Dr.WEB

Enterprise Security Suite

Guida rapida all'installazione della rete antivirus

Dr.Web Enterprise Security Suite
Versione 13.0
Guida rapida all'installazione della rete antivirus
07/03/2024

Doctor Web, Sede centrale in Russia

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

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

Telefono +7 (495) 789-45-87

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

Doctor Web

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

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

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

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

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

Sommario

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 ulteriormente forniti i seguenti manuali:

1. **Manuali 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 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 costantemente aggiornati, la loro ultima versione è ritrovabile sul sito ufficiale dell'azienda Doctor Web all'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
Rete antivirus	Un nuovo termine o un termine accentato nelle descrizioni.
<*indirizzo_IP*>	Campi in cui nomi di funzione vanno sostituiti con valori effettivi.
Salva	Nomi dei pulsanti di schermo, delle finestre, delle voci di menu e di altri elementi dell'interfaccia del programma.
CTRL	Nomi dei tasti della tastiera.
`C:\Windows\`	Nomi di file e directory, frammenti di codice.
Allegato 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:

- 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,
- 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).

Capitolo 2: Dr.Web Enterprise Security Suite

2.1. Sul prodotto

Dr.Web Enterprise Security Suite è progettato per organizzare una protezione antivirus completa unica e affidabile sia della rete interna aziendale, compresi i dispositivi mobili, e sia 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.

