



# Dr.WEB

Enterprise Security Suite

## Guida all'installazione



## © Doctor Web, 2024. 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, SpIDer Mail, SpIDer 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 13.0**

**Guida all'installazione**

**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

<b>Capitolo 1: Introduzione</b>	<b>6</b>
1.1. Scopo del documento	6
1.2. Segni convenzionali e abbreviazioni	7
<b>Capitolo 2: Dr.Web Enterprise Security Suite</b>	<b>9</b>
2.1. Sul prodotto	9
2.2. Requisiti di sistema	19
2.3. Contenuto del pacchetto	31
<b>Capitolo 3: Concessione delle licenze</b>	<b>33</b>
<b>Capitolo 4: Introduzione all'uso</b>	<b>35</b>
4.1. Creazione della rete antivirus	35
4.2. Configurazione delle connessioni di rete	39
4.2.1. Connessioni dirette	40
4.2.2. Servizio di rilevamento di Server Dr.Web	41
4.2.3. Utilizzo del protocollo SRV	42
4.3. Connessione sicura	42
4.3.1. Cifratura e compressione del traffico dati	42
4.3.2. Strumenti per la connessione sicura	49
4.3.3. Connessione dei client al Server Dr.Web	51
4.4. Integrazione di Dr.Web Enterprise Security Suite con Active Directory	53
<b>Capitolo 5: Installazione dei componenti di Dr.Web Enterprise Security Suite</b>	<b>56</b>
5.1. Installazione di Server Dr.Web	56
5.1.1. Installazione di Server Dr.Web per SO Windows	57
5.1.2. Installazione di Server Dr.Web per SO della famiglia UNIX	63
5.2. Installazione di Agent Dr.Web	65
5.2.1. File di installazione	67
5.2.2. Installazione locale di Agent Dr.Web	70
5.2.3. Installazione remota di Agent Dr.Web	81
5.3. Installazione di Server di scansione Dr.Web	99
5.4. Installazione di NAP Validator	101
5.5. Installazione del Server proxy Dr.Web	101
5.5.1. Creazione dell'account del Server proxy Dr.Web	102



5.5.2. Installazione di Server proxy Dr.Web durante l'installazione di Agent Dr.Web per Windows	104
5.5.3. Installazione del Server proxy Dr.Web tramite l'installer	105
5.5.4. Connessione del Server proxy Dr.Web al Server Dr.Web	109
<b>5.6. Codici di errore restituiti nel processo di installazione</b>	<b>112</b>
<b>Capitolo 6: Rimozione dei componenti di Dr.Web Enterprise Security Suite</b>	<b>114</b>
<b>6.1. Rimozione di Server Dr.Web</b>	<b>114</b>
6.1.1. Rimozione di Server Dr.Web per SO Windows	114
6.1.2. Rimozione di Server Dr.Web per SO della famiglia UNIX	114
<b>6.2. Rimozione di Agent Dr.Web</b>	<b>115</b>
6.2.1. Rimozione di Agent Dr.Web per SO Windows	115
6.2.2. Rimozione di Agent Dr.Web con utilizzo del servizio Active Directory	119
<b>6.3. Rimozione di Server di scansione Dr.Web</b>	<b>119</b>
<b>6.4. Rimozione del Server proxy Dr.Web</b>	<b>120</b>
6.4.1. Rimozione del Server proxy Dr.Web in locale	120
6.4.2. Rimozione del Server proxy Dr.Web in remoto	122
<b>Capitolo 7: Aggiornamento dei componenti di Dr.Web Enterprise Security Suite</b>	<b>123</b>
<b>7.1. Aggiornamento di Server Dr.Web per SO Windows</b>	<b>124</b>
<b>7.2. Aggiornamento di Server Dr.Web per SO della famiglia UNIX</b>	<b>128</b>
<b>7.3. Aggiornamento di Agent Dr.Web</b>	<b>132</b>
7.3.1. Aggiornamento di Agent Dr.Web per le postazioni SO Windows	132
7.3.2. Aggiornamento di Agent Dr.Web per le postazioni SO Android	135
7.3.3. Aggiornamento di Agent Dr.Web per le postazioni SO Linux e macOS	136
<b>7.4. Aggiornamento del Server proxy Dr.Web</b>	<b>136</b>
7.4.1. Aggiornamento del Server proxy Dr.Web durante il funzionamento	136
7.4.2. Aggiornamento del Server proxy Dr.Web attraverso l'installer	137
<b>Indice analitico</b>	<b>140</b>



## Capitolo 1: Introduzione

### 1.1. Scopo del documento

La documentazione dell'amministratore della rete antivirus Dr.Web Enterprise Security Suite contiene informazioni che descrivono sia i principi generali che i dettagli di implementazione di una protezione antivirus completa di computer aziendali tramite Dr.Web Enterprise Security Suite.

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

#### 1. Guida all'installazione

Sarà utile per il responsabile aziendale che prende decisioni sull'acquisto e sull'installazione di un sistema di protezione antivirus completa.

Nella guida all'installazione è descritto il processo di creazione di una rete antivirus e di installazione dei suoi componenti principali.

#### 2. Manuale dell'amministratore

È indirizzato *all'amministratore della rete antivirus* — dipendente dell'azienda, che è incaricato della gestione della protezione antivirus dei computer (postazioni e server) di questa rete.

