



## Guida rapida all'installazione della rete antivirus

Жасағаныңды қорға

دافع عن إبداعاتك

Защити созданное

Defend what you create

Protégez votre univers

Verteidige, was du erschaffen hast

Захисти створене

保护您创建的一切

Защити созданное

Proteggi ciò che crei

Жасағаныңды қорға

Защити созданное

Proteggi ciò che crei

Verteidige, was du erschaffen hast

Захисти створене

**Defend what you create**

脅威からの保護を提供します

Protégez votre univers

Proteggi ciò che crei

Захисти створене

دافع عن إبداعاتك

脅威からの保護を提供します

Defend what you create

Жасағаныңды қорға

دافع عن إبداعاتك

دافع عن إبداعاتك

Protégez votre univers

保护您创建的一切

Защити созданное

脅威からの保護を提供します

Захисти створене

Verteidige, was du erschaffen hast

© **Doctor Web, 2017. Tutti i diritti riservati**

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, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, AV-Desk 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.

## **Dr.Web Enterprise Security Suite**

**Versione 10.01.0**

**Guida rapida all'installazione della rete antivirus**

**28/04/2017**

Doctor Web, Sede centrale in Russia

125040

Russia, Mosca

3° via Yamskogo polya, 2, 12A

Sito web: <http://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>Capitolo 1: Dr.Web Enterprise Security Suite</b>	<b>5</b>
<b>1.1. Introduzione</b>	<b>5</b>
1.1.1. Scopo del documento	5
1.1.2. Segni convenzionali	6
<b>1.2. Sul prodotto</b>	<b>7</b>
<b>1.3. Requisiti di sistema</b>	<b>11</b>
<b>1.4. Contenuto del pacchetto</b>	<b>13</b>
<b>Capitolo 2: Creazione della rete antivirus</b>	<b>15</b>
<b>Allegato A. Concessione delle licenze</b>	<b>19</b>
<b>Allegato B. Supporto tecnico</b>	<b>21</b>



# Capitolo 1: Dr.Web Enterprise Security Suite

## 1.1. Introduzione

### 1.1.1. Scopo del documento

Le istruzioni per l'implementazione della rete antivirus contengono le brevi informazioni sull'installazione e sulla prima configurazione dei componenti della rete antivirus. Per le informazioni dettagliate, consultare la documentazione dell'amministratore.

La documentazione dell'amministratore della rete antivirus Dr.Web Enterprise Security Suite si compone delle seguenti parti principali:

1. **Guida all'installazione** (file **drweb-esuite-10-install-manual-it.pdf**)
2. **Manuale dell'amministratore** (file **drweb-esuite-10-admin-manual-it.pdf**)
3. **Allegati** (file **drweb-esuite-10-appendices-it.pdf**)



Nella documentazione sono presenti i riferimenti incrociati tra i documenti elencati. Se i documenti sono stati scaricati su un computer locale, i riferimenti incrociati saranno operanti solo se i documenti sono situati nella stessa directory e hanno i nomi originali.



Prima di leggere i documenti, assicurarsi che questa sia la versione più recente dei Manuali. I manuali vengono aggiornati in continuazione, l'ultima versione può sempre essere reperita sul sito ufficiale della società Doctor Web <https://download.drweb.com/doc/>.



## 1.1.2. Segni convenzionali

In questo manuale vengono utilizzati i segni convenzionali riportati nella tabella 1-1.