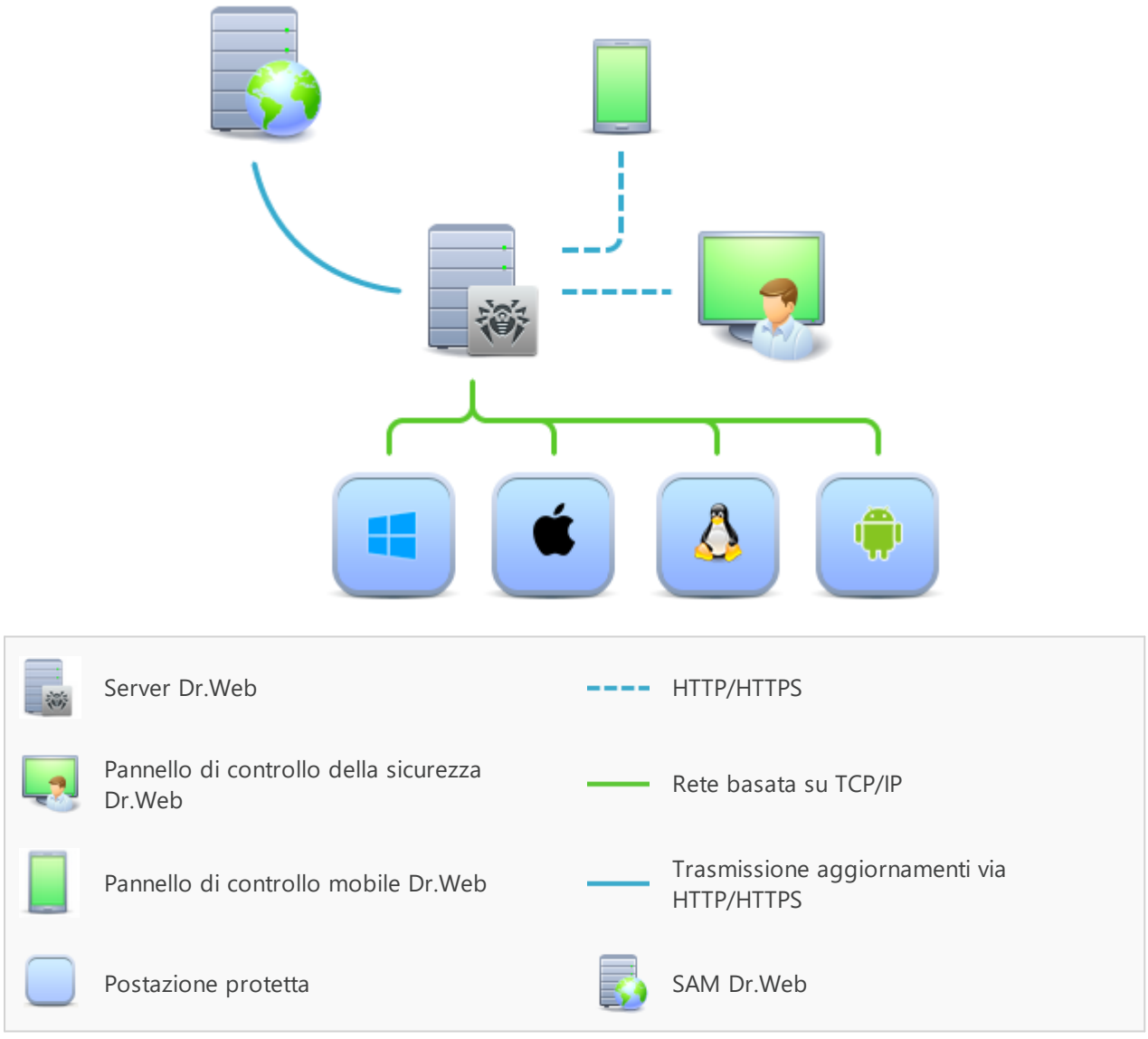

Immagine 1-1. Struttura logica della rete antivirus

La rete antivirus di Dr.Web Enterprise Security Suite ha un'architettura *client-server*. I suoi componenti vengono installati su postazioni. In questo contesto, il termine "postazione" indica un dispositivo protetto nella rete antivirus, su cui è installato un Agent Dr.Web e un pacchetto

antivirus e il quale agisce come client e interagisce con Server Dr.Web. Nel ruolo della postazione possono agire computer, dispositivi virtuali e mobili di utenti e amministratori, nonché computer che svolgono le funzioni di server LAN.

I componenti della rete antivirus si scambiano informazioni attraverso i protocolli di rete TCP/IP. Il software antivirus può essere installato sulle postazioni protette (e successivamente gestito) sia via rete locale che via internet.

Server di protezione centralizzata

Il Server di protezione centralizzata (qui di seguito Server Dr.Web) viene installato su uno dei computer della rete antivirus, l'installazione è possibile su qualsiasi computer e non solo su quello che svolge le funzioni di server LAN. I requisiti principali per tale computer sono riportati in **Guida all'installazione**, p. Requisiti di sistema.

Il carattere multipiattaforma del software server permette di utilizzare come Server Dr.Web un computer con i seguenti sistemi operativi:

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

Il Server Dr.Web conserva i pacchetti antivirus per i diversi sistemi operativi dei computer protetti, gli aggiornamenti dei database dei virus e dei pacchetti antivirus, le chiavi di licenza e le impostazioni dei pacchetti antivirus dei computer protetti. Il Server Dr.Web 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

Un unico database si connette al Server Dr.Web e conserva i dati statistici sugli eventi della rete antivirus, le impostazioni del Server Dr.Web stesso, i parametri delle postazioni protette e dei componenti antivirus installati sulle postazioni protette.

Pannello di controllo di protezione centralizzata

Il Pannello di controllo di protezione centralizzata (qui di seguito Pannello di controllo della sicurezza Dr.Web) viene installato automaticamente insieme al Server Dr.Web e fornisce un'interfaccia web per la gestione remota del Server Dr.Web e della rete antivirus tramite la modifica delle impostazioni del Server Dr.Web, nonché delle impostazioni dei computer protetti, conservate sul Server Dr.Web e sui computer protetti.

Il Pannello di controllo può essere aperto su qualsiasi computer che abbia accesso di rete al Server Dr.Web. L'uso del Pannello di controllo è possibile su quasi tutti i sistemi operativi, le complete funzionalità possono essere utilizzate nei seguenti browser:

- Windows Internet Explorer,
- Microsoft Edge,

- Mozilla Firefox,
- Google Chrome,
- Yandex.Browser.

Un elenco di possibili varianti di utilizzo è riportato in **Guida all'installazione**, p. Requisiti di sistema.

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

Pannello di controllo mobile di protezione centralizzata

Come componente separato per dispositivi mobili con iOS e Android, viene fornito un Pannello di controllo mobile. I requisiti di base per i dispositivi per l'uso di questa applicazione sono riportati in **Guida all'installazione**, p. Requisiti di sistema.

Il Pannello di controllo mobile si connette al Server Dr.Web attraverso il protocollo crittografico e per il funzionamento utilizza le credenziali dell'amministratore della rete antivirus.

Dr.Web Mobile Control Center può essere scaricato dal Pannello di controllo o direttamente negli store di applicazioni App Store e Google Play.

Protezione delle postazioni della rete

Sui computer e dispositivi mobili protetti della rete vengono installati un modulo di gestione (Agent Dr.Web) e un pacchetto antivirus per il sistema operativo corrispondente.

Il carattere multipiattaforma del software permette di proteggere dai virus computer e dispositivi mobili con i seguenti sistemi operativi:

- SO Windows,
- SO della famiglia UNIX,
- macOS,
- SO Android.

