **Pannello di controllo** del sistema operativo.
2. Selezionare la sezione **Amministrazione** → **Visualizza eventi**.
3. Nella parte destra della finestra **Visualizza eventi** selezionare la voce **Applicazione**. Si apre una lista degli eventi registrati nel log dalle applicazioni dell'utente. La fonte dei messaggi di Dr.Web per Outlook è l'applicazione Dr.Web per Outlook.

#### Log di testo di debug

Nel log di testo di debug vengono registrate le seguenti informazioni:

- messaggi sul rilevamento dei virus;
- messaggi sugli errori di scrittura o lettura dei file, errori di analisi degli archivi o dei file protetti da password;
- impostazioni dei moduli del software: dello scanner, del motore, dei database dei virus;
- messaggi sui crash del motore del software.



## Configurazione della registrazione degli eventi

1. Nella scheda **Antivirus Dr.Web** premere il pulsante **Log**. Si apre la finestra di configurazione del log.
2. Per registrare le informazioni massimamente dettagliate sugli eventi, spuntare il flag **Registra log dettagliato**. Di default gli eventi vengono registrati in modalità normale.



Se viene registrato un log di testo dettagliato, questo porta a un calo delle prestazioni del sistema perciò è consigliabile attivare la registrazione massimamente dettagliata degli eventi soltanto in caso di errori nel funzionamento dell'applicazione Dr.Web per Outlook.

3. Premere il pulsante **OK** per salvare le modifiche.



La finestra **Log** è disponibile solo se l'utente possiede i permessi dell'amministratore del sistema.

Nel sistema operativo Windows Vista e superiori, quando si fa clic sul pulsante **Log**:

- se l'UAC è attivato: all'amministratore viene visualizzata una richiesta per confermare le azioni del programma, a un utente senza i permessi di amministratore viene visualizzata una richiesta per inserire le credenziali dell'amministratore del sistema;
- se l'UAC è disattivato: l'amministratore può modificare le impostazioni del programma, un utente non può avere l'accesso alla modifica delle impostazioni.

## Visualizzazione del log degli eventi del programma

Per visualizzare il log di testo degli eventi del programma, premere il pulsante **Mostra nella cartella**. Si apre la cartella in cui è memorizzato il log.

### 11.6.4. Statistiche

Nell'applicazione di posta Microsoft Outlook sezione **Servizi** → **Impostazioni** → scheda **Antivirus Dr.Web** (in caso di Microsoft Outlook 2010 sezione **File** → **Impostazioni** → **Estensioni** selezionare **Dr.Web per Outlook** e premere il pulsante **Impostazioni dell'estensione**) sono contenute le informazioni statistiche circa il numero totale di oggetti controllati e processati dal programma.

Gli oggetti sono suddivisi nelle seguenti categorie:

- **Controllati** — il numero totale di messaggi controllati;
- **Infetti** — il numero di messaggi che contengono virus;
- **Sospetti** — il numero di messaggi presumibilmente infettati da un virus (rilevati tramite l'analisi euristica);
- **Curati** — il numero di oggetti guariti con successo dal programma;



- **Non controllati** — il numero di oggetti di cui la scansione non è possibile o durante la cui scansione si sono verificati degli errori;
- **Puliti** — il numero di messaggi che non contengono oggetti dannosi.

Quindi viene indicato il numero di oggetti a cui sono state applicate le azioni:

- **Spostati** — il numero di oggetti spostati in Quarantena;
- **Rimossi** — il numero di oggetti eliminati dal sistema;
- **Saltati** — il numero di oggetti saltati senza modifiche;
- **Messaggi spam** — il numero di messaggi riconosciuti come lo spam.

Di default le statistiche vengono salvate nel file drwebforoutlook.stat situato nella cartella %USERPROFILE%\Doctor Web.



Le informazioni statistiche vengono accumulate entro una sessione. Dopo il riavvio del computer o dopo il riavvio di Agent Dr.Web, le statistiche vengono azzerate.

## 11.7. Protezione preventiva

In questa sezione è possibile configurare la reazione di Dr.Web alle azioni delle applicazioni di terze parti, che possono portare all'infezione del computer, e selezionare il livello di protezione dagli exploit.

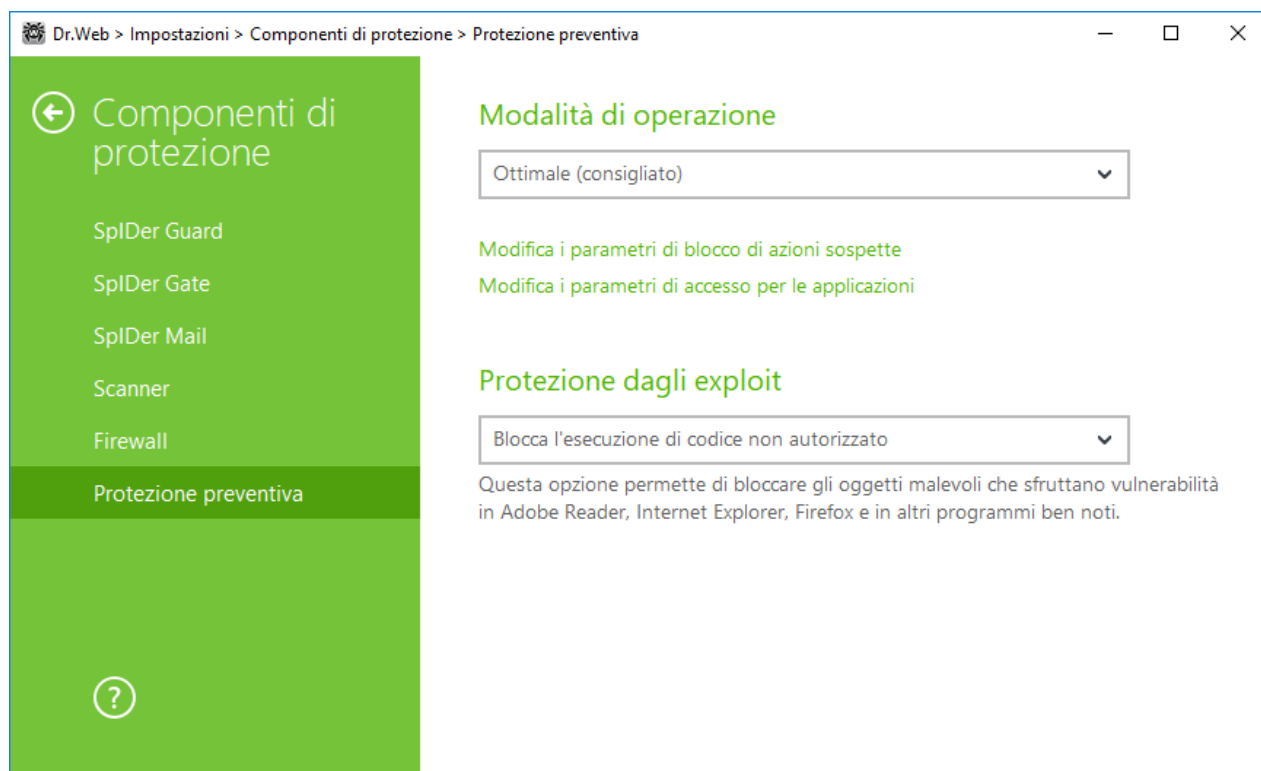



Immagine 33. Configurazione di Protezione preventiva



È possibile impostare una modalità di protezione separata per singole applicazioni e una modalità generale le cui impostazioni verranno impiegate per tutti gli altri processi.


Per impostare la modalità generale di protezione preventiva, selezionarla dalla lista **Modalità di operazione** o fare clic sull'opzione **Modifica i parametri di blocco di azioni sospette**. In quest'ultimo caso si apre una finestra in cui è possibile conoscere più nel dettaglio le impostazioni di ciascuna modalità o modificarle. Tutte le modifiche nelle impostazioni vengono salvate in modalità di operazione Personalizzata. In questa finestra è inoltre possibile creare un nuovo profilo per la memorizzazione delle impostazioni richieste.


### Creazione di un nuovo profilo


1. Premere il pulsante .
2. Nella finestra che si è aperta indicare il nome per il nuovo profilo.
3. Visualizzare le impostazioni di protezione di default e, se necessario, modificarle.