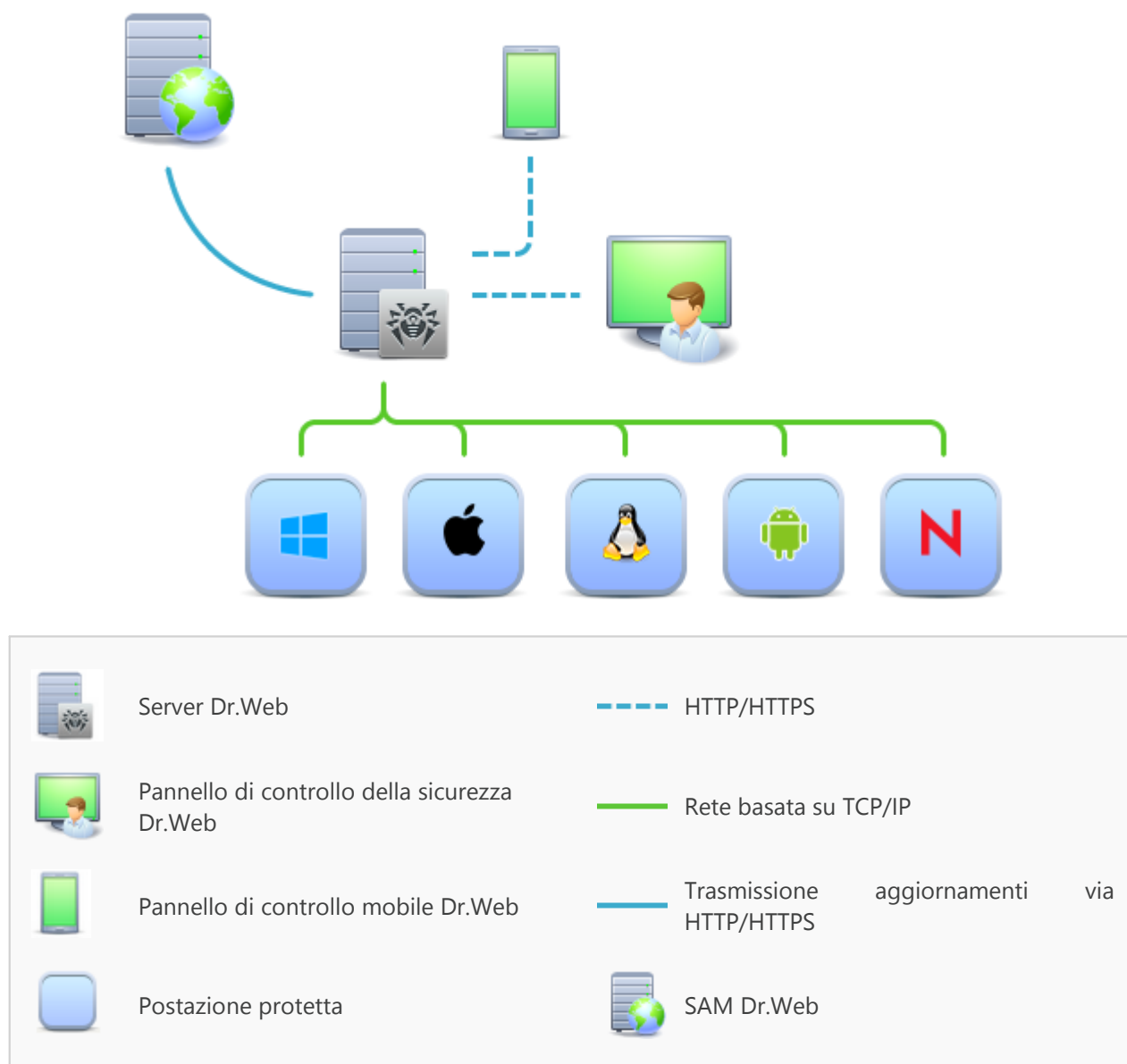
**Tabella 1-1. Segni convenzionali**

Segno	Commento
	Nota importante o istruzione.
	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.
<b>Salva</b>	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.

## 1.2. Sul prodotto

Dr.Web Enterprise Security Suite è progettato per installare e gestire una protezione antivirus completa e affidabile della rete interna aziendale, compresi i dispositivi mobili, e dei computer di casa dei dipendenti.

L'insieme dei computer e dei dispositivi mobili su cui sono installati i componenti interagenti di Dr.Web Enterprise Security Suite costituisce una *rete antivirus* unica.



**Immagine 1-1. Struttura logica della rete antivirus**

La rete antivirus Dr.Web Enterprise Security Suite ha l'architettura *client-server*. I suoi componenti vengono installati sui computer e dispositivi mobili degli utenti e degli amministratori, nonché sui computer che svolgono le funzioni server della rete locale. I componenti della rete antivirus scambiano le informazioni attraverso i protocolli di rete TCP/IP. Si può installare (e successivamente gestire) il software antivirus sulle postazioni protette sia via LAN che via Internet.



## Server di protezione centralizzata

Il server di protezione centralizzata viene installato su uno dei computer della rete antivirus, e l'installazione è possibile su qualsiasi computer e non soltanto sul computer che svolge le funzioni server LAN. I requisiti principali di tale computer sono riportati in [Requisiti di sistema](#).

