



# Dr.WEB

Enterprise Security Suite

## Guida rapida all'installazione della rete antivirus



© **Doctor Web, 2021. 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.

**Dr.Web Enterprise Security Suite**  
**Versione 12.0**  
**Guida rapida all'installazione della rete antivirus**  
**20/02/2021**

Doctor Web, Sede centrale in Russia

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

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

Telefono +7 (495) 789-45-87

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

## **Doctor Web**

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

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

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

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

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



## Sommario

<b>Capitolo 1: Introduzione</b>	<b>5</b>
1.1. Scopo del documento	5
1.2. Segni convenzionali	5
<b>Capitolo 2: Dr.Web Enterprise Security Suite</b>	<b>7</b>
2.1. Sul prodotto	7
2.2. Requisiti di sistema	10
2.3. Contenuto del pacchetto	13
<b>Capitolo 3: Creazione della rete antivirus</b>	<b>15</b>
<b>Allegato A. Concessione delle licenze</b>	<b>20</b>
<b>Allegato B. Supporto tecnico</b>	<b>22</b>



## Capitolo 1: Introduzione

### 1.1. Scopo del documento

La guida rapida all'installazione della rete antivirus contiene brevi informazioni sull'installazione e sulla configurazione iniziale dei componenti della rete antivirus. Per informazioni dettagliate consultare la documentazione dell'amministratore.

La documentazione dell'amministratore della rete antivirus è composta dalle seguenti parti principali:

1. **Guida all'installazione**
2. **Manuale dell'amministratore**
3. **Allegati**

Inoltre, sono forniti i seguenti Manuali:

1. **Manuale dell'amministratore per la gestione delle postazioni**
2. **Manuali dell'utente**
3. **Guide alle Web API**
4. **Guida al database del Server Dr.Web**

Tutti i manuali elencati sopra sono forniti anche come parte del prodotto Dr.Web Enterprise Security Suite e possono essere aperti attraverso il Pannello di controllo della sicurezza Dr.Web.



Prima di leggere i documenti, assicurarsi che questa sia l'ultima versione dei Manuali corrispondenti per la versione del prodotto in uso. I Manuali vengono aggiornati in continuazione, e la loro ultima versione è ritrovabile sul sito ufficiale dell'azienda Doctor Web sull'indirizzo

<https://download.drweb.com/doc/>.

### 1.2. Segni convenzionali

#### Segni convenzionali

In questo manuale vengono utilizzati i seguenti simboli:

Simbolo	Commento
	Nota importante o istruzione.
	Avviso di possibili situazioni di errore, nonché di punti importanti cui prestare particolare attenzione.



Simbolo	Commento
<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.

## Abbreviazioni

Nel testo del Manuale possono essere utilizzate le seguenti abbreviazioni senza spiegazione:

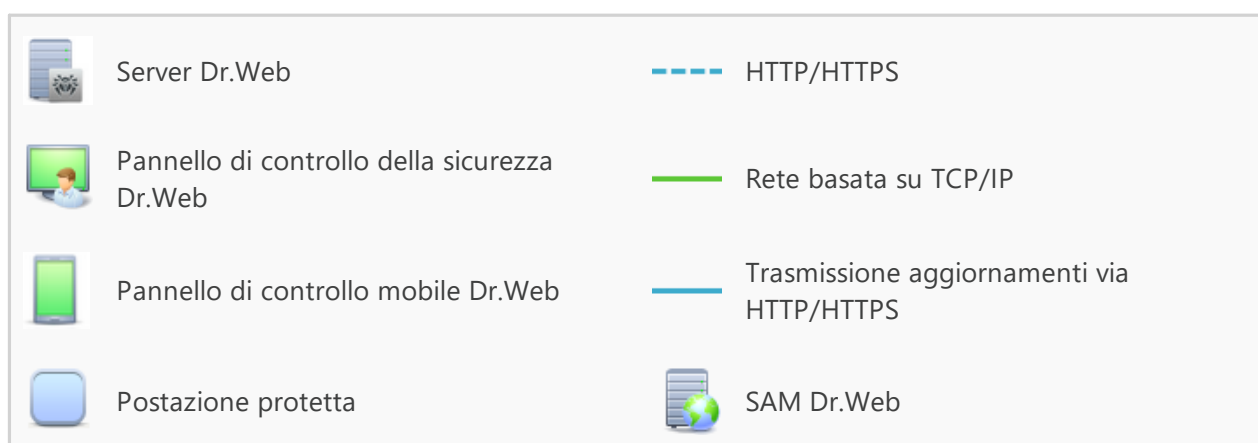
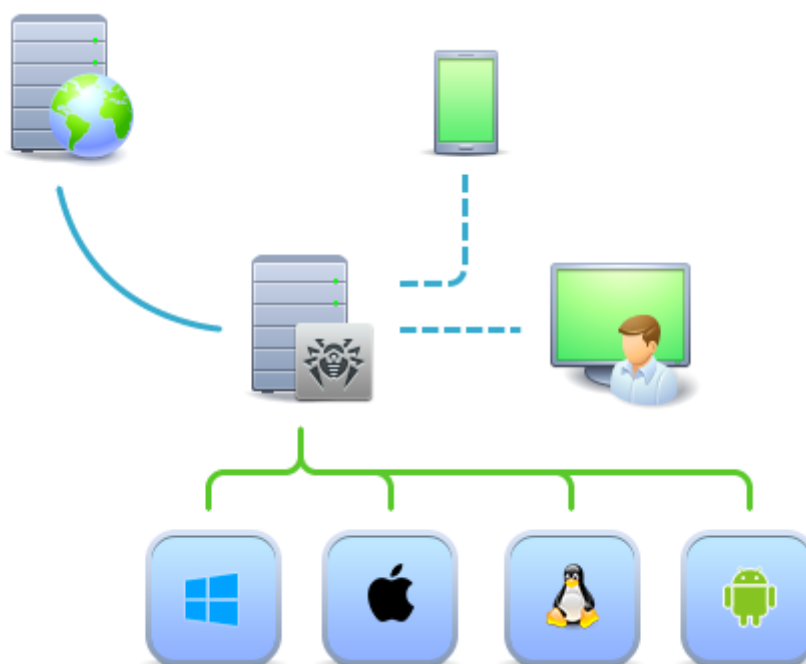
- ACL — lista di controllo degli accessi (Access Control List),
- CDN — rete di distribuzione di contenuti (Content Delivery Network),
- DFS — file system distribuito (Distributed File System),
- DNS — sistema dei nomi a dominio (Domain Name System),
- FQDN — nome di dominio completo (Fully Qualified Domain Name),
- GUI — interfaccia utente grafica (Graphical User Interface), versione del programma con la GUI — una versione che utilizza gli strumenti della GUI,
- MIB — database delle informazioni di gestione (Management Information Base),
- MTU — dimensione massima di un pacchetto dati (Maximum Transmission Unit),
- NAP — Network Access Protection,
- TTL — tempo di vita pacchetto (Time To Live),
- UDS — socket di dominio UNIX (UNIX Domain Socket),
- DB, DBMS — database, database management system,
- SAM Dr.Web — Sistema di aggiornamento mondiale di Dr.Web,
- LAN — rete locale,
- SO — sistema operativo,
- SW, software — programmi per computer.

## Capitolo 2: Dr.Web Enterprise Security Suite

### 2.1. 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 di computer e 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).

Il Server di protezione centralizzata conserva i pacchetti antivirus per i diversi SO dei computer protetti, gli 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,
- Microsoft Edge,
- 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 componente separato, viene fornito un Pannello di controllo mobile progettato per l'installazione e l'avvio su dispositivi mobili iOS e 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,
- macOS,
- SO Android.

Possono essere postazioni protette 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 delle postazioni protette possono essere aggiornati direttamente tramite internet dal Sistema di aggiornamento mondiale.

## Assicurazione della comunicazione tra i componenti della rete antivirus

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 della rete antivirus.

L'obiettivo principale del Server proxy è quello di fornire 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.