Postazioni protette possono essere sia i computer degli utenti che i server LAN. È supportata la protezione antivirus del sistema email Microsoft Outlook.

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

Se il Server Dr.Web 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 opzionalmente essere incluso nella struttura della rete antivirus. L'obiettivo principale del Server proxy è quello di provvedere alla comunicazione tra il Server Dr.Web e le 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 addizionali

NAP Validator

NAP Validator viene fornito come componente addizionale 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 viene fornito come utility addizionale e permette di scaricare i prodotti Dr.Web Enterprise Security Suite dal Sistema di aggiornamento mondiale. Il Loader di repository può essere utilizzato per scaricare gli aggiornamenti dei prodotti Dr.Web Enterprise Security Suite e per collocare gli aggiornamenti su un Server Dr.Web non connesso a internet.

Server di scansione Dr.Web

Server di scansione Dr.Web viene fornito come componente separato, progettato per il funzionamento in ambienti virtuali. Il Server di scansione viene installato su una macchina virtuale separata ed elabora le richieste di scansione antivirus che arrivano dalle altre macchine virtuali.

2.2. Requisiti di sistema

Per l'installazione e il funzionamento di Dr.Web Enterprise Security Suite occorre:

- Che i computer della rete antivirus abbiano accesso al Server Dr.Web, o al Server proxy Dr.Web.
- Per la comunicazione dei componenti antivirus sui computer in uso devono essere aperte le seguenti porte:

Numeri di porte	Protocolli	Connessioni	Scopo
2193	TCP	• in ingresso, in uscita per Server Dr.Web e Server proxy • in uscita per Agent Dr.Web	Per la comunicazione dei componenti antivirus con Server Dr.Web e per le connessioni tra server Tra l'altro, viene utilizzata da Server proxy per stabilire la connessione con i client
	UDP	in ingresso, in uscita	Per il funzionamento di Scanner di rete
139, 445	TCP	• in uscita per Server Dr.Web • in ingresso per Agent Dr.Web	Per l'installazione remota di Agent Dr.Web
	UDP	in ingresso, in uscita	
9080	HTTP	• in ingresso per Server Dr.Web • in uscita per il computer su cui viene aperto Pannello di controllo	Per il funzionamento di Pannello di controllo della sicurezza Dr.Web
9081	HTTPS		
10101	TCP		Per il funzionamento dell'utility di diagnostica remota di Server Dr.Web
80	HTTP	in uscita	Per la ricezione degli aggiornamenti da SAM
443	HTTPS		
18008	UDP	• in ingresso, in uscita per Server di scansione • in ingresso, in uscita per Agent virtuale Dr.Web	Per il rilevamento di qualsiasi Server di scansione disponibile da parte di Agenti virtuali Dr.Web con l'utilizzo del meccanismo Discovery
7090	TCP	• in ingresso per Server di scansione • in uscita per Agent virtuale Dr.Web	Per la comunicazione di Agent virtuali Dr.Web con un Server di scansione specifico

Server Dr.Web

Parametro	Requisiti
Processore	CPU con supporto delle istruzioni SSE2 e frequenza di clock di 1,3 GHz o superiori
Memoria operativa	• requisiti minimi: 1 GB; • requisiti consigliati: da 2 GB

Spazio su disco rigido	• almeno 50 GB per il software Server Dr.Web e spazio aggiuntivo per la memorizzazione dei file temporanei, per esempio, pacchetti di installazione Agent individuali (circa 17 MB ognuno) nella sottodirectory `var\installers-cache` della directory di installazione di Server Dr.Web;
	• fino a 5 GB per il database;
	• indipendentemente dal percorso di installazione di Server Dr.Web, sul disco di sistema in caso di SO Windows o in `/var/tmp` in caso di SO della famiglia UNIX (o in un'altra directory per file temporanei, se è stata ridefinita):
	  ▫ per installare Server Dr.Web sono necessari almeno 4,3 GB per l'avvio dell'installer e l'estrazione dei file temporanei;
	  ▫ per il funzionamento di Server Dr.Web 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

Supporto di ambienti virtuali e cloud	È supportato il funzionamento su sistemi operativi che soddisfano i requisiti sopra elencati in ambienti virtuali e cloud, tra cui: • VMware, • Hyper-V, • Xen, • KVM, • ECP Veil, • Rosa Virtualization RV2.1
Altro	Per l'utilizzo del database Oracle è richiesta la libreria `Linux kernel AIO access library (libaio)`. Le utility di amministrazione, disponibili per il download attraverso il Pannello di controllo, sezione **Amministrazione** → **Utility**, devono essere eseguite su un computer che soddisfi i requisiti di sistema per Server Dr.Web

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

Server Dr.Web non può essere installato sulla stessa postazione di Server proxy Dr.Web.