Il carattere multiplatforma del software server permette di utilizzare come Server un computer gestito dai seguenti sistemi operativi:

- SO Windows®,
- SO della famiglia UNIX® (Linux®, FreeBSD®, Solaris™).

Il server di protezione centralizzata conserva pacchetti antivirus per i diversi SO dei computer protetti, aggiornamenti dei database dei virus e dei pacchetti antivirus, le chiavi di licenza e le impostazioni dei pacchetti dei computer protetti. Il Server riceve gli aggiornamenti dei componenti di protezione antivirus e dei database dei virus tramite Internet dai server del Sistema di aggiornamento mondiale e distribuisce gli aggiornamenti alle postazioni protette.

## Database unico

Il database unico viene collegato al Server di protezione centralizzata e conserva i dati statistici di eventi della rete antivirus, le impostazioni del Server stesso, le impostazioni delle postazioni protette e dei componenti antivirus da installare sulle postazioni protette.

## Pannello di controllo di protezione centralizzata

Il Pannello di controllo di protezione centralizzata viene installato automaticamente insieme al Server e fornisce un'interfaccia web utilizzata per gestire su remoto il Server e la rete antivirus modificando le impostazioni del Server, nonché le impostazioni dei computer protetti, conservate sul Server e sui computer protetti.

Il Pannello di controllo può essere aperto su qualsiasi computer che ha l'accesso di rete al Server. È possibile utilizzare il Pannello di controllo sotto quasi ogni sistema operativo, con l'utilizzo delle complete funzioni sotto i seguenti browser:

- Windows® Internet Explorer®,
- Mozilla® Firefox®,
- Google Chrome®.

L'elenco delle possibili varianti di utilizzo è riportato nel p. [Requisiti di sistema](#).

Fa parte del Pannello di controllo della sicurezza Dr.Web il Web server che viene installato automaticamente insieme al Server. L'obiettivo principale del Web server è assicurare il lavoro con le pagine del Pannello di controllo e con le connessioni di rete client.

## Pannello di controllo mobile di protezione centralizzata

Come un componente separato, viene fornito il Pannello di controllo mobile che è progettato per l'installazione e l'esecuzione su dispositivi mobili iOS e SO Android. I requisiti di base per l'applicazione sono riportati in p. [Requisiti di sistema](#).





Il Pannello di controllo mobile viene connesso al Server sulla base delle credenziali dell'amministratore di rete antivirus, anche attraverso il protocollo criptato.

Si può scaricare il Pannello di controllo mobile dal Pannello di controllo o direttamente da [App Store](#) e [Google Play](#).

## Protezione delle postazioni della rete

Sui computer e dispositivi mobili protetti vengono installati il modulo di gestione (Agent) e il pacchetto antivirus corrispondente al sistema operativo in uso.

Il carattere multiplatforma del software permette di proteggere contro i virus i computer e dispositivi mobili gestiti dai seguenti sistemi operativi:

- SO Windows®,
- SO della famiglia UNIX®,
- OS X®,
- Android,
- SO Novell® NetWare®.

Postazioni protette possono essere sia i computer degli utenti che i server LAN. In particolare, è supportata la protezione antivirus del sistema email Microsoft® Outlook®.

Il modulo di gestione aggiorna regolarmente dal Server i componenti antivirus e i database dei virus, nonché invia al Server informazioni sugli eventi di virus accaduti sul computer protetto.

Se il Server di protezione centralizzata non è disponibile, i database dei virus di postazioni protette possono essere aggiornati direttamente tramite Internet dal Sistema di aggiornamento mondiale.

## Assicurazione della comunicazione tra i componenti della rete anti-virus

Per assicurare la comunicazione stabile e sicura tra i componenti della rete antivirus, vengono fornite le seguenti possibilità:

### Server proxy Dr.Web

Il Server proxy può essere incluso opzionalmente nella struttura di rete antivirus. L'obiettivo principale del Server proxy è assicurare la comunicazione del Server e delle postazioni protette nel caso non sia possibile organizzare l'accesso diretto.

### Compressione del traffico

Vengono forniti gli algoritmi di compressione dei dati per la comunicazione tra i componenti di rete antivirus, il che riduce il traffico di rete al minimo.



## Cifratura del traffico

Viene fornita la possibilità di cifrare i dati trasmessi tra i componenti di rete antivirus, il che assicura un ulteriore livello di protezione.