Per configurare le impostazioni di protezione preventiva per specifiche applicazioni, fare clic sull'opzione **Modifica i parametri di accesso per le applicazioni**. Nella finestra che si è aperta si può aggiungere una nuova regola per un'applicazione, modificare una regola già creata o eliminarne una non richiesta.

### Aggiunta della regola

1. Premere il pulsante .
2. Nella finestra che si è aperta premere il pulsante **Sfoglia** e indicare il percorso del file eseguibile dell'applicazione.
3. Visualizzare le impostazioni di protezione di default e, se necessario, modificarle.

Per modificare una regola già creata, selezionarla dalla lista e premere .

Per eliminare una regola già creata, selezionarla dalla lista e premere .

Maggiori informazioni circa le impostazioni di ciascuna delle modalità di operazione si possono avere di seguito nella sezione Livello di protezione preventiva.

## Livello di protezione preventiva

In modalità di operazione **Ottimale**, Dr.Web proibisce le modifiche automatiche degli oggetti di sistema la cui modifica indica chiaramente un tentativo di impatto malevolo sul sistema operativo. Inoltre, viene proibito l'accesso al disco a basso livello e la modifica del file HOSTS per le applicazioni le cui attività anche vengono definite chiaramente come un tentativo di impatto malevolo sul sistema operativo.



Vengono bloccate solo le azioni delle applicazioni che non sono affidabili.

Il livello di protezione **Media** può essere impostato nel caso di aumentato rischio di infezione. In questa modalità viene proibito additionally l'accesso a quegli oggetti critici che potenzialmente possono essere sfruttati da programmi malevoli.



In questa modalità di protezione sono possibili conflitti di compatibilità con programmi di terzi che utilizzano i rami di registro protetti.

Il livello di protezione **Paranoiciale** è necessario per un completo controllo degli accessi agli oggetti critici di Windows. In questo caso sarà inoltre disponibile un controllo interattivo del caricamento dei driver e dell'esecuzione automatica dei programmi.

In modalità di operazione **Personalizzato** si possono selezionare a propria discrezione i livelli di protezione per ciascun oggetto.

| Oggetto protetto                           | Descrizione  |
|--|--|
| Integrità delle applicazioni in esecuzione | Questa impostazione consente di monitorare i processi che si incorporano nelle applicazioni in esecuzione, il che costituisce una minaccia per la sicurezza del computer. Non viene monitorato il comportamento dei processi che sono stati aggiunti alle <a href="#">Eccezioni</a> .  |
| Integrità dei file degli utenti            | Questa impostazione consente di cercare processi che modificano file degli utenti secondo un algoritmo conosciuto che indica che tali processi sono una minaccia alla sicurezza del computer. Non viene monitorato il comportamento dei processi che sono stati aggiunti a <a href="#">Eccezioni</a> .                             |
| File HOSTS                                 | Il file HOSTS viene utilizzato dal sistema operativo per semplificare l'accesso a Internet. Le modifiche a questo file possono essere il risultato del funzionamento di un virus o di un altro programma malevolo.   |
| Accesso al disco a basso livello           | Questa impostazione consente di proibire alle applicazioni di registrare informazioni su disco settore per settore senza utilizzare il file system.  |
| Caricamento dei driver                     | Questa impostazione consente di proibire alle applicazioni di caricare driver nuovi o sconosciuti.   |
| Aree critiche di Windows                   | Le altre impostazioni consentono di proteggere i rami di registro contro le modifiche (sia nel profilo di sistema che nei profili di tutti gli utenti).<br><br>Accesso a Image File Execution Options: <ul style="list-style-type: none"><li>• Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options</li></ul> |



| Oggetto protetto | Descrizione  |
|------------------|--|
|                  | <p>Accesso a User Drivers:</p> <ul style="list-style-type: none"><li>• Software\Microsoft\Windows NT\CurrentVersion\Drivers32</li><li>• Software\Microsoft\Windows NT\CurrentVersion\Userinstallable.drivers</li></ul> <p>Parametri della shell Winlogon:</p> <ul style="list-style-type: none"><li>• Software\Microsoft\Windows NT\CurrentVersion\Winlogon, Userinit, Shell, UIHost, System, Taskman, GinaDLL</li></ul> <p>Notifiche di Winlogon:</p> <ul style="list-style-type: none"><li>• Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify</li></ul> <p>Avvio automatico della shell di Windows:</p> <ul style="list-style-type: none"><li>• Software\Microsoft\Windows NT\CurrentVersion\Windows, Applnit_DLLs, LoadApplnit_DLLs, Load, Run, IconServiceLib</li></ul> <p>Associazione dei file eseguibili:</p> <ul style="list-style-type: none"><li>• Software\Classes\.exe, .pif, .com, .bat, .cmd, .scr, .lnk (chiavi)</li><li>• Software\Classes\exefile, piffile, comfile, batfile, cmdfile, scrfile, lnkfile (chiavi)</li></ul> <p>Criteri restrizione software (SRP):</p> <ul style="list-style-type: none"><li>• Software\Policies\Microsoft\Windows\Safer</li></ul> <p>Plugin di Internet Explorer (BHO):</p> <ul style="list-style-type: none"><li>• Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects</li></ul> <p>Esecuzione automatica programmi:</p> <ul style="list-style-type: none"><li>• Software\Microsoft\Windows\CurrentVersion\Run</li><li>• Software\Microsoft\Windows\CurrentVersion\RunOnce</li><li>• Software\Microsoft\Windows\CurrentVersion\RunOnceEx</li><li>• Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup</li><li>• Software\Microsoft\Windows\CurrentVersion\RunOnceEx\Setup</li><li>• Software\Microsoft\Windows\CurrentVersion\RunServices</li><li>• Software\Microsoft\Windows\CurrentVersion\RunServicesOnce</li></ul> <p>Esecuzione automatica criteri:</p> <ul style="list-style-type: none"><li>• Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run</li></ul> <p>Configurazione della modalità provvisoria:</p> <ul style="list-style-type: none"><li>• SYSTEM\ControlSetXXX\Control\SafeBoot\Minimal</li></ul> |



| Oggetto protetto | Descrizione  |
|------------------|--|
|                  | <ul style="list-style-type: none"><li>• SYSTEM\ControlSetXXX\Control\SafeBoot\Network</li></ul> Impostazioni della Gestione sessioni: <ul style="list-style-type: none"><li>• System\ControlSetXXX\Control\Session Manager\SubSystems, Windows</li></ul> Servizi di sistema: <ul style="list-style-type: none"><li>• System\CurrentControlXXX\Services</li></ul> |



In caso di problemi con l'installazione degli aggiornamenti critici di Microsoft o con l'installazione e il funzionamento dei programmi (compresi programmi di deframmentazione), disattivare temporaneamente la protezione preventiva.

È possibile [configurare](#) la visualizzazione degli avvisi sulle attività della protezione preventiva sullo schermo.

## Protezione dagli exploit


Questa opzione permette di bloccare gli oggetti malevoli che sfruttano vulnerabilità presenti nelle applicazioni popolari. Dalla lista a cascata corrispondente selezionare il livello di protezione dagli exploit adatto.

| Livello di protezione                           | Descrizione  |
|---|--|
| Blocca l'esecuzione di codice non autorizzato   | Verrà bloccato automaticamente il tentativo da parte di un oggetto malevolo di sfruttare le vulnerabilità nei software per ottenere l'accesso alle aree critiche del sistema operativo.  |
| Modalità interattiva                            | Se un oggetto malevolo cercherà di sfruttare le vulnerabilità nei software per ottenere l'accesso alle aree critiche del sistema operativo, Dr.Web visualizzerà un avviso corrispondente. Leggere le informazioni dell'avviso e selezionare l'azione desiderata. |
| Consenti l'esecuzione di codice non autenticato | Verrà consentito automaticamente un tentativo da parte di un oggetto malevolo di sfruttare le vulnerabilità nei software per ottenere l'accesso alle aree critiche del sistema operativo.  |



## 12. Statistiche

In questa finestra sono raccolte statistiche su eventi importanti nel funzionamento dei componenti di protezione.

Per visualizzare informazioni sul funzionamento dei componenti, aprire il menu  in [modalità amministratore](#) e andare alla sezione **Statistiche** . Sulla pagina **Statistiche** sono disponibili i report per i seguenti gruppi:

- Minacce
- Aggiornamento
- Office control


Per le registrazioni dei gruppi **Minacce** e **Aggiornamento** è disponibile un report dettagliato. È possibile utilizzare filtri per le registrazioni del report.