Per l'installazione su ALT Linux è necessario disattivare SELinux.

Per l'installazione su SO della famiglia UNIX di Server Dr.Web e di Server proxy Dr.Web, è necessario il supporto da parte del sistema operativo del sistema di inizializzazione SysVinit. Se non è presente, è necessario installare il pacchetto corrispondente.

Lista dei sistemi operativi supportati:

Windows	**UNIX**
Per sistemi operativi a 32 bit: • Windows 7, • Windows 8, • Windows 8.1, • Windows 10. *Per sistemi operativi a 64 bit:* • Windows Server 2008 R2, • Windows 7, • Windows Server 2012, • Windows Server 2012 R2, • Windows 8, • Windows 8.1, • Windows 10, • Windows 11, • Windows Server 2016, • Windows Server 2019, • Windows Server 2022	• Linux con libreria glibc 2.13 o versioni successive, • FreeBSD 11.3 e versioni successive. Inoltre, versioni speciali di distribuzioni Linux: ▪ ALT Linux 8, ▪ ALT Linux 9, ▪ Astra Linux Special Edition 1.5 (con patch cumulativa 20201201SE15), ▪ Astra Linux 1.6 (con patch cumulativa 20200722SE16), ▪ Astra Linux 1.7, ▪ Astra Linux Common Edition 2.12 Orel, ▪ ALT 8 SP, ▪ GosLinux IC6, ▪ RED OS 7.3 MUROM. In SO ALT 8 SP e GosLinux IC6 l'uso dei livelli di accesso vincolati non è supportato.

Server proxy Dr.Web

Parametro	**Requisiti**
Processore	CPU con supporto delle istruzioni SSE2 e frequenza di clock di 1,3 GHz o superiori
Memoria operativa	Almeno 1 GB

Parametro	Requisiti
Spazio su disco rigido	Almeno 1 GB
Sistema operativo	La lista dei sistemi operativi corrisponde a quella per Server Dr.Web

Server proxy Dr.Web non può essere installato sulla stessa postazione di Server Dr.Web.

Pannello di controllo della sicurezza Dr.Web

Parametro	Requisiti
Browser	Uno di: • 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, • Yandex.Browser di ultima versione
Risoluzione schermo	Risoluzione dello schermo consigliata 1280×1024
Altro	Se viene utilizzato il web browser Windows Internet Explorer, è necessario tenere conto delle seguenti caratteristiche: • la completa operatività del Pannello di controllo nel web browser Windows Internet Explorer con la modalità attivata Enhanced Security Configuration for Windows Internet Explorer non è garantita; • se Server Dr.Web è installato su un computer il cui nome include il carattere "_" (trattino basso), l'uso di Server Dr.Web attraverso il Pannello di controllo nel browser non sarà possibile. In tale caso è necessario utilizzare un altro web browser; • per il corretto funzionamento del Pannello di controllo, l'indirizzo IP e/o il nome DNS del computer su cui è installato Server Dr.Web devono essere aggiunti ai siti affidabili del web browser in cui viene aperto il Pannello di controllo; • per la corretta apertura del Pannello di controllo tramite il menu Start su SO Windows 8 e SO Windows Server 2012 con interfaccia a piastrelle è necessario configurare le seguenti impostazioni del web browser: Opzioni Internet → Programmi → Apertura di Internet Explorer spuntare il flag Sempre in Internet Explorer in visualizzazione classica; • per il corretto uso del Pannello di controllo attraverso il web browser

	Windows Internet Explorer tramite il protocollo sicuro https è necessario installare tutti gli ultimi aggiornamenti del web browser; • l'uso del Pannello di controllo attraverso il web browser Windows Internet Explorer in modalità di compatibilità non è supportato

Se nell'azienda dell'utente per l'accesso al Pannello di controllo della sicurezza Dr.Web è utilizzato un server proxy inverso (reverse proxy), per il suo utilizzo sono necessarie determinate impostazioni. Esempi di impostazioni possono essere consultati ai seguenti link:

Per Nginx:

https://nginx.org/docs/http/websocket.html

Per Apache:

https://httpd.apache.org/docs/2.4/mod/mod_proxy_wstunnel.html

https://www.serverlab.ca/tutorials/linux/web-servers-linux/how-to-reverse-proxy-websockets-with-apache-2-4/

Pannello di controllo mobile Dr.Web

Sistema operativo	**Requisiti**	
	Versione del sistema operativo	**Dispositivo**
iOS	iOS 9 e versioni successive	• Apple iPhone, • Apple iPad
Android	Android 5.0-12	–