## Possibilità aggiuntive

### NAP Validator

NAP Validator viene fornito come un componente aggiuntivo e permette di utilizzare la tecnologia Microsoft Network Access Protection (NAP) per controllare l'operatività del software delle postazioni protette.

### Loader di repository

Il Loader di repository Dr.Web, fornito come utility aggiuntiva, permette di scaricare i prodotti Dr.Web Enterprise Security Suite dal Sistema di aggiornamento mondiale. Si può utilizzarlo per scaricare aggiornamenti dei prodotti Dr.Web Enterprise Security Suite per mettere gli aggiornamenti su un Server non connesso a Internet.



## 1.3. Requisiti di sistema

Per il funzionamento del Server Dr.Web occorre:

Componente	Requisiti
Processore e sistema operativo	<p>Sono supportati i seguenti sistemi operativi installati sui computer con le CPU corrispondenti:</p> <ul style="list-style-type: none"><li>• CPU con il supporto del set di istruzioni SSE2 e con la frequenza di clock di 1,3 GHz e superiori:<ul style="list-style-type: none"><li>▫ SO Windows;</li><li>▫ SO Linux;</li><li>▫ SO FreeBSD;</li><li>▫ SO Solaris x86.</li></ul></li><li>• CPU V9 UltraSPARC III e superiori:<ul style="list-style-type: none"><li>▫ SO Solaris Sparc.</li></ul></li></ul> <p>La lista completa degli SO supportati è riportata nel documento <b>Allegati</b>, in <a href="#">Allegato A</a>.</p>
Memoria operativa	<ul style="list-style-type: none"><li>• Requisiti minimi: 1 GB.</li><li>• Requisiti consigliati: 2 GB e superiori.</li></ul>
Spazio su disco rigido	almeno 12 GB: fino ai 8 GB per il database incorporato (directory di installazione), fino ai 4 GB nella directory temporanea di sistema (per i file operativi).

Per il funzionamento del Pannello di controllo della sicurezza Dr.Web occorre:

a) Browser web:

Web browser	Supporto
Windows Internet Explorer 8 e superiori	È supportato
Mozilla Firefox 25 e superiori	
Google Chrome 30 e superiori	
Opera® 10 e superiori	L'uso è ammissibile, però la possibilità di lavoro non è garantita.
Safari® 4 e superiori	

b) Per utilizzare le piene funzionalità del Pannello di controllo, è necessario installare l'estensione del Pannello di controllo della sicurezza Dr.Web. L'estensione viene fornita insieme al pacchetto Server e viene installata a richiesta del browser nel processo di utilizzo degli elementi del



Pannello di controllo che necessitano del caricamento dell'estensione (per Scanner di rete, per l'installazione remota di componenti antivirus).

L'installazione dell'estensione è possibile nei seguenti browser:

Web browser	Versione minima supportata	Versione massima supportata
Windows Internet Explorer	8	11
Mozilla Firefox	25	50.0.1
Google Chrome	30	44.0.2403

La risoluzione schermo consigliata per l'utilizzo del Pannello di controllo è 1280x1024 px.

### Per il funzionamento del Pannello di controllo mobile Dr.Web occorre:

I requisiti variano a seconda del sistema operativo su cui viene installata l'applicazione:

Sistema operativo	Requisito	
	Versione del sistema operativo	Dispositivo
iOS	iOS® 7 e superiori	Apple® iPhone® Apple® iPad®
Android	Android 4.0 e superiori	–

### Per il funzionamento dell'Agent Dr.Web e del pacchetto antivirus completo occorre:

I requisiti sono diversi a seconda del sistema operativo in cui viene installata la soluzione antivirus (la lista completa dei sistemi operativi supportati è riportata nel documento **Allegati**, in [Allegato A. Lista completa delle versioni supportate dei SO](#)):

- SO Windows:

Componente	Requisito
Processore	CPU con la frequenza di clock di 1 GHz e superiori.
Memoria operativa libera	Almeno 512 MB.
Spazio libero su disco rigido	Almeno 1 GB per i file eseguibili + spazio aggiuntivo per i log di funzionamento e per i file temporanei.