## Funzioni 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. Può essere utilizzato per scaricare gli aggiornamenti dei prodotti Dr.Web Enterprise Security Suite per collocare gli aggiornamenti su un Server non connesso a internet.

## 2.2. Requisiti di sistema

### Server Dr.Web

Componente	Requisiti
Processore	CPU con il supporto del set di istruzioni SSE2 e con la frequenza di clock di 1,3 GHz e superiori.
Memoria operativa	<ul style="list-style-type: none"><li>• Requisiti minimi: 1 GB.</li><li>• Requisiti consigliati: 2 GB o più.</li></ul>
Spazio su disco rigido	<ul style="list-style-type: none"><li>• Almeno 50 GB per il software Server e uno spazio aggiuntivo per la memorizzazione dei file temporanei, per esempio, pacchetti di installazione Agent individuali (circa 17 MB ognuno) nella sottodirectory <code>var\installers-cache</code> della directory di installazione Server Dr.Web.</li><li>• Fino a 5 GB per il database.</li><li>• A seconda del percorso di installazione del Server, sul disco di sistema in SO Windows o in <code>/var/tmp</code> nei sistemi operativi della famiglia UNIX (o in un'altra directory per i file temporanei, se è stata ridefinita):<ul style="list-style-type: none"><li>▫ per l'installazione del Server, sono necessari almeno 4,3 GB per l'avvio dell'installer e per l'estrazione dei file temporanei;</li></ul></li></ul>



Componente	Requisiti
	<ul style="list-style-type: none"><li>▫ per il funzionamento del Server, è necessario uno spazio libero sul disco di sistema per la memorizzazione dei file temporanei e di lavoro, a seconda delle dimensioni del database e delle impostazioni del repository.</li></ul>
Sistema operativo	<ul style="list-style-type: none"><li>• Windows (la lista completa dei sistemi operativi supportati è riportata nel documento <b>Allegati</b>, in <a href="#">Allegato A</a>).</li><li>• Linux, nel caso di presenza della libreria <code>glibc</code> 2.13 o versioni successive; incluso ALT Linux 5.0 o versioni successive, Astra Linux Special Edition 1.3 o versioni successive.</li><li>• FreeBSD 10.3 o versioni successive.</li></ul>
Supporto di ambienti virtuali e cloud	<p>È supportato il funzionamento sui sistemi operativi che soddisfano i requisiti elencati sopra, negli ambienti virtuali e cloud, tra cui:</p> <ul style="list-style-type: none"><li>• VMware;</li><li>• Hyper-V;</li><li>• Xen;</li><li>• KVM.</li></ul>



Server Dr.Web non può essere installato su dischi logici con file system che non supportano link simbolici, in particolare, con file system dalla famiglia FAT.



Le utility di amministrazione sono disponibili per il download attraverso il Pannello di controllo, sezione **Amministrazione** → **Utility**, devono essere eseguite su un computer che soddisfa i requisiti di sistema per il Server Dr.Web.

## Pannello di controllo della sicurezza Dr.Web

a) Browser web:

- Internet Explorer 11,
- Microsoft Edge 0.10 o versioni successive,
- Mozilla Firefox 44 o versioni successive,
- Google Chrome 49 o versioni successive,
- Opera di ultima versione,
- Safari di ultima versione.

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



## Pannello di controllo mobile Dr.Web

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

Sistema operativo	Requisito	
	Versione del sistema operativo	Dispositivo
iOS	iOS 9 e versioni successive	Apple iPhone Apple iPad
Android	Android 4.1–10	–

## Agent Dr.Web e il pacchetto antivirus

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 e uno spazio aggiuntivo per i log di funzionamento e per i file temporanei.

- SO della famiglia Linux:

Componente	Requisito
Processore	Processori con l'architettura e il set di istruzioni <ul style="list-style-type: none"><li>• Intel/AMD: 32 bit (IA-32, x86) e 64 bit (x86-64, x64, amd64);</li><li>• ARM64.</li></ul>
Memoria operativa libera	Almeno 512 MB (consigliato 1 GB o più).
Spazio libero su disco rigido	Almeno 500 MB di spazio libero sul volume su cui sono situate le directory di Antivirus.