NAP Validator

Parametro	**Requisiti**	
	Per Server Dr.Web	**Per Agent Dr.Web**
Sistema operativo	SO Windows Server 2008	• SO Windows XP SP3, • SO Windows Vista con SP2
Altro	I requisiti di sistema per NAP Validator coincidono con quelli per Agent Dr.Web. I requisiti possono essere diversi a seconda del sistema operativo su cui viene installata la soluzione antivirus	

Server di scansione Dr.Web

Parametro	Requisiti
Processore	Processori con architettura e set di istruzioni Intel/AMD: 32 bit (IA-32, x86) e 64 bit (x86_64, x64, AMD64)
Memoria operativa	Almeno 500 MB di memoria operativa libera (consigliato 1 GB o più)
Spazio su disco rigido	Almeno 1 GB di spazio su disco libero
Hypervisor	• VMware, • Hyper-V, • Xen, • KVM
Sistema operativo	Linux, FreeBSD. La lista dei sistemi operativi supportati è analoga a quella per il pacchetto antivirus per SO UNIX
Connessioni di rete	Presenza delle connessioni di rete: • connessione a Server Dr.Web per l'aggiornamento dei database dei virus e dei database dei filtri incorporati; • connessione per l'elaborazione delle richieste provenienti dagli agent virtuali

Agent Dr.Web e il pacchetto antivirus

I requisiti variano a seconda del sistema operativo su cui viene installata la soluzione antivirus.

Sulle postazioni di una rete antivirus gestita tramite Dr.Web Enterprise Security Suite non devono essere utilizzati altri software antivirus (inclusi software di altre versioni dei programmi antivirus Dr.Web, firewall o programmi di filtraggio di contenuti web).

Windows

Parametro	Requisito
Processore	Con supporto del set di istruzioni i686

Parametro	Requisito
Sistema operativo	Per sistemi operativi a 32 bit: • Windows XP con pacchetto di aggiornamento SP2 o successivi; • Windows Vista con pacchetto di aggiornamento SP2 o successivi; • Windows 7 con pacchetto di aggiornamento SP1 o successivi; • Windows 8; • Windows 8.1; • Windows 10 22H2 o versioni precedenti; • Windows Server 2003 con pacchetto di aggiornamento SP1; • Windows Server 2008 con pacchetto di aggiornamento SP2 o successivi. Per sistemi operativi a 64 bit: • Windows Vista con pacchetto di aggiornamento SP2 o successivi; • Windows 7 con pacchetto di aggiornamento SP1 o successivi; • Windows 8; • Windows 8.1; • Windows 10 22H2 o versioni precedenti; • Windows 11 22H2 o versioni precedenti; • Windows Server 2008 con pacchetto di aggiornamento SP2 o successivi; • Windows Server 2008 R2 con pacchetto di aggiornamento SP1 o successivi; • Windows Server 2012; • Windows Server 2012 R2; • Windows Server 2016; • Windows Server 2019; • Windows Server 2022
Memoria operativa libera	512 MB o più
Risoluzione schermo	Risoluzione minima consigliata 1024×768
Supporto di ambienti virtuali e cloud	È supportato il funzionamento del programma nei seguenti ambienti: • VMware; • Hyper-V; • Xen; • KVM
Altro	Per l'aggiornamento dei database dei virus Dr.Web e dei componenti Dr.Web è richiesta la connessione al server di protezione centralizzata o a internet in Modalità mobile.

Parametro	Requisito
	Per il plugin Dr.Web per Microsoft Outlook è richiesto un client installato Microsoft Outlook di MS Office: • Outlook 2000; • Outlook 2002; • Outlook 2003; • Outlook 2007; • Outlook 2010 con pacchetto di aggiornamento SP2; • Outlook 2013; • Outlook 2016; • Outlook 2019; • Outlook 2021

UNIX

Componente	Requisito
Piattaforma	Sono supportati i processori delle seguenti architetture e set di istruzioni: • Intel/AMD: a 32 bit (*IA-32*, *x86*); a 64 bit (*x86-64*, *x64*, *amd64*); • ARM64; • E2K (*Elbrus*); • IBM POWER (*ppc64el*)
Memoria operativa	Almeno 500 MB di memoria operativa libera (consigliato 1 GB o più)
Spazio su disco rigido	Almeno 2 GB di spazio disco libero sul volume su cui vengono collocate le directory del prodotto installato
Sistema operativo	GNU/Linux (basato su un kernel versione 2.6.37 o successive, che utilizza la libreria `glibc` versione 2.13 o successive, il sistema di inizializzazione `systemd` versione 209 o successive), FreeBSD. L'elenco delle versioni supportate dei sistemi operativi è riportato di seguito. Il sistema operativo deve supportare il meccanismo di autenticazione PAM
Altro	Presenza della connessione di rete: • connessione internet per l'aggiornamento dei database dei virus e dei componenti del prodotto antivirus; • con il funzionamento in modalità di protezione centralizzata, è sufficiente solo la connessione al server utilizzato all'interno della rete locale, l'accesso a internet non è richiesto