- SO della famiglia Linux:

Componente	Requisito
Processore	Sono supportati i processori con l'architettura e il set di istruzioni Intel/AMD: 32 bit (IA-32, x86); 64 bit (x86-64, x64, amd64).
Memoria operativa libera	Almeno 512 MB.
Spazio libero su disco rigido	Almeno 400 MB di spazio libero sul volume su cui sono situate le directory di Antivirus.

- OS X, SO Android, SO Novell NetWare: i requisiti di configurazione coincidono con i requisiti di sistema operativo.

## 1.4. Contenuto del pacchetto

**Il pacchetto Dr.Web Enterprise Security Suite viene fornito a seconda di SO di Server Dr.Web scelto:**

1. In caso di UNIX – come file in formato `run`:

Nome del file	Componente
<code>drweb-esuite-server-10.01.0-&lt;build&gt;-&lt;versione_SO&gt;.run</code>	Pacchetto principale di Server Dr.Web*
<code>drweb-esuite-extra-10.01.0-&lt;build&gt;-&lt;versione_SO&gt;.run</code>	Pacchetto supplementare di Server Dr.Web
<code>drweb-esuite-proxy-10.01.0-&lt;build&gt;-&lt;versione_SO&gt;.run</code>	Server proxy

2. In caso di Windows – come file eseguibili:

Nome del file	Componente
<code>drweb-esuite-server-10.01.0-&lt;build&gt;-&lt;versione_SO&gt;.exe</code>	Pacchetto principale di Server Dr.Web*
<code>drweb-esuite-extra-10.01.0-&lt;build&gt;-&lt;versione_SO&gt;.exe</code>	Pacchetto supplementare di Server Dr.Web
<code>drweb-esuite-proxy-10.01.0-&lt;build&gt;-&lt;versione_SO&gt;.msi</code>	Server proxy
<code>drweb-esuite-agent-activedirectory-10.01.0-&lt;build&gt;.msi</code>	Agent Dr.Web per Active Directory
<code>drweb-esuite-modify-ad-schema-10.01.0-&lt;build&gt;-&lt;versione_SO&gt;.exe</code>	Utility per modificare lo schema Active Directory



Nome del file	Componente
drweb-esuite-aduac-10.01.0-<build>-<versione_SO>.msi	Utility per modificare gli attributi degli oggetti Active Directory
drweb-esuite-napshv-10.01.0-<build>-<versione_SO>.msi	NAP Validator
drweb-esuite-agent-full-11.00.0-<versione_build>-windows.exe	Installer completo di Agent Dr.Web. Anche fa parte del pacchetto supplementare di Server Dr.Web.

**\*Il pacchetto principale di Server Dr.Web include i seguenti componenti:**

- software di Server Dr.Web per il SO corrispondente,
- software di Agent Dr.Web e di pacchetti antivirus per le postazioni SO Windows,
- software di Pannello di controllo della sicurezza Dr.Web,
- database dei virus,
- Estensione del Pannello di controllo della sicurezza Dr.Web,
- Estensione Dr.Web Server FrontDoor,
- documentazione, moduli ed esempi.

Oltre al pacchetto, vengono forniti anche i numeri di serie, dopo la registrazione dei quali si ottengono i file con le chiavi di licenza.



## Capitolo 2: Creazione della rete antivirus

### Brevi istruzioni per l'installazione di una rete antivirus:

1. Preparare uno schema della struttura della rete antivirus, includerci tutti i computer e dispositivi mobili protetti.

Selezionare il computer che svolgerà le funzioni di Server Dr.Web. In una rete antivirus potrebbero rientrare diversi Server Dr.Web. Le caratteristiche di tale configurazione sono descritte in **Manuale dell'amministratore**, p. [Caratteristiche di una rete con diversi Server Dr.Web](#).



Il Server Dr.Web può essere installato su qualsiasi computer e non soltanto su quello che svolge le funzioni server LAN. I requisiti principali nei confronti di tale computer sono riportati in p. [Requisiti di sistema](#).

Su tutte le postazioni protette, compresi i server di rete locale, viene installata la stessa versione di Agent Dr.Web. La differenza sta nella lista dei componenti antivirus che vengono installati, definita in base alle impostazioni sul Server.

Per installare il Server Dr.Web e l'Agent Dr.Web, è necessario accedere una volta ai relativi computer (fisicamente o utilizzando strumenti di gestione e di avvio programmi su remoto). Tutte le operazioni successive vengono eseguite dalla postazione di lavoro dell'amministratore della rete antivirus (anche probabilmente dall'esterno della rete locale) e non richiedono l'accesso ai Server Dr.Web o alle postazioni.