L'amministratore della rete antivirus deve avere privilegi di amministratore di sistema o collaborare con l'amministratore della rete locale, deve essere cosciente in materia di strategia della protezione antivirus e conoscere in dettaglio i pacchetti antivirus Dr.Web per tutti i sistemi operativi utilizzati nella rete.

#### 3. Allegati

Contengono informazioni tecniche che descrivono i parametri di configurazione dei componenti dell'Antivirus, nonché la sintassi e i valori delle istruzioni utilizzate per la gestione degli stessi.



Sono presenti riferimenti incrociati tra i documenti elencati sopra. Se i documenti sono stati scaricati su un computer locale, i riferimenti incrociati saranno operativi solo se i documenti sono situati in una stessa directory e hanno i nomi originali.

Inoltre, sono forniti i seguenti manuali:

#### 1. 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.



## 2. Manuali per la gestione delle postazioni

Contengono informazioni sulla configurazione centralizzata dei componenti del software antivirus delle postazioni, effettuata dall'amministratore della rete antivirus attraverso il Pannello di controllo della sicurezza Dr.Web.

## 3. Manuali dell'utente

Contiene informazioni sulla configurazione della soluzione antivirus Dr.Web direttamente sulle postazioni protette.

## 4. Guida alle Web API

Contiene informazioni tecniche sull'integrazione di Dr.Web Enterprise Security Suite con software di terzi tramite le Web API.

## 5. Guida alla struttura del database del Server Dr.Web

Contiene una descrizione della struttura interna del database di Server Dr.Web e di esempi del suo utilizzo.

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 e abbreviazioni

### 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.
<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.



Simbolo	Commento
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:

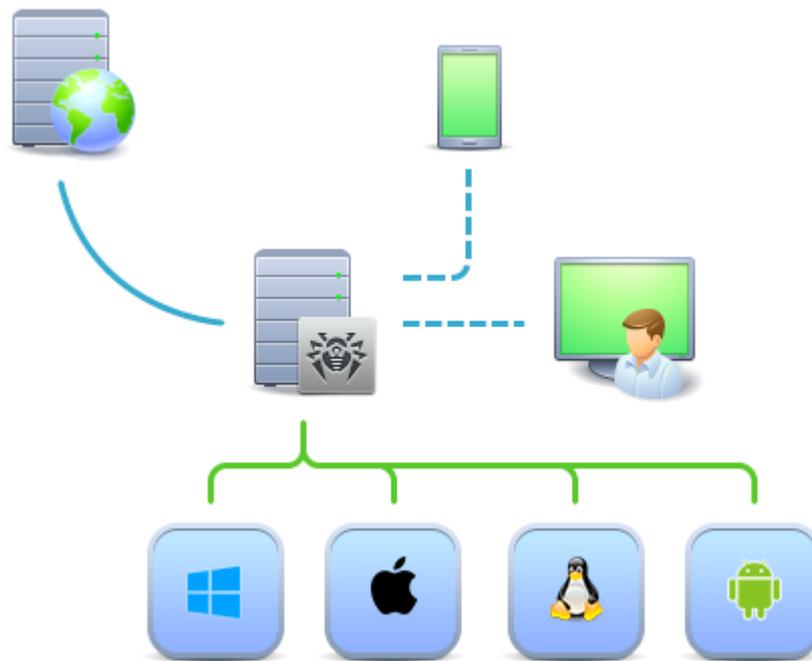
- DB, DBMS — database, database management system,
- SAM Dr.Web — Sistema di aggiornamento mondiale di Dr.Web,
- LAN — rete locale,
- SO — sistema operativo,
- SW, software — programmi per computer,
- ACL — lista di controllo degli accessi (Access Control List),
- CDN — rete di distribuzione di contenuti (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 multiplatforma 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.

È possibile creare una struttura gerarchica di più Server Dr.Web utilizzati dalle postazioni protette della rete antivirus.

Il Server Dr.Web supporta la funzione di backup dei dati critici (database, file di configurazione ecc.).

Il Server Dr.Web registra gli eventi della rete antivirus in un log unico.

## 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.

È possibile utilizzare i seguenti tipi di database:

**Database incorporato.** Viene fornito un database SQLite3 direttamente incorporato nel Server Dr.Web.

**Database esterno.** Vengono forniti i driver incorporati per la connessione dei seguenti database:

- MySQL, Maria DB,
- Oracle,



- PostgreSQL (PostgreSQL Pro, Jatoba ecc.),
- Driver ODBC per la connessione di altri database quali Microsoft SQL Server/Microsoft SQL Server Express.

È possibile utilizzare qualsiasi database che corrisponda alle proprie esigenze, come per esempio: la possibilità di essere utilizzato in una rete antivirus di dimensioni adeguate, le caratteristiche di manutenzione del software del database, le funzionalità di amministrazione fornite dal database stesso, nonché i requisiti e gli standard adottati per l'uso nell'azienda.

## 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](#).

Il Pannello di controllo fornisce le seguenti possibilità:

- Comodità di installazione di Antivirus sulle postazioni protette, in particolare, è possibile: installare in remoto su postazioni eseguendo una scansione della rete preliminare per cercare computer; creare pacchetti con identificatori univoci e con i parametri di connessione al Server di protezione centralizzata per semplificare il processo di installazione di Antivirus da parte dell'amministratore o per consentire agli utenti di installare Antivirus