Nel gruppo **Office control** vengono visualizzate le statistiche degli URL bloccati per ciascun account.

Nel report vengono registrate le seguenti informazioni:

- Frequenza delle visite;
- Azione;
- URL.

Per le registrazioni del report ci sono dei filtri predefiniti che sono disponibili in una lista a cascata in cima alla pagina.

Tramite il pulsante  è possibile eliminare, copiare, esportare eventi selezionati o il report per intero, nonché cancellare il report.

### Attività di rete

Se è installato Firewall Dr.Web, è disponibile un report sulle attività di rete.

È possibile visualizzare i dati per le applicazioni attive, un log delle applicazioni, un log del filtro pacchetti. A questo scopo, selezionare l'oggetto richiesto dalla lista a cascata.

Per ogni applicazione attiva nel report vengono visualizzati i seguenti dati:

- direzione della trasmissione dei dati;
- log di funzionamento;
- indirizzo locale;
- indirizzo remoto;
- dimensione di un pacchetto dati inviato;






- dimensione di un pacchetto dati ricevuto.

Nel log delle applicazioni si può vedere:


- ora di inizio del funzionamento di un'applicazione;
- nome dell'applicazione;
- nome della regola di processamento dell'applicazione;
- direzione della trasmissione dei dati;
- azione;
- indirizzo di destinazione.

Nel log del filtro pacchetti vengono visualizzati i seguenti dati:

- ora di inizio del processamento di un pacchetto dati;
- direzione della trasmissione del pacchetto dati;
- nome della regola di processamento;
- interfaccia;
- contenuto del pacchetto.

Tramite il pulsante  è possibile esportare record dei log o cancellare record nei log.

### Report dettagliato


Per visualizzare un report dettagliato sugli eventi di funzionamento Dr.Web, selezionare l'evento richiesto e premere il pulsante . Premendo nuovamente questo pulsante, vengono nascosti i dati dettagliati dell'evento.

Tramite il pulsante  è possibile eliminare, copiare, esportare singoli eventi o il report per intero, nonché cancellare il report.

Per selezionare eventi, è possibile utilizzare dei filtri.

### Filtri

Per visualizzare nella lista soltanto gli eventi che corrispondono a determinati parametri, utilizzare i filtri. Per tutti i report ci sono dei filtri predefiniti che sono disponibili in una lista a cascata in cima alla pagina di ciascun gruppo.

Si possono inoltre creare filtri di eventi personalizzati. Per creare un nuovo filtro, premere il pulsante  e selezionare la voce **Crea** dalla lista a cascata. Nella finestra che si è aperta indicare i criteri di filtraggio necessari. Notare che nel campo **Componente** è possibile impostare più componenti alla volta.



Gli eventi possono essere filtrati per codice. A tale scopo specificare i codici nel campo **Codice (ad esempio: 100-103, -102, 403)** in conformità con le seguenti regole:

- i codici vengono separati da virgole;
- è possibile indicare un intervallo di codici (per esempio 100-103);
- il carattere "-" che precede un codice lo esclude dall'intervallo.

Pertanto, una registrazione tipo "100-103, -102, 403" significa che devono essere visualizzati tutti gli eventi da "100" a "103", ma deve essere escluso dal filtro il codice "-102" e deve essere visualizzato l'evento "403".


I filtri creati dall'utente possono essere modificati o rimossi.



## 13. Messaggi del server

L'amministratore della rete ha la possibilità di configurare l'invio dei messaggi di server su qualsiasi delle postazioni. Questa funzione è utile quando l'amministratore della rete lavora su una delle postazioni per ricevere gli avvisi dal server.

Tutti i messaggi ricevuti vengono visualizzati in una lista nella parte superiore della finestra. Per visualizzare nella lista solo i messaggi che corrispondono a determinati parametri, utilizzare filtri. Ci sono filtri predefiniti disponibili in una lista a cascata.

Si possono inoltre creare filtri di messaggi personalizzati. Per creare un nuovo filtro, premere il pulsante  e selezionare la voce **Crea** dalla lista a cascata. Nella finestra che si è aperta indicare i criteri di filtraggio necessari.

I messaggi possono essere filtrati secondo le seguenti categorie:

- Postazioni;
- Repository;
- Licenze;
- Amministratori;
- Altro.

I filtri creati dall'utente possono essere modificati o rimossi.

Tramite il pulsante  è possibile eliminare, copiare, esportare i messaggi selezionati, nonché eliminare tutti i messaggi.



## 14. Supporto tecnico

Se si verificano dei problemi con l'installazione o il funzionamento dei prodotti della società, prima di chiedere aiuto al reparto di supporto tecnico, provare a trovare una soluzione nei seguenti modi:

- leggere le ultime versioni delle descrizioni e dei manuali sull'indirizzo <https://download.drweb.com/doc/>;
- leggere la sezione delle domande ricorrenti sull'indirizzo [https://support.drweb.com/show\\_faq/](https://support.drweb.com/show_faq/);
- 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:

- compilare il modulo web nella relativa sezione della pagina <https://support.drweb.com/>;
- chiamare il numero di telefono a Mosca: +7 (495) 789-45-86 o il numero verde per tutta la Russia: 8-800-333-7932.

Le informazioni sulle rappresentanze regionali e sedi della società Doctor Web sono ritrovabili sul sito ufficiale sull'indirizzo <https://company.drweb.com/contacts/offices/>.



## 15. Allegato A. Parametri aggiuntivi da riga di comando

I parametri da riga di comando si usano per configurare programmi che possono essere avviati tramite l'esecuzione di un file eseguibile. Questo vale per Scanner Dr.Web e Scanner console. Le opzioni possono impostare parametri non disponibili nel file di configurazione e hanno la precedenza sui parametri impostati nel file di configurazione.

Le opzioni iniziano con il carattere "/" e, come gli altri parametri da riga di comando, vengono separate da spazi.

### 15.1. Parametri per Scanner e Scanner console

| Opzione                          | Descrizione  |
|----------------------------------|--|
| /AA                              | Applica automaticamente le azioni alle minacce rilevate. (Solo per Scanner).   |
| /AC                              | Controlla i pacchetti di installazione. Di default l'opzione è attivata.   |
| /AFS                             | Utilizza la barra quando si indica la nidificazione all'interno dell'archivio. Di default l'opzione è disattivata.   |
| /AR                              | Controlla archivi. Di default l'opzione è attivata.  |
| /ARC: <rapporto_di_compressione> | Il livello massimo di compressione. Se Scanner determina che il rapporto di compressione dell'archivio eccede il limite indicato, la decompressione e la scansione non vengono eseguite. Di default è senza limitazioni.           |
| /ARL: <livello_di_nidificazione> | Il livello massimo di nidificazione dell'archivio controllato. Di default è senza limitazioni.   |
| /ARS: <dimensione>               | la dimensione massima in kilobyte dell'archivio controllato. Di default è senza limitazioni.   |
| /ART: <dimensione>               | Il valore soglia in kilobyte del controllo del livello di compressione (la dimensione minima di un file all'interno dell'archivio a partire da cui viene controllato il rapporto di compressione). Di default è senza limitazioni. |
| /ARX: <dimensione>               | La dimensione massima in kilobyte degli oggetti in archivi controllati. Di default è senza limitazioni.  |
| /BI                              | Visualizza informazioni sui database dei virus. Di default l'opzione è attivata.   |