2. In base allo schema progettato determinare quali prodotti per quali sistemi operativi si dovranno installare sui nodi della rete corrispondenti. Le informazioni dettagliate sui prodotti disponibili sono riportate nella sezione [Contenuto del pacchetto](#).

Tutti i prodotti richiesti possono essere acquistati come le soluzioni boxed Dr.Web Enterprise Security Suite o scaricati sul sito web della società Doctor Web <https://download.drweb.com/>.



Agent Dr.Web per le postazioni SO Android, SO Linux, OS X possono anche essere installati dai pacchetti di prodotti standalone e successivamente connessi al Server Dr.Web centralizzato. Le relative impostazioni di Agent sono descritte in **Guida all'installazione**, p. [Installazione di Agent Dr.Web attraverso il pacchetto d'installazione personale](#).

3. Installare il pacchetto principale di Server Dr.Web su uno o diversi computer selezionati. L'installazione viene descritta in **Guida all'installazione**, p. [Installazione di Server Dr.Web](#).

Insieme al Server viene installato il Pannello di controllo della sicurezza Dr.Web.

Di default, Server Dr.Web viene avviato automaticamente dopo l'installazione e dopo ogni riavvio del sistema operativo.

4. Se la rete antivirus includerà le postazioni protette SO Android, SO Linux, OS X, installare il pacchetto supplementare di Server Dr.Web su tutti i computer su cui è installato il pacchetto principale di Server.
5. Se necessario, installare e configurare il Server proxy. La descrizione viene riportata in **Guida all'installazione**, p. [Installazione del Server proxy](#).



6. Per configurare il Server e il software antivirus su postazioni, è necessario connettersi al Server attraverso il Pannello di controllo della sicurezza Dr.Web.



Il Pannello di controllo può essere aperto su qualsiasi computer e non soltanto su quello su cui è installato il Server. Basta che ci sia una connessione di rete con il computer su cui è installato il Server.

Il Pannello di controllo è disponibile sull'indirizzo:

`http://<Indirizzo_Server>:9080`

o

`https://<Indirizzo_Server>:9081`

dove come <Indirizzo\_Server> indicare l'indirizzo IP o il nome a dominio del computer su cui è installato il Server Dr.Web.

Nella finestra di dialogo di richiesta di autenticazione impostare il nome utente e la password dell'amministratore.

Il nome di amministratore predefinito è **admin**.

La password:

- in caso di SO Windows – la password che è stata impostata quando veniva installato il Server.
- in caso di SO della famiglia UNIX – **root**.



Per il Server sotto SO della famiglia UNIX modificare la password di amministratore predefinita al momento della prima connessione al Server.

In caso di una connessione riuscita al Server, si apre la finestra principale del Pannello di controllo (per la descrizione dettagliata v. in **Manuale dell'amministratore**, in p. [Pannello di controllo della sicurezza Dr.Web](#)).

7. Effettuare la configurazione iniziale di Server (le impostazioni di Server vengono descritte dettagliatamente in **Manuale dell'amministratore**, in [Capitolo 8: Configurazione di Server Dr.Web](#)):
- a. Nella sezione [Gestione licenze](#) aggiungere uno o più chiavi di licenza e distribuirle ai gruppi corrispondenti, in particolare, al gruppo **Everyone**. Il passaggio è obbligatorio se durante l'installazione di Server la chiave di licenza non è stata impostata.
  - b. Nella sezione [Configurazione generale del repository](#) impostare quali componenti della rete antivirus verranno aggiornati da SAM Dr.Web. Nella sezione [Stato del repository](#) eseguire un aggiornamento dei prodotti nel repository di Server. L'aggiornamento può richiedere un lungo tempo. Attendere fino a quando il processo di aggiornamento non sarà terminato prima di proseguire con la successiva configurazione.
  - c. Sulla pagina **Amministrazione** → **Server Dr.Web** sono riportate le informazioni sulla versione di Server. Se è disponibile una nuova versione, aggiornare Server, come descritto in **Manuale dell'amministratore**, p. [Aggiornamento di Server Dr.Web e ripristino da copia di backup](#).