- macOS, Android: i requisiti della configurazione coincidono con i requisiti del sistema operativo;



È supportato il funzionamento di Agent Dr.Web sui sistemi operativi che soddisfano i requisiti elencati sopra, negli ambienti virtuali e cloud, tra cui:

- VMware;
- Hyper-V;
- Xen;
- KVM.

## 2.3. 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 SO della famiglia UNIX:

- `drweb-<versione_pacchetto>-<build>-esuite-server-<versione_SO>.tar.gz.run`  
Pacchetto di Server Dr.Web\*
- `drweb-reploader-<sistema_operativo>-<numero_di_bit>`  
Versione console di Loader di repository Dr.Web.

2. In caso di SO Windows:

- `drweb-<versione_pacchetto>-<build>-esuite-server-<versione_SO>.exe`  
Pacchetto di Server Dr.Web\*
- `drweb-<versione_pacchetto>-<build>-esuite-agent-full-windows.exe`  
Installer completo di Agent Dr.Web.
- `drweb-reploader-windows-<numero_di_bit>.exe`  
Versione console di Loader di repository Dr.Web.
- `drweb-reploader-gui-windows-<numero_di_bit>.exe`  
Versione grafica di Loader di repository Dr.Web.

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

- software di Server Dr.Web per il SO corrispondente,
- dati di sicurezza di Server Dr.Web,
- software di Pannello di controllo della sicurezza Dr.Web,
- software di Agent Dr.Web e dei pacchetti antivirus per le postazioni con SO Windows,
- modulo di aggiornamento di Agent Dr.Web per Windows,
- Antispam di Dr.Web per Windows,
- database dei virus, database dei filtri incorporati dei componenti antivirus e di Antispam di Dr.Web per Windows,
- documentazione,



- notizie di Doctor Web.

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

**Dopo aver installato il Server Dr.Web, è inoltre possibile scaricare nel repository dai server SAM i seguenti Prodotti aziendali Dr.Web:**

- Installer completo di Agent Dr.Web per Windows,
- Prodotti per l'installazione sulle postazioni protette sotto SO UNIX (inclusi i server LAN), Android, macOS,
- Dr.Web per IBM Lotus Domino,
- Dr.Web per Microsoft Exchange Server,
- Server proxy Dr.Web,
- Agent Dr.Web per Active Directory,
- Utility per modificare lo schema Active Directory,
- Utility per modificare gli attributi degli oggetti Active Directory,
- NAP Validator.



Informazioni dettagliate su come gestire il repository di Server sono riportate in **Manuale dell'amministratore**, sezione [Gestione del repository di Server Dr.Web](#).



## Capitolo 3: 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 possono 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 di un server LAN. I principali requisiti 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.

Quando si pianifica una rete antivirus, si consiglia inoltre di creare un elenco di persone che devono avere accesso al Pannello di controllo in base alle loro mansioni e di preparare un elenco di ruoli con una lista di responsabilità funzionali assegnate a ciascun ruolo. Per ciascun ruolo deve essere creato un gruppo di amministratori. Amministratori specifici vengono associati a ruoli tramite l'inserimento dei loro account in gruppi di amministratori. Se necessario, i gruppi di amministratori (ruoli) possono essere gerarchicamente raggruppati in un sistema multilivello con la possibilità di configurare individualmente i permessi di accesso di amministratori per ciascun livello.

La descrizione dettagliata della gestione dei gruppi di amministratori e dei permessi di accesso è riportata in **Manuale dell'amministratore**, [Capitolo 6: Amministratori della rete antivirus](#)

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

Tutti i prodotti richiesti possono essere acquistati sotto forma di una soluzione boxed Dr.Web Enterprise Security Suite o scaricati sul sito web dell'azienda Doctor Web <https://download.drweb.com/>.



Gli Agent Dr.Web per le postazioni SO Android, SO Linux, macOS possono inoltre essere installati dai pacchetti dei prodotti standalone e successivamente connessi al Server



Dr.Web centralizzato. Le impostazioni degli Agent sono descritte nei relativi **Manuali utente**.