| Opzione                     | Descrizione  |
|-----------------------------|--|
| /CUSTOM                     | Avvia Scanner sulla pagina di scansione personalizzata. Se vengono impostati parametri aggiuntivi (per esempio, oggetti da controllare o i parametri /TM, /TB), verrà avviata una scansione personalizzata degli oggetti indicati. (Vale solo per Scanner).  |
| /DCT                        | Non visualizzare il tempo di scansione stimato. (Vale solo per Scanner console).   |
| /DR                         | Controlla ricorsivamente le cartelle (controlla le sottocartelle). Di default l'opzione è attivata.  |
| /E: <numero_di_thread>      | Esegui la scansione con il numero di thread indicato.  |
| /FAST                       | Esegui una <b>scansione rapida</b> del sistema. Se vengono impostati parametri aggiuntivi (per esempio, oggetti da controllare o i parametri /TM, /TB), gli oggetti indicati anche verranno controllati. (Vale solo per Scanner).  |
| /FL: <nome_di_file>         | Controlla i percorsi indicati nel file.  |
| /FM: <maschera>             | Controlla i file in base a una maschera. Di default, tutti i file vengono controllati.   |
| /FR: <espressione_regolare> | Controlla i file in base a un'espressione regolare. Di default tutti i file vengono controllati.   |
| /FULL                       | Esegui una scansione completa di tutti i dischi rigidi e supporti rimovibili (compresi i settori di avvio). Se vengono impostati parametri aggiuntivi (per esempio, gli oggetti da controllare o i parametri /TM, /TB), verrà eseguita una scansione rapida e una scansione degli oggetti indicati. (Vale solo per Scanner).   |
| /FX: <maschera>             | Non controllare i file che corrispondono alla maschera. (Vale solo per Scanner console).   |
| /GO                         | Modalità di funzionamento di Scanner in cui vengono saltate le domande che sottintendono l'attesa di una risposta dell'utente, vengono prese in automatico le decisioni che richiedono una scelta. Questa modalità è utile per la verifica di file automatica, per esempio al controllo giornaliero o settimanale del disco rigido. Nella riga di comando deve essere indicato l'oggetto da sottoporre a scansione. Insieme al parametro /GO possono inoltre essere utilizzati i parametri /LITE, /FAST, /FULL. In questa modalità la scansione viene fermata se il computer passa all'alimentazione a batteria. |



| Opzione                    | Descrizione   |
|----------------------------|---|
| /H o /?                    | Visualizza una breve guida all'utilizzo del programma. (Vale solo per Scanner console).   |
| /HA                        | Esegui un'analisi euristica dei file e cerca nei file minacce sconosciute. Di default l'opzione è attivata.   |
| /KEY: <file_della_chiave>  | Indica il percorso del file della chiave. Il parametro è necessario se il file della chiave si trova in una cartella diversa da quella dello scanner. Di default, si usa drweb32.key o un altro file adatto dalla cartella C:\Program Files\DrWeb\. |
| /LITE                      | Esegui una scansione iniziale del sistema con cui vengono controllati la memoria operativa e i settori di avvio di tutti i dischi, inoltre esegui una verifica della presenza di rootkit. (Vale solo per Scanner).                                  |
| /LN                        | Controlla i file a cui indicano i collegamenti. Di default l'opzione è disattivata.   |
| /LS                        | Esegui una scansione sotto l'account LocalSystem. Di default l'opzione è disattivata.   |
| /MA                        | Controlla file di posta. Di default l'opzione è attivata.   |
| /MC: <numero_di_tentativi> | Imposta il numero massimo di tentativi di cura del file. Di default è senza limitazioni.  |
| /NB                        | Non creare copie di backup dei file curati/rimossi. Di default l'opzione è disattivata.   |
| /NI[:X]                    | il livello di utilizzo delle risorse di sistema. Definisce la quantità di memoria utilizzata per la scansione e la priorità di sistema della scansione. Di default è senza limitazioni.   |
| /NOREBOOT                  | Annula il riavvio e lo spegnimento dopo la scansione. (Vale solo per Scanner).  |
| /NT                        | Controlla stream NTFS. Di default l'opzione è attivata.   |
| /OK                        | Visualizza una lista completa degli oggetti controllati, contrassegnando quelli non infetti con OK. Di default l'opzione è disattivata  |
| /P: <priorità>             | La priorità del task di verifica avviato nella coda generale dei task di verifica:<br><br>0 — minima.<br>L — bassa.   |



| Opzione                          | Descrizione   |
|----------------------------------|---|
|                                  | N — normale. La priorità predefinita.<br>H — alta.<br>M — massima.  |
| /PAL: <livello_di_nidificazione> | Il livello massimo di nidificazione dei packer di un file eseguibile. Se il livello di nidificazione supera quello indicato, la scansione viene eseguita solo fino al livello di nidificazione indicato. Di default, è 1000.  |
| /QL                              | Visualizza la lista di tutti i file messi in quarantena su tutti i dischi. (Vale solo per Scanner console).   |
| /QL: <nome_del_disco_logico>     | Visualizza la lista di tutti i file messi in quarantena sul disco logico indicato. (Vale solo per Scanner console).   |
| /QNA                             | visualizza i percorsi tra virgolette doppie.  |
| /QR[: [d] [:p]]                  | Rimuovi i file dal disco <d> (nome_del_disco_logico) indicato, che si trovano in quarantena per più di <p> (quantità) giorni. Se <d> e <p> non sono impostati, verranno rimossi tutti i file in quarantena da tutti i dischi logici. (Vale solo per Scanner console). |
| /QUIT                            | Chiudi Scanner dopo la scansione (a prescindere da quello se le azioni sono state applicate alle minacce rilevate). (Vale solo per Scanner).  |
| /RA: <nome_di_file>              | Aggiungi il report sul funzionamento del programma al file indicato. Di default, nessuna registrazione viene effettuata nel file di log.  |
| /REP                             | Controlla in base a collegamenti simbolici. Di default l'opzione è disattivata.   |
| /RK                              | Verifica della presenza di rootkit. Di default l'opzione è disattivata.   |
| /RP: <nome_di_file>              | Scrivi il report sul funzionamento del programma nel file indicato. Di default, nessuna registrazione viene effettuata nel file di log.   |
| /RPC: <sec>                      | Il time-out in secondi della connessione con Scanning Engine. Di default è di 30 secondi. (Vale solo per Scanner console).  |
| /RPCD                            | Utilizza l'identificatore dinamico RPC. (Vale solo per Scanner console).  |





| Opzione                            | Descrizione   |
|------------------------------------|---|
| /RPCE                              | Utilizza l'indirizzo di destinazione dinamico RPC. (Vale solo per Scanner console).   |
| /RPCE: <indirizzo_di_destinazione> | Utilizza l'indirizzo di destinazione RPC indicato. (Vale solo per Scanner console).   |
| /RPCH: <nome_di_host>              | Utilizza il nome di host indicato per le chiamate RPC. (Vale solo per Scanner console).   |
| /RPCP: <protocollo>                | Utilizza il protocollo RPC indicato. È possibile utilizzare i protocolli: lpc, np, tcp. (Vale solo per Scanner console).  |
| /SCC                               | Visualizza il contenuto degli oggetti composti. Di default l'opzione è disattivata.   |
| /SCN                               | Visualizza il nome del pacchetto di installazione. Di default l'opzione è disattivata.  |
| /SLS                               | Visualizza i log sullo schermo. Di default l'opzione è attivata. (Vale solo per Scanner console).   |
| /SPN                               | Visualizza il nome del packer. Di default l'opzione è disattivata.  |
| /SPS                               | Visualizza l'avanzamento della scansione. Di default l'opzione è attivata. (Vale solo per Scanner console).   |
| /SST                               | Visualizza il tempo di verifica dell'oggetto. Di default l'opzione è disattivata.   |
| /ST                                | Avvia Scanner in background. Se il parametro /GO non è impostato, la modalità grafica viene visualizzata solo quando vengono rilevate minacce. In questa modalità la scansione viene fermata se il computer passa all'alimentazione a batteria. |
| /TB                                | Controlla i settori di avvio e i settori di avvio principali (MBR) del disco rigido.  |
| /TM                                | Cerca minacce nella memoria operativa (compresa l'area di sistema di Windows).  |
| /TR                                | Controlla i punti di ripristino di sistema.   |
| /W: <sec>                          | Il tempo massimo di scansione in secondi. Di default è senza limitazioni.   |
| /WCL                               | Output compatibile con drwebwcl. (Vale solo per Scanner console).   |



| Opzione  | Descrizione  |
|----------|--|
| /X:S[:R] | A termine della scansione fai passare la macchina in modalit  indicata: spegnimento/riavvio/sospensione/ibernazione. |