Piattaforma	Versioni supportate di GNU/Linux
x86_64	• Astra Linux Special Edition 1.5 (con patch cumulativa 20201201SE15), 1.6 (con patch cumulativa 20200722SE16), 1.7; • Astra Linux Common Edition Orel 2.12; • Debian 9, 10; • Fedora 31, 32; • CentOS 7, 8; • Ubuntu 18.04, 20.04, 22.04; • ALT Workstation 9, 10; • ALT Server 9, 10; • ALT 8 SP; • RED OS 7.2 MUROM, RED OS 7.3 MUROM; • GosLinux IC6; • SUSE Linux Enterprise Server 12 SP3; • Red Hat Enterprise Linux 7, 8
x86	• CentOS 7; • Debian 10; • ALT Workstation 9, 10; • ALT 8 SP;
ARM64	• Ubuntu 18.04; • CentOS 7, 8; • ALT Workstation 9, 10; • ALT Server 9, 10; • ALT 8 SP; • Astra Linux Special Edition (Novorossiysk) 4.7
E2K	• Astra Linux Special Edition (Leningrad) 8.1 (con patch cumulativa 20200429SE81); • ALT 8 SP; • Elbrus-D MCST 1.4; • Software generale Complesso informatico Elbrus-8.32 TVGI.00311-28
ppc64el	• CentOS 8; • Ubuntu 20.04;

In SO ALT 8 SP, Astra Linux Special Edition (Novorossiysk) 4.11 e GosLinux IC6 l'uso dei livelli di accesso vincolati non è supportato.

Per altre distribuzioni Linux corrispondenti ai requisiti descritti la piena compatibilità con l'applicazione non è garantita. Se si verificano problemi di compatibilità con la distribuzione in uso, contattare il supporto tecnico: https://support.drweb.com.

Piattaforma	Versioni supportate di FreeBSD
x86	11, 12, 13
x86_64	11, 12, 13

In caso di SO FreeBSD l'installazione dell'applicazione è possibile solo dal pacchetto universale.

macOS

Parametro	Requisiti
Dispositivo	Mac con sistema operativo macOS
Spazio su disco rigido	2 GB
Sistema operativo	• OS X 10.11 El Capitan; • macOS 10.12 Sierra; • macOS 10.13 High Sierra; • macOS 10.14 Mojave; • macOS 10.15 Catalina; • macOS 11 Big Sur; • macOS 12 Monterey; • macOS 13 Ventura.

SO Android

Parametro	Requisito
Sistema operativo	Android versione 4.4 - 14.0 Android TV (su televisori, lettori multimediali e console per videogiochi)
Processore	x86/x86-64/ARMv7/ARMv8/ARMv9
Memoria operativa libera	Almeno 512 MB
Spazio su disco rigido	Almeno 45 MB (per la conservazione dei dati)
Risoluzione schermo	Risoluzione minima 800×480
Altro	Connessione internet (per l'aggiornamento dei database dei virus).

Parametro	Requisito
	Su dispositivi Android TV la modalità di protezione centralizzata non è disponibile

Dr.Web per Exchange Server

Parametro	Requisito
Memoria operativa libera	512 MB o più
Spazio su disco libero	1 GB o più
Sistema operativo	• Windows Server 2008 x64 con pacchetto di aggiornamento installato SP2; • Windows Server 2008 R2; • Windows Server 2012; • Windows Server 2012 R2; • Windows Server 2016; • Windows Server 2019; • Windows Server 2022
Versione di Microsoft Exchange Server	• Microsoft Exchange Server 2007 x64 con pacchetto di aggiornamento installato SP1; • Microsoft Exchange Server 2010 x64 con pacchetto di aggiornamento installato SP1; • Microsoft Exchange Server 2013 con pacchetto di aggiornamento installato SP1 (inoltre, sono richiesti l'installazione di Cumulative Update 5 o l'avvio dello script Exchange2013-KB2938053-Fixit); • Microsoft Exchange Server 2016 con Cumulative Update 3 installato (o versioni successive); • Microsoft Exchange Server 2019