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 necessario, installare e configurare il Server proxy. La descrizione viene riportata in **Guida all'installazione**, p. [Installazione del Server proxy](#).
5. 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 inserire le credenziali dell'amministratore. Le credenziali dell'amministratore con i permessi completi di default:

- Nome utente — **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 — la password che è stata creata automaticamente durante l'installazione di Server (vedi inoltre **Guida all'installazione**, p. [Installazione di Server Dr.Web per SO della famiglia UNIX](#)).

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](#)).

6. Effettuare la configurazione iniziale di Server (le impostazioni di Server vengono descritte dettagliatamente in **Manuale dell'amministratore**, in [Capitolo 9: 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. Se la rete antivirus includerà postazioni protette con SO Android, SO Linux, macOS, è necessario caricare i **Prodotti aziendali Dr.Web**.

Nella sezione [Stato del repository](#) eseguire un aggiornamento dei prodotti nel repository di Server. L'aggiornamento può richiedere un lungo tempo. Attendere che il processo di aggiornamento sia completato prima di continuare l'ulteriore configurazione.



Se è installato il Server versione 12, di default gli aggiornamenti dei prodotti del repository **Agent Dr.Web per Android**, **Agent Dr.Web per UNIX** e **Server proxy Dr.Web** vengono scaricati da SAM solo quando questi prodotti vengono richiesti dalle postazioni. Per maggiori informazioni vedi **Manuale dell'amministratore**, p. [Configurazione dettagliata del repository](#).

Se il Server non è connesso a internet, e gli aggiornamenti vengono caricati manualmente da un altro Server o attraverso il Loader di repository, prima di installare o aggiornare i prodotti per cui nelle impostazioni del repository è attivata l'opzione **Aggiorna solo su richiesta**, è necessario prima caricare questi prodotti nel repository manualmente.

- c. Sulla pagina **Amministrazione** → **Server Dr.Web** sono riportate 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 [Conessioni 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 del Server. Inoltre, è disponibile l'autenticazione esterna degli amministratori. Per maggiori informazioni vedi **Manuale dell'amministratore**, [Capitolo 6: 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.
7. Configurare il software antivirus per postazioni (la configurazione dei gruppi e delle postazioni viene descritta dettagliatamente in **Manuale dell'amministratore**, in [Capitolo 7](#) e [Capitolo 8](#)):
- 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.
8. 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 individuali 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.
- Se è necessario installare l'antivirus su più postazioni da un gruppo custom, è possibile utilizzare un pacchetto di installazione di gruppo che viene creato attraverso il Pannello di controllo in un unico esemplare per diverse postazioni di un determinato gruppo.
- Per installare in remoto via rete su una o più postazioni allo stesso tempo (solo per le postazioni SO Windows), utilizzare l'installer di rete. L'installazione viene effettuata attraverso il Pannello di controllo.
- 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, macOS può essere eseguita localmente secondo le regole generali. Inoltre, un prodotto standalone già installato può connettersi al Server sulla base della configurazione corrispondente.



Per il corretto funzionamento di Agent Dr.Web su un sistema operativo Windows server, a partire da Windows Server 2016, è necessario disattivare manualmente Windows Defender utilizzando i criteri di gruppo.

9. 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.
10. 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.

11. È possibile configurare le postazioni e il software antivirus anche dopo l'installazione (la descrizione dettagliata è riportata in **Manuale dell'amministratore**, in [Capitolo 8](#)).



## 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 dell'azienda Doctor Web sull'indirizzo <https://products.drweb.com/register/v4/>, se nessun altro indirizzo è indicato nella scheda di registrazione allegata al prodotto. Andare al sito indicato, compilare il modulo con informazioni sull'acquirente e inserire nel campo indicato il numero di serie di registrazione (si trova nella scheda di registrazione). Un archivio con i file della chiave verrà inviato sull'indirizzo email indicato dall'utente. È inoltre possibile 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 prima 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.



Informazioni dettagliate sui principi e le caratteristiche di concessione delle licenze Dr.Web Enterprise Security Suite sono fornite in **Manuale dell'amministratore**, sottosezioni di [Capitolo 3. 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 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/>.