Per impostare le azioni su vari oggetti (C — cura, Q — sposta in quarantena, D — elimina, I — ignora, R — informa. L'azione R   possibile solo per Scanner console. Di default, per tutti   impostata l'azione informa (anche vale solo per Scanner console)):

| Azione        | Descrizione   |
|---------------|---|
| /AAD:<azione> | le azioni su adware (le azioni possibili: DQIR)                             |
| /AAR:<azione> | le azioni su archivi infetti (le azioni possibili: DQIR)                    |
| /ACN:<azione> | le azioni su pacchetti di installazione infetti (le azioni possibili: DQIR) |
| /ADL:<azione> | le azioni su dialer (le azioni possibili: DQIR)                             |
| /AHT:<azione> | le azioni su hacktool (le azioni possibili: DQIR)                           |
| /AIC:<azione> | le azioni su file incurabili (le azioni possibili: DQR)                     |
| /AIN:<azione> | le azioni su file infetti (le azioni possibili: CDQR)                       |
| /AJK:<azione> | le azioni su joke (le azioni possibili: DQIR)                               |
| /AML:<azione> | le azioni su file di posta infetti (le azioni possibili: QIR)               |
| /ARW:<azione> | le azioni su file potenzialmente pericolosi (le azioni possibili: DQIR)     |
| /ASU:<azione> | le azioni su file sospetti (le azioni possibili: DQIR)                      |

Alcune opzioni possono avere modificatori attraverso cui una modalit  viene esplicitamente attivata o disattivata. Per esempio:

|           |  |
|-----------|--|
| /AC-      | la modalit  viene esplicitamente disattivata |
| /AC, /AC+ | la modalit  viene esplicitamente attivata    |

Tale possibilit  pu  essere utile se la modalit    attivata/disattivata di default o secondo le impostazioni precedentemente definite nel file di configurazione. La lista delle opzioni che permettono l'uso dei modificatori:

/AC, /AFS, /AR, /BI, /DR, /HA, /LN, /LS, /MA, /NB, /NT, /OK, /QNA, /REP, /SCC, /SCN, /SLS, /SPN, /SPS, /SST, /TB, /TM, /TR, /WCL.



Per l'opzione `/FL` il modificatore "-" significa: controlla i percorsi elencati nel file indicato ed elimina il file.

Per le opzioni `/ARC`, `/ARL`, `/ARS`, `/ART`, `/ARX`, `/NI[:X]`, `/PAL`, `/RPC`, `/W` il valore di parametro "0" significa che il parametro si usa senza limitazioni.

Un esempio di utilizzo delle opzioni per l'avvio di Scanner console:

```
[<percorso_del_programma>]dwscancl /AR- /AIN:C /AIC:Q C:\
```

controlla tutti i file ad eccezione degli archivi sul disco C, cura i file infetti, metti in quarantena i file incurabili. Per avviare a un modo analogo Scanner per Windows, è necessario invece di `dwscancl` digitare il nome del comando `dwscanner`.

## 15.2. Parametri per i pacchetti di installazione

`/compression <modalità>` — la modalità di compressione dei dati che vengono scambiati con il server di protezione centralizzata. Il parametro `<modalità>` può assumere i seguenti valori:

- `yes` — utilizza la compressione.
- `no` — non utilizzare la compressione.
- `possible` — la compressione è possibile. La decisione finale viene presa a seconda delle impostazioni sul lato server.

Se l'opzione non è impostata, di default si usa il valore `possible`.

`/encryption <modalità>` — la modalità di cifratura dei dati che vengono scambiati con il server di protezione centralizzata. Il parametro `<modalità>` può assumere i seguenti valori:

- `yes` — utilizza la cifratura.
- `no` — non utilizzare la cifratura.
- `possible` — la cifratura è possibile. La decisione finale viene presa a seconda delle impostazioni sul lato server.

Se l'opzione non è impostata, di default si usa il valore `possible`.

`/excludeFeatures <componenti>` — una lista dei componenti che verranno esclusi al momento dell'installazione. Se vengono impostati diversi componenti, utilizzare come separatore il carattere ";". I componenti disponibili:

- `scanner` — Scanner Dr.Web,
- `spider-mail` — SpIDer Mail,
- `spider-g3` — SpIDer Guard,
- `outlook-plugin` — Dr.Web per Microsoft Outlook,
- `firewall` — Firewall Dr.Web,
- `spider-gate` — SpIDer Gate,



- `parental-control` — Office control,
- `antispam-outlook` — Antispam Dr.Web per il componente Dr.Web per Microsoft Outlook,
- `antispam-spidermail` — Antispam Dr.Web per il componente SplDer Mail.

Per i componenti non direttamente indicati viene mantenuto lo status di installazione impostato per essi di default.

`/id <identificatore_della_postazione>` — l'identificatore della postazione su cui viene installato Agent Dr.Web.

Viene impostato insieme alla password (l'opzione `/pwd`) per l'autenticazione manuale sul server. Se i parametri di autenticazione non sono impostati, la decisione circa l'autenticazione viene presa sul lato server.

`/includeFeatures <componenti>` — una lista dei componenti da installare. Se vengono impostati diversi componenti, utilizzare come separatore il carattere `,`. I componenti disponibili:

- `scanner` — Scanner Dr.Web,
- `spider-mail` — SplDer Mail,
- `spider-g3` — SplDer Guard,
- `outlook-plugin` — Dr.Web per Microsoft Outlook,
- `firewall` — Firewall Dr.Web,
- `spider-gate` — SplDer Gate,
- `parental-control` — Office control,
- `antispam-outlook` — Antispam Dr.Web per il componente Dr.Web per Microsoft Outlook,
- `antispam-spidermail` — Antispam Dr.Web per il componente SplDer Mail.

Per i componenti non direttamente indicati viene mantenuto lo status di installazione impostato per essi di default.

`/installdir <cartella>` — la cartella di installazione.

Se l'opzione non è impostata, di default l'installazione viene eseguita nella directory Program Files\DrWeb sul disco di sistema.

`/instMode <modalità>` — la modalità di avvio dell'installer. Il parametro `<modalità>` può assumere i seguenti valori:

- `remove` — rimuovi il prodotto installato.

Se l'opzione non è impostata, di default l'installer definisce automaticamente la modalità di avvio.

`/lang <codice_di_lingua>` — la lingua dell'installer e del prodotto che viene installato. Viene impostata nel formato ISO-639-1 per il codice di lingua.

Se l'opzione non è impostata, di default si usa la lingua di sistema.



`/pubkey <percorso>` — il percorso completo del file del certificato o della chiave pubblica del server.

Se il certificato o la chiave pubblica non sono impostati, di default all'avvio dell'installazione locale l'installer accetta automaticamente il certificato (con l'estensione .pem) o la chiave pubblica (drwcsd.pub) dalla cartella del suo avvio. Se il certificato o la chiave pubblica si trovano in una cartella diversa dalla cartella dell'installer, è necessario specificare manualmente il percorso completo del certificato o della chiave pubblica.

Se viene avviato un pacchetto di installazione creato nel Pannello di controllo, il certificato o la chiave pubblica fanno parte del pacchetto di installazione e non è richiesta alcuna indicazione aggiuntiva.

`/pwd <password>` — la password di Agent Dr.Web per l'accesso al server.

Viene impostata insieme all'identificatore di postazione (l'opzione `/id`) per l'autenticazione manuale sul server. Se i parametri di autenticazione non sono impostati, la decisione circa l'autenticazione viene presa sul lato server.

`/regagent <modalità>` — determina se Agent Dr.Web verrà registrato nella lista delle applicazioni installate. Il parametro `<modalità>` può assumere i seguenti valori:

- `yes` — registra Agent Dr.Web nella lista delle applicazioni installate.
- `no` — non registrare Agent Dr.Web nella lista delle applicazioni installate.

Se l'opzione non è impostata, di default si usa il valore `no`.

`/retry <numero>` — il numero di tentativi di ricerca del server tramite l'invio delle richieste multicast. Se non c'è una risposta dal server dopo il numero di tentativi impostato, si ritiene che il server non è stato trovato.

Se l'opzione non è impostata, di default vengono eseguiti 3 tentativi di ricerca del server.

`/server [<protocollo>]/<indirizzo_del_server>[:<porta>]` — l'indirizzo del server da cui verrà effettuata l'installazione di Agent Dr.Web e a cui Agent Dr.Web si conatterà dopo l'installazione.

Se l'opzione non è impostata, di default il server viene cercato tramite l'invio delle richieste multicast.

`/silent <modalità>` — determina se l'installer verrà eseguito in modalità silenziosa. Il parametro `<modalità>` può assumere i seguenti valori:

- `yes` — avvia l'installer in modalità silenziosa.
- `no` — avvia l'installer in modalità grafica.

Se l'opzione non è impostata, di default l'installazione di Agent Dr.Web viene eseguita in modalità grafica.