Dr.Web per Lotus Domino

Parametro	Requisito
Processore	Compatibile con il set di istruzioni i686
Memoria operativa	512 MB o più
Spazio su disco rigido	750 MB o più. I file temporanei creati durante l'installazione richiederanno spazio aggiuntivo
Risoluzione schermo	Risoluzione minima consigliata 1280×1024 con supporto di almeno

Parametro	Requisito
	256 colori
File system	NTFS o FAT32
Sistema operativo	Per sistemi operativi a 32 bit: • Windows Server 2008, • Windows Server 2008 R2. Per sistemi operativi a 64 bit: • Windows Server 2008, • Windows Server 2008 R2, • Windows Server 2012, • Windows Server 2012 R2, • Windows Server 2016, • Windows Server 2019, • Windows Server 2022
Altri software	Software Lotus: • IBM Lotus Domino per Windows versione 8.5 - 9.0.1, • IBM Lotus Notes per Windows versione 7.0.2 - 9.0.1, • IBM Domino per Windows 10.1, • IBM Notes per Windows 10.0, • HCL Domino per Windows 11.0, • HCL Notes per Windows 11.0. Browser per l'utilizzo dell'interfaccia web: • Internet Explorer 8 o versioni successive, • Mozilla Firefox 3 o versioni successive, • Opera 9 o versioni successive

2.3. Contenuto del pacchetto

Il pacchetto Dr.Web Enterprise Security Suite viene fornito a seconda del sistema operativo di Server Dr.Web selezionato:

1. In caso di SO della famiglia UNIX:
   - `drweb-esuite-server-<versione_pacchetto>-<build>-<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-esuite-server-<versione_pacchetto>-<build>-<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 sistema operativo corrispondente;
- dati di sicurezza di Server Dr.Web;
- software di Pannello di controllo della sicurezza Dr.Web;
- software di Agent Dr.Web e pacchetto antivirus per postazioni con SO Windows;
- modulo di aggiornamento di Agent Dr.Web per Windows;
- Antispam Dr.Web per Windows;
- database dei virus, database dei filtri incorporati dei componenti antivirus e di Antispam 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:

- Prodotti per l'installazione su postazioni protette con SO UNIX (inclusi i server LAN), Android, macOS;
- Server di scansione Dr.Web;
- Dr.Web per IBM Lotus Domino;
- Dr.Web per Microsoft Exchange Server;
- Server proxy Dr.Web;
- Installer completo di Agent Dr.Web per Windows;
- Agent Dr.Web per Active Directory;
- Utility per la modifica dello schema Active Directory;
- Utility per la modifica degli attributi degli oggetti Active Directory;

- NAP Validator.

Informazioni dettagliate sulla gestione del repository di Server Dr.Web 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. Progettare uno schema della struttura della rete antivirus, includere in esso tutti i computer, macchine virtuali 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 solo su quello che svolge le funzioni di server LAN. I requisiti principali per tale computer sono riportati in **Guida all'installazione**, 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 Dr.Web.

   Per l'installazione di Server Dr.Web e Agent Dr.Web, è necessario un singolo accesso (fisico o tramite strumenti di gestione e avvio programmi remoto) alle relative postazioni. Tutte le operazioni successive vengono eseguite dalla postazione di lavoro dell'amministratore della rete antivirus (anche possibilmente 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 dovranno essere installati 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 soluzione scatola 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 di prodotti standalone e successivamente connessi al Server Dr.Web. Le impostazioni degli Agent Dr.Web 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 Dr.Web 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 è riportata in **Guida all'installazione**, p. Installazione del Server proxy Dr.Web.
5. Se la rete antivirus consiste di macchine virtuali, si consiglia di utilizzare il Server di scansione. Le procedure di installazione e configurazione sono descritte in **Guida all'installazione,** p. Installazione di Server di scansione Dr.Web.
6. Per configurare il Server Dr.Web e il software antivirus su postazioni, è necessario connettersi al Server Dr.Web 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 Dr.Web. Basta che ci sia una connessione di rete con il computer su cui è installato il Server Dr.Web.

   Il Pannello di controllo è disponibile sull'indirizzo:

   `http://<Indirizzo_Server_Dr.Web>:9080`

   o

   `https://<Indirizzo_Server_Dr.Web>:9081`

   dove come *<Indirizzo_Server_Dr.Web>* indicare l'indirizzo IP, il NetBIOS o il nome a dominio del computer su cui è installato 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 Dr.Web.
     - in caso di SO della famiglia UNIX — la password che è stata creata automaticamente durante l'installazione di Server Dr.Web (v. inoltre **Guida all'installazione**, p. Installazione di Server Dr.Web per SO della famiglia UNIX).