- d. Se necessario, configurare [Connessioni di rete](#) per modificare le impostazioni di rete di default utilizzate per l'interazione di tutti i componenti della rete antivirus.
  - e. Se necessario, configurare la lista degli amministratori di Server. Inoltre, è disponibile l'autenticazione di amministratori esterna. Per maggiori informazioni v. **Manuale dell'amministratore**, [Capitolo 5: Amministratori della rete antivirus](#).
  - f. Prima di iniziare ad utilizzare il software antivirus, è consigliabile modificare l'impostazione della directory per il backup dei dati critici del Server (v. **Manuale dell'amministratore**, p. [Configurazione del calendario di Server Dr.Web](#)). È preferibile collocare questa directory su un altro disco locale per ridurre la probabilità di una perdita simultanea dei file del software Server e della copia di backup.
8. Configurare il software antivirus per le postazioni (la configurazione dei gruppi e delle postazioni viene descritta dettagliatamente in **Manuale dell'amministratore**, in [Capitolo 6](#) e [Capitolo 7](#)):
- a. Se necessario, creare gruppi di postazioni personalizzati.
  - b. Configurare il gruppo **Everyone** e i gruppi personalizzati creati. In particolare, configurare la sezione dei componenti da installare.
9. Installare il software Agent Dr.Web sulle postazioni.
- Nella sezione [File di installazione](#) controllare l'elenco dei file disponibili per l'installazione di Agent. Selezionare la variante di installazione adatta, basandosi sul sistema operativo della postazione, sulla possibilità di installazione su remoto, sulla variante di configurazione delle impostazioni di Server nel corso dell'installazione di Agent ecc. Per esempio:
- Se gli utenti installano l'antivirus in autonomo, utilizzare pacchetti di installazione personali che vengono creati attraverso il Pannello di controllo separatamente per ciascuna postazione. Questo tipo di pacchetti può inoltre essere inviato agli utenti via email direttamente dal Pannello di controllo. Dopo l'installazione le postazioni si connettono al Server in modo automatico.
  - Per un'installazione remota attraverso la rete allo stesso tempo su una o più postazioni (soltanto per le postazioni SO Windows) utilizzare l'installer di rete. L'antivirus viene installato attraverso il Pannello di controllo con l'impiego di una determinata estensione del browser.
  - Inoltre, è possibile installare l'antivirus in remoto attraverso la rete su una o più postazioni, utilizzando il servizio Active Directory. A tale scopo si usa l'installer di Agent Dr.Web per le reti con Active Directory che viene fornito insieme al pacchetto Dr.Web Enterprise Security Suite, ma separatamente dall'installer di Server.
  - Se nel processo dell'installazione è necessario ridurre il carico sul canale di comunicazione tra Server e postazioni, è possibile utilizzare l'installer completo che installa contemporaneamente Agent e i componenti di protezione.
  - L'installazione su postazioni Android, Linux, OS X può essere eseguita localmente secondo le regole generali. Inoltre, un prodotto standalone già installato può connettersi al Server sulla base della configurazione corrispondente.
10. Non appena installati sui computer, gli Agent si connettono automaticamente al Server. Le postazioni antivirus vengono autenticate sul Server a seconda dei criteri scelti (v. **Manuale dell'amministratore**, p. [Criteri di approvazione delle postazioni](#)):



- a. In caso di installazione dai pacchetti di installazione e inoltre in caso di configurazione di conferma automatica sul Server, le postazioni vengono registrate automaticamente al momento della prima connessione al Server e non è richiesta alcuna ulteriore conferma.
  - b. In caso di installazione dagli installer e di configurazione di conferma di accesso manuale, l'amministratore deve confermare manualmente le nuove postazioni in modo da registrarle sul Server. In questo caso, le nuove postazioni non vengono connesse automaticamente, ma vengono messe dal Server nel gruppo dei nuovi arrivi.
11. Dopo che la postazione si è connessa al Server e ha ottenuto le impostazioni, su di essa viene installato il relativo set di componenti del pacchetto antivirus, definito nelle impostazioni del gruppo primario della postazione.



Per completare l'installazione dei componenti della postazione, sarà necessario il riavvio del computer.

12. È possibile configurare le postazioni e il software antivirus anche dopo l'installazione (la descrizione dettagliata viene riportata in **Manuale dell'amministratore**, in [Capitolo 7](#)).