`/timeout <tempo>` — il limite di tempo per aspettare ciascuna risposta nel corso della ricerca del server. Viene impostato in secondi. I messaggi di risposta continuano ad essere accettati fino a quando il tempo di attesa della risposta non supererà il valore del time-out.

Se l'opzione non è impostata, di default si usa il valore di 3 secondi.

## 15.3. Codici di ritorno

I valori possibili del codice di ritorno e gli eventi corrispondenti sono i seguenti:

| Codice di ritorno | Evento  |
|-------------------|---|
| 0                 | Non sono stati rilevati virus o casi sospetti di virus.   |
| 1                 | Sono stati rilevati virus conosciuti.   |
| 2                 | Sono state rilevate varianti di virus sconosciuti.  |
| 4                 | Sono stati rilevati oggetti sospetti di virus.  |
| 8                 | Virus conosciuti sono stati rilevati in un archivio, un container o una casella di posta.               |
| 16                | Varianti di virus conosciuti sono state rilevate in un archivio, un container o una casella di posta.   |
| 32                | Oggetti sospetti di virus sono stati rilevati in un archivio, un container o una casella di posta.      |
| 64                | È stata completata con successo la cura di almeno un oggetto infettato da un virus.                     |
| 128               | È stata completata con successo la rimozione/la rinominazione/lo spostamento di almeno un file infetto. |

Il codice di ritorno risultante generato al completamento della scansione è uguale alla somma dei codici degli eventi che si sono verificati durante la scansione (e gli addendi possono essere ripristinati da esso in modo univoco).

Per esempio, il codice di ritorno  $9 = 1 + 8$  indica che uno o più virus conosciuti sono stati rilevati durante la scansione, tra l'altro anche in un archivio; la neutralizzazione non veniva eseguita; non c'erano altri eventi di virus.



## 16. Allegato B. Minacce informatiche e metodi per neutralizzarle

Con l'evoluzione delle tecnologie informatiche e delle soluzioni di rete, diventano sempre più diffusi vari programmi malevoli volti a recare danno agli utenti in un modo o nell'altro. La loro evoluzione iniziò nella lontana epoca della nascita del computer, e durante tutto il periodo si evolvevano anche gli strumenti di protezione da tali programmi. Tuttavia, non esiste ancora un'unica classificazione di tutte le possibili minacce, il che è dovuto, in primo luogo, alla natura imprevedibile della loro evoluzione e al continuo miglioramento delle tecnologie utilizzate.

I programmi malevoli possono diffondersi tramite Internet, la rete locale, l'email e supporti di memorizzazione rimovibili. Alcuni di essi fanno affidamento sull'incuria e sull'inesperienza dell'utente e possono funzionare in modo del tutto autonomo, altri sono solo strumenti nelle mani di hacker e sono in grado di recare danno anche a sistemi protetti in modo sicuro.

Questo capitolo fornisce le descrizioni di tutti i principali tipi di programmi malevoli più diffusi che le tecnologie Doctor Web sono volti a combattere in primo luogo.

### 16.1. Classificazione delle minacce

In questa classificazione il termine "minaccia informatica" significa qualsiasi strumento software che sia indirettamente o direttamente capace di causare un danno al computer, alla rete, alle informazioni o ai diritti dell'utente (cioè programmi malevoli e altri programmi indesiderati). In senso più ampio, il termine "minaccia informatica" può significare qualsiasi potenziale pericolo per il computer o la rete (cioè una vulnerabilità che può essere sfruttata per condurre attacchi hacker).

Tutti i tipi di programmi descritti sotto sono potenzialmente capaci di mettere a rischio i dati dell'utente o la loro riservatezza. Di solito, non vengono categorizzati come minacce i programmi che non nascondono la loro presenza nel sistema (per esempio, alcuni programmi per l'invio dello spam o per l'analisi del traffico dati), sebbene in determinate circostanze tali programmi possano causare un danno all'utente.

Nei prodotti e nella documentazione della società Doctor Web le minacce informatiche sono divise in due tipi in base al livello di pericolo:

- **minacce significative** — minacce informatiche classiche che di per sé sono capaci di eseguire varie attività distruttive ed illegali nel sistema (cancellazione e furto di informazioni importanti, violazione dell'operatività di una rete ecc.). Questo tipo di minacce informatiche include programmi che tradizionalmente vengono chiamati malevoli (virus, worm e trojan);
- **minacce insignificanti** — minacce informatiche che sono ritenute meno pericolose rispetto alle minacce significative, ma che possono essere utilizzate da terzi per eseguire azioni dannose. Inoltre, la presenza stessa delle minacce insignificanti nel sistema è una chiara indicazione di un basso livello della sua protezione. Gli esperti di sicurezza informatica chiamano talvolta questo tipo di minacce informatiche programmi "grigi" o potenzialmente indesiderati. Alle minacce insignificanti appartengono gli adware, i dialer, gli joke, i riskware e gli hacktool.



## Minacce significative

### Virus informatici

Questo tipo di minacce informatiche può incorporare il suo codice eseguibile in altri programmi. Tale incorporazione si chiama *infezione*. Nella maggior parte dei casi il file infetto diventa lui stesso portatore del virus, mentre il codice incorporato non necessariamente del tutto corrisponde all'originale. La maggior parte dei virus viene creata per danneggiare o distruggere dati.

Nell'azienda Doctor Web i virus sono divisi per il tipo di file che loro infettano:

- **i virus di file** infettano i file del sistema operativo (di solito, file eseguibili e librerie dinamiche) e diventano attivati ad accesso a un file infetto;
- **i virus di macro** infettano i file di documenti utilizzati dalle applicazioni Microsoft® Office o da altri programmi che consentono comandi macro, scritti, il più delle volte, nel linguaggio Visual Basic. Le macro sono programmi incorporati scritti in un linguaggio di programmazione a pieno titolo che possono avviarsi in determinate condizioni (per esempio, in Microsoft® Word le macro possono avviarsi all'avvio, alla chiusura o al salvataggio di un documento);
- **i virus di script** sono scritti nei linguaggi di script, e nella maggior parte dei casi infettano altri file di script (per esempio, i file di servizio del sistema operativo). Loro possono infettare anche gli altri tipi di file che supportano l'esecuzione degli script, sfruttando script vulnerabili in applicazioni web;
- **i virus di boot** infettano i settori di avvio di dischi e partizioni, nonché i master boot record di dischi rigidi. Occupano poca memoria e rimangono pronti a svolgere le loro funzioni fino a quando il sistema operativo non verrà scaricato da memoria, riavviato o arrestato.

La maggior parte dei virus possiede alcuni meccanismi di difesa dal rilevamento. I metodi di difesa dal rilevamento vengono migliorati di continuo, perciò per i programmi antivirus vengono sviluppati nuovi metodi per superare questa difesa. I virus possono essere divisi secondo il principio di difesa dal rilevamento:

- **i virus cifrati** criptano il proprio codice a ogni infezione nuova, il che ostacola il rilevamento di tale codice in un file, nella memoria o in un settore di avvio. Ogni copia di tale virus contiene soltanto un frammento comune (la procedura di decifratura) il quale può essere selezionato come firma antivirale;
- **i virus polimorfi** utilizzano, oltre alla cifratura del codice, una procedura di decifratura specifica che cambia sé stessa in ciascuna copia nuova del virus, quindi per tale virus non esistono firme antivirali di byte.

Inoltre, i virus possono essere classificati secondo il linguaggio in cui sono scritti (la maggior parte è scritta in assembler, nei linguaggi di programmazione di altro livello, linguaggi di script ecc.), nonché secondo il sistema operativo bersaglio.





## Worm

Recentemente i programmi malevoli del tipo "worm" sono diventati molto più diffusi dei virus e degli altri programmi malevoli. Così come i virus, i worm possono creare copie di sé stessi. Un worm si infila su un computer dalla rete (il più delle volte come un allegato a un'email) e invia le proprie copie funzionanti su altri computer. Per iniziare a diffondersi, i worm possono utilizzare sia le attività dell'utente che una modalità automatica di selezione e di attacco a un computer.