   In caso di una connessione riuscita al Server Dr.Web, 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).

Se è stato installato il Server di scansione, indicarne l'indirizzo nelle impostazioni delle postazioni (per la descrizione dettagliata v. **Manuale dell'amministratore,** p. Connessione delle postazioni a Server di scansione).

7. Effettuare la configurazione iniziale del Server Dr.Web (una descrizione dettagliata delle impostazioni è riportata in **Manuale dell'amministratore**, in Capitolo 10: 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 Dr.Web 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 aggiornare i prodotti nel repository di Server Dr.Web. 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 Dr.Web versione 13, di default gli aggiornamenti dei prodotti del repository **Database di 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 v. **Manuale dell'amministratore**, p. Configurazione dettagliata del repository.

      Se il Server Dr.Web non è connesso a internet, e gli aggiornamenti vengono caricati manualmente da un altro Server Dr.Web 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 Dr.Web. Se è disponibile una nuova versione, aggiornare il Server Dr.Web, come descritto in **Manuale dell'amministratore**, p. Aggiornamento di Server Dr.Web e ripristino da copia di backup.
   d. Se necessario, configurare Configurazione delle 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 del Server Dr.Web. Inoltre, è disponibile l'autenticazione esterna degli amministratori. Per maggiori informazioni v. **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 Dr.Web (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 Dr.Web e della copia di backup.

8. Configurare il software antivirus per postazioni (la configurazione dei gruppi e delle postazioni è 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.
9. Installare il software Agent Dr.Web sulle postazioni.

   Nella sezione File di installazione controllare l'elenco dei file forniti per l'installazione di Agent Dr.Web. Selezionare la variante di installazione più adatta basandosi sul sistema operativo della postazione, sulla possibilità di installazione remota, sulla variante di definizione delle impostazioni di Server Dr.Web nel corso dell'installazione di Agent Dr.Web ecc. Per esempio:

   - Se gli utenti installano l'antivirus in autonomo, utilizzare i pacchetti di installazione individuali che vengono creati attraverso il Pannello di controllo separatamente per ciascuna postazione. Questo tipo di pacchetti può anche essere inviato agli utenti via email direttamente dal Pannello di controllo. Dopo l'installazione le postazioni si connettono al Server Dr.Web 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 l'installazione remota via rete su una postazione o contemporaneamente su più postazioni con SO Windows o OS Linux, 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 Dr.Web.
   - Se nel processo dell'installazione è necessario ridurre il carico sul canale di comunicazione tra Server Dr.Web e postazioni, è possibile utilizzare l'installer completo che installa contemporaneamente Agent Dr.Web e i componenti di protezione.
   - L'installazione su postazioni con SO Android e macOS può essere eseguita localmente secondo le regole generali. Inoltre, un prodotto standalone già installato può connettersi al Server Dr.Web 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.

10. Subito dopo l'installazione sui computer, gli Agent Dr.Web si connettono automaticamente al Server Dr.Web. Le postazioni antivirus vengono autenticate sul Server Dr.Web secondo i 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 della conferma automatica sul Server Dr.Web, le postazioni vengono registrate

automaticamente al momento della prima connessione al Server Dr.Web, e ulteriore conferma non è richiesta.

b. In caso di installazione dagli installer e di impostazione della conferma di accesso manuale, l'amministratore deve confermare manualmente le nuove postazioni in modo da registrarle sul Server Dr.Web. In questo caso, le nuove postazioni non vengono connesse automaticamente, ma vengono messe dal Server Dr.Web nel gruppo nuovi arrivi.

11. Dopo che la postazione si è connessa al Server Dr.Web 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 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 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 riscontrano problemi con l'installazione o il funzionamento dei prodotti della società, prima di contattare per l'assistenza il servizio di supporto tecnico, provare a trovare una soluzione nei seguenti modi:

1. Leggere le ultime versioni delle descrizioni e dei manuali sull'indirizzo https://download.drweb.com/doc/.
2. Leggere la sezione delle domande ricorrenti sull'indirizzo https://support.drweb.com/show_faq/.
3. Visitare i forum della società Doctor Web sull'indirizzo https://forum.drweb.com/.

Se provati questi modi, non si è riusciti a risolvere il problema, è possibile utilizzare uno dei seguenti modi per contattare il servizio di supporto tecnico della società Doctor Web:

1. Compilare il modulo web nella relativa sezione della pagina https://support.drweb.com/.
2. Chiamare il numero +7 (495) 789-45-86 o 8-800-333-7932 (numero gratuito per utenti in Russia).

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