## Allegato A. Concessione delle licenze

Per il funzionamento della soluzione antivirus Dr.Web Enterprise Security Suite è necessaria una licenza.

Il contenuto e il prezzo di una licenza di utilizzo di Dr.Web Enterprise Security Suite dipendono dal numero di postazioni protette, compresi i server che rientrano nella rete di Dr.Web Enterprise Security Suite come postazioni protette.



Queste informazioni si devono obbligatoriamente comunicare al rivenditore della licenza prima dell'acquisto della soluzione Dr.Web Enterprise Security Suite. Il numero di Server Dr.Web in uso non influisce sull'aumento del prezzo della licenza.

### File della chiave di licenza

I diritti di utilizzo di Dr.Web Enterprise Security Suite vengono regolati tramite i file della chiave di licenza.



Il formato del file della chiave è protetto da modifica tramite il metodo di firma digitale. La modifica del file lo rende non valido. Per evitare danni accidentali al file della chiave di licenza, non si deve modificarlo e/o salvarlo dopo averlo visualizzato in un editor di testo.

I file della chiave di licenza vengono forniti in un archivio .zip contenente uno o più file della chiave per postazioni protette.

### L'utente può ottenere i file della chiave di licenza in uno dei seguenti modi:

- Il file della chiave di licenza fa parte del set antivirus Dr.Web Enterprise Security Suite acquistato, se è stato incluso nel pacchetto software all'assemblaggio. Tuttavia, di regola, vengono forniti solamente i numeri di serie.
- Il file della chiave di licenza viene inviato agli utenti via email dopo la registrazione del numero di serie sul sito web della società Doctor Web sull'indirizzo <http://products.drweb.com/register/>, se un altro indirizzo non è indicato nella scheda di registrazione allegata al prodotto. Andare al sito indicato, compilare il modulo con le informazioni sull'acquirente e inserire nel campo indicato il numero di serie di registrazione (è reperibile nella scheda di registrazione). Un archivio con i file della chiave verrà inviato sull'indirizzo email indicato dall'utente. Si potrà inoltre scaricare i file della chiave direttamente dal sito indicato.
- Il file della chiave di licenza può essere fornito su un supporto separato.

Si consiglia di conservare il file della chiave di licenza fino alla scadenza della sua validità e di utilizzarlo per la reinstallazione o per il ripristino dei componenti del programma. In caso di perdita del file della chiave di licenza, si può rifare la procedura di registrazione sul sito indicato e ottenere nuovamente un file della chiave di licenza. A questo scopo occorre indicare lo stesso numero di serie di registrazione e le stesse informazioni sull'acquirente che sono state indicate per la pri-



ma registrazione; soltanto l'indirizzo email può essere diverso. In questo caso il file della chiave di licenza verrà inviato sul nuovo indirizzo email.

Per provare l'Antivirus, è possibile utilizzare i file della chiave demo. Tali file della chiave assicurano le funzionalità complete dei principali componenti antivirus, ma hanno una validità limitata. Per ottenere i file della chiave demo, è necessario compilare un modulo situato sulla pagina <https://download.drweb.com/demoreq/biz/>. La richiesta verrà valutata su base individuale. Nel caso di decisione positiva, un archivio con i file della chiave di licenza verrà inviato sull'indirizzo email indicato dall'utente.



Per maggiori informazioni circa i principi e le caratteristiche della concessione delle licenze Dr.Web Enterprise Security Suite consultare **Manuale dell'amministratore**, sottosezioni di [Capitolo 2. Concessione delle licenze](#).

L'utilizzo dei file della chiave di licenza nel processo di installazione del programma è descritto in **Guida all'installazione**, p. [Installazione di Server Dr.Web](#).

L'utilizzo dei file della chiave di licenza per una rete antivirus già dispiegata è descritto in **Manuale dell'amministratore**, p. [Gestione licenze](#).



## Allegato B. Supporto tecnico

Se si verificano dei problemi con l'installazione o il funzionamento dei prodotti della società, prima di chiedere assistenza al servizio 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 [http://support.drweb.com/show\\_faq/](http://support.drweb.com/show_faq/);
- visitare i forum della società Doctor Web sull'indirizzo <http://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 <http://support.drweb.com/>;
- chiamare al telefono a Mosca: +7 (495) 789-45-86 o il numero verde per la Russia: 8-800-333-7932.

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