I worm non necessariamente sono costituiti per intero da un singolo file (il corpo del worm). Molti worm hanno la cosiddetta parte di infezione (un codice shell) che viene caricata nella memoria operativa del computer e ulteriormente scarica dalla rete il corpo stesso del worm come un file eseguibile. Fino a quando il corpo del worm non c'è nel sistema, è possibile liberarsene riavviando il computer (a riavvio la memoria operativa viene azzerata). Ma se il corpo del worm è già presente nel sistema, soltanto un antivirus può affrontarlo.

Propagandosi intensamente, i worm possono mettere fuori servizio intere reti anche quando non hanno alcun payload (cioè non causano un danno diretto al sistema).

In Doctor Web i worm sono divisi in base al modo (ambiente) di propagazione:

- **i worm di rete** si diffondono tramite vari protocolli di rete e protocolli di condivisione di file;
- **i worm di posta** si diffondono tramite protocolli di email (POP3, SMTP ecc.).

## Trojan

Questo tipo di programmi malevoli non è in grado di auto-replicarsi. I trojan eseguono qualche attività dannosa (danneggiano e cancellano dati, inviano dal computer informazioni riservate ecc.) o rendono possibile un utilizzo non autorizzato del computer da parte di un malintenzionato, per esempio, per causare danni a terzi.

Questi programmi hanno funzioni malevole e mimetiche simili a quelle dei virus e persino possono essere un modulo dei virus, ma di regola i trojan vengono distribuiti come i file eseguibili separati (vengono collocati su file server, registrati su supporti di informazione o inviati in email come allegati) che vengono eseguiti dall'utente stesso o da un determinato processo del sistema.

Di seguito è riportato un elenco di alcuni tipi di trojan che Doctor Web mette in classi separate:

- **i backdoor** — programmi trojan che consentono di ottenere l'accesso privilegiato al sistema aggirando il meccanismo esistente di concessione dell'accesso e di protezione. I backdoor non infettano file, si trascrivono nel registro, modificando chiavi;
- **i dropper** — file-portatori che contengono nel loro corpo programmi malevoli. Quando viene avviato, il dropper copia file malevoli sul disco dell'utente, senza avvisare l'utente, e li esegue;
- **i keylogger** vengono usati per raccogliere i dati che l'utente immette tramite la tastiera. Lo scopo di tali azioni è il furto di informazioni personali (per esempio, password di rete, login, numeri di carte di credito ecc.);



- **i clicker** ridefiniscono link quando si fa clic su di essi e in questo modo reindirizzano l'utente su determinati siti web (probabilmente malevoli). Di solito il reindirizzamento viene effettuato per aumentare il traffico pubblicitario di siti web o per organizzare attacchi distributed denial of service (attacchi DDoS);
- **i trojan proxy** forniscono al malintenzionato l'accesso anonimo alla rete Internet attraverso il computer della vittima;
- **i rootkit** sono studiati per intercettare le funzioni del sistema operativo per nascondere la propria presenza nel sistema. Inoltre, i rootkit possono nascondere processi di altri programmi, diverse chiavi del registro, cartelle e file. Un rootkit si diffonde come un programma indipendente o come un componente aggiuntivo di un altro programma malevolo. In base al principio di funzionamento i rootkit possono convenzionalmente essere divisi in due gruppi: quelli che funzionano in modalità utente (intercettano le funzioni delle librerie di modalità utente) (User Mode Rootkits (UMR)) e quelli che funzionano in modalità kernel (intercettano le funzioni a livello del kernel di sistema, il che ne rende notevolmente più difficile il rilevamento e la neutralizzazione) (Kernel Mode Rootkits (KMR)).

Oltre a quelle elencate, i trojan possono eseguire anche altre funzioni malevole, per esempio cambiare la pagina iniziale nel browser o rimuovere determinati file. Tali azioni però possono essere eseguite anche da altri tipi di minacce (per esempio, dai virus e worm).

## Minacce insignificanti

### Hacktool

Gli hacktool vengono creati per lo scopo di aiutare un intruso. Il tipo più comune di tali programmi sono gli scanner delle porte che consentono di scoprire vulnerabilità nei firewall e in altri componenti di protezione del computer. Oltre agli hacker, anche gli amministratori possono utilizzare questi strumenti per controllare la sicurezza delle loro reti. Talvolta vengono classificati come hacktool i programmi che utilizzano metodi di social engineering (ingegneria sociale).

### Adware

Il più delle volte questo termine significa un codice software incorporato in vari programmi gratuiti, utilizzando i quali l'utente è costretto a visualizzare pubblicità. Tuttavia, tale codice può talvolta essere distribuito di nascosto attraverso altri programmi malevoli e può visualizzare pubblicità, per esempio nei browser. Spesso gli adware funzionano sulla base dei dati raccolti dai programmi spyware.

### Joke

Questo tipo di programmi malevoli, così come gli adware, non causa alcun danno diretto al sistema. Il più delle volte, gli joke generano avvisi di errori inesistenti e minacciano di azioni che possono portare alla corruzione dei dati. La loro funzione principale è quella di intimidire o infastidire l'utente.



## Dialer

Questi sono programmi specifici che utilizzano l'accesso alla rete Internet con il permesso dell'utente per andare su determinati siti. Di solito hanno un certificato firmato e notificano di tutte le loro azioni.

## Riskware

Questi programmi non sono stati creati per provocare danni, ma in virtù delle loro caratteristiche possono rappresentare una minaccia alla sicurezza del sistema. A tali software appartengono non soltanto quelli che possono accidentalmente danneggiare o cancellare dati, ma anche quelli che possono essere utilizzati dagli hacker o da altri programmi per provocare danni al sistema. Possono essere classificati come riskware diversi programmi di comunicazione e amministrazione remota, server FTP ecc.

## Oggetti sospetti

Agli oggetti sospetti appartiene qualsiasi minaccia potenziale rilevata tramite l'analisi euristica. Tali oggetti possono essere qualsiasi tipo di minacce informatiche (probabilmente persino uno non ancora conosciuto dagli specialisti nella sicurezza informatica) e possono essere un oggetto sicuro in caso di falso positivo. È consigliabile mettere in quarantena i file che contengono oggetti sospetti, nonché spedirli per l'analisi agli specialisti del laboratorio antivirus Doctor Web.



## 16.2. Azioni per neutralizzare le minacce

Esistono molti metodi diversi per combattere le minacce informatiche. Per fornire una protezione affidabile dei computer e delle reti, i prodotti Doctor Web combinano questi metodi tramite le impostazioni flessibili e un approccio integrato alla sicurezza. Le principali azioni per neutralizzare i programmi malevoli sono:

1. **Cura** — azione applicabile ai virus, worm e trojan. Implica la rimozione del codice malevolo dai file infetti o la rimozione delle copie funzionali dei programmi malevoli, e inoltre, se possibile, il ripristino dell'operatività degli oggetti colpiti (cioè il ripristino della struttura e delle funzionalità di un programma allo stato precedente all'infezione). Non tutti i programmi malevoli possono essere curati, ma proprio i prodotti Doctor Web forniscono gli algoritmi più efficaci di cura e ripristino di file infettati.
2. **Spostamento in quarantena** — azione con cui un oggetto malevolo viene messo in una cartella specifica in cui esso è isolato dal resto del sistema. Questa azione va preferita quando la cura non è possibile, così come per tutti gli oggetti sospetti. È preferibile inviare le copie di simili file per l'analisi al laboratorio antivirus Doctor Web.
3. **Rimozione** — un'azione efficace per combattere le minacce informatiche. È applicabile a qualsiasi tipo di oggetti malevoli. Va notato che talvolta la rimozione verrà applicata ad alcuni file per cui è selezionata l'azione cura. Ciò accade quando l'intero file è costituito da codice malevolo e non contiene alcuna informazione utile. Così, per esempio, sotto la cura di un worm è sottintesa la rimozione di tutte le sue copie funzionali.
4. **Blocco, rinominazione** — anche queste sono azioni che consentono di neutralizzare i programmi malevoli, con cui, tuttavia, le loro copie complete rimangono nel file system. Nel primo caso, vengono bloccati tutti i tentativi di accesso effettuati dall'oggetto malevolo e i tentativi di accesso all'oggetto malevolo. Nel secondo caso, viene modificata l'estensione del file, il che lo rende non operativo.



## 17. Allegato C. Principi di denominazione delle minacce

Se viene rilevato un codice di virus, i componenti Dr.Web ne informano l'utente tramite gli strumenti dell'interfaccia e scrivono nel file di log il nome del virus assegnato ad esso dagli specialisti Doctor Web. Questi nomi si basano su determinati principi e rispecchiano la struttura del virus, le classi di oggetti vulnerabili, l'ambiente di diffusione (sistema operativo e pacchetti applicativi) e una serie di altre caratteristiche. Conoscere questi principi può essere utile per identificare le vulnerabilità di software e organizzative del sistema protetto. Di seguito è riportato un riepilogo dei principi di denominazione dei virus; una versione più completa e costantemente aggiornata della descrizione è disponibile sull'indirizzo <https://vms.drweb.com/classification/>.

Questa classificazione in alcuni casi è condizionale in quanto tipi specifici di virus possono avere più caratteristiche allo stesso tempo da quelle riportate. Inoltre, essa non può essere considerata esauriente in quanto appaiono costantemente nuovi tipi di virus e, di conseguenza, viene precisata la classificazione.

Il nome completo di un virus è costituito da diversi elementi separati da punti. Alcuni elementi all'inizio del nome completo (prefissi) e alla fine (suffissi) sono tipici secondo la classificazione adottata.

### Principali prefissi

#### Prefissi del sistema operativo

I seguenti prefissi vengono utilizzati per denominare i virus che infettano i file eseguibili di determinate piattaforme (sistemi operativi):

- `Win` — programmi a 16 bit per Windows 3.1;
- `Win95` — programmi a 32 bit per Windows 95, Windows 98, Windows Me;
- `WinNT` — programmi a 32 bit per Windows NT, Windows 2000, Windows XP, Windows Vista;
- `Win32` — programmi a 32 bit per diversi ambienti di Windows 95, Windows 98, Windows Me e Windows NT, Windows 2000, Windows XP, Windows Vista;
- `Win32.NET` — programmi nel sistema operativo Microsoft .NET Framework;
- `OS2` — programmi per OS/2;
- `Unix` — programmi per diversi sistemi operativi UNIX;
- `Linux` — programmi per il sistema operativo Linux;
- `FreeBSD` — programmi per il sistema operativo FreeBSD;
- `SunOS` — programmi per il sistema operativo SunOS (Solaris);
- `Symbian` — programmi per il sistema operativo Symbian OS (un sistema operativo mobile).

Va notato che alcuni virus possono infettare programmi di un sistema, sebbene essi stessi operino in un altro.



## Virus che infettano i file di MS Office

Gruppo di prefissi dei virus che infettano gli oggetti di MS Office (è indicato il linguaggio delle macro che vengono infettate da questo tipo di virus):

- WM — Word Basic (MS Word 6.0-7.0);
- XM — VBA3 (MS Excel 5.0-7.0);
- W97M — VBA5 (MS Word 8.0), VBA6 (MS Word 9.0);
- X97M — VBA5 (MS Excel 8.0), VBA6 (MS Excel 9.0);
- A97M — database MS Access'97/2000;
- PP97M — file di presentazione MS PowerPoint;
- O97M — VBA5 (MS Office'97), VBA6 (MS Office'2000), il virus infetta i file di più di un componente di MS Office.

## Prefissi del linguaggio di sviluppo software

Il gruppo di prefissi HLL è usato per denominare virus scritti in linguaggi di programmazione di alto livello, come per esempio C, C++, Pascal, Basic ecc. Sono usati modificatori che indicano l'algoritmo di funzionamento di base, in particolare:

- HLLW — worm;
- HLLM — worm di email;
- HLL0 — virus che sovrascrivono il codice del programma vittima;
- HLLP — virus parassiti;
- HLLC — virus satelliti.

Inoltre, il gruppo di prefissi del linguaggio di sviluppo software può includere:

- Java — virus per l'ambiente della macchina virtuale Java.

## Trojan

Trojan — nome generico di vari programmi trojan. In molti casi i prefissi di questo gruppo sono usati insieme al prefisso Trojan.

- PWS — trojan che ruba password;
- Backdoor — trojan con la funzionalità RAT (Remote Administration Tool — utility di amministrazione in remoto);
- IRC — trojan che utilizza per il suo funzionamento l'ambiente Internet Relay Chat channels;
- Downloader — trojan che scarica da Internet vari file malevoli all'insaputa dell'utente;
- MulDrop — trojan che carica di nascosto vari virus che sono contenuti direttamente nel suo corpo;



- **Proxy** — trojan che consente a un malintenzionato di navigare su Internet in modo anonimo attraverso il computer infetto;
- **StartPage** (sinonimo: **Seeker**) — trojan che sostituisce in modo non autorizzato l'indirizzo della pagina impostata nel browser come la homepage (pagina iniziale);
- **Click** — trojan che organizza il reindirizzamento delle richieste fatte dall'utente al browser su uno specifico sito (o siti);
- **KeyLogger** — trojan spione; segue e registra le battiture sulla tastiera; può inviare periodicamente i dati raccolti a un malintenzionato;
- **AVKill** — arresta il funzionamento dei programmi di protezione antivirus, firewall ecc.; e inoltre, può rimuovere dal disco questi programmi;
- **KillFiles**, **KillDisk**, **DiskEraser** — rimuovono uno specifico insieme di file (file in determinate directory, file in base a una maschera, tutti i file su un disco ecc.);
- **DelWin** — rimuove i file necessari per il funzionamento del sistema operativo (Windows);
- **FormatC** — formatta il disco C: (sinonimo: **FormatAll** — formatta alcuni o tutti i dischi);
- **KillMBR** — danneggia o cancella il contenuto del settore di avvio principale (MBR);
- **KillCMOS** — danneggia o cancella il contenuto del CMOS.

### Strumento per l'utilizzo delle vulnerabilità

- **Exploit** — strumento che utilizza le vulnerabilità conosciute di un sistema operativo o di un'applicazione al fine di introdurre nel sistema un codice malevolo, un virus od eseguire azioni non autorizzate.

### Strumenti per gli attacchi di rete

- **Nuke** — strumenti per gli attacchi di rete ad alcune vulnerabilità conosciute dei sistemi operativi al fine di causare un arresto di emergenza del sistema attaccato;
- **DDoS** — programma agent studiato per effettuare gli attacchi di rete distribuiti di "negazione del servizio" (Distributed Denial Of Service);
- **FDOS** (sinonimo: **Flooder**) — **Flooder Denial Of Service** — programmi per vari tipi di azioni malevole nella Rete che in un modo o nell'altro utilizzano l'idea di un attacco "negazione del servizio" (denial-of-service); a differenza del DDoS quando molti agent su più computer vengono utilizzati contemporaneamente contro lo stesso bersaglio, l'FDOS funziona come un programma separato "autosufficiente".

### Script virus

Prefissi dei virus scritti in diversi linguaggi di scripting:

- **VBS** — Visual Basic Script;
- **JS** — Java Script;
- **Wscript** — Visual Basic Script e/o Java Script;



- Perl — Perl;
- PHP — PHP;
- BAT — linguaggio dell'interprete comandi del sistema operativo MS-DOS.

## Programmi malevoli

Prefissi degli oggetti che sono altri programmi malevoli, anziché virus:

- Adware — programma di visualizzazione di pubblicità;
- Dialer — programma di effettuazione di chiamate del modem (reindirizza una chiamata del modem a un numero o una riscorsa a pagamento che sono impostati nel programma);
- Joke — programma scherzo;
- Program — programma potenzialmente pericoloso (riskware);
- Tool — utility di hacking (hacktool).

## Varie

Il prefisso `generic` è usato dopo un altro prefisso che indica l'ambiente o il metodo di sviluppo software per indicare un campione tipico di questo tipo di virus. Tale virus non possiede alcuni tratti distintivi (come per esempio stringhe di testo, effetti speciali ecc.) che avrebbero permesso di attribuirgli un nome specifico.

In precedenza, per denominare i virus più semplici senza volto, veniva utilizzato il prefisso `Silly` con diversi modificatori.

## Suffissi

I suffissi vengono utilizzati per denominare alcuni oggetti di virus specifici:

- `generator` — l'oggetto non è un virus, ma è un generatore di virus;
- `based` — il virus è stato sviluppato tramite il generatore di virus specificato o tramite la modifica del virus specificato. In entrambi i casi i nomi di questo tipo sono gentilizi e possono denotare centinaia e talvolta persino migliaia di virus;
- `dropper` — indica che l'oggetto non è un virus, ma è l'installer del virus specificato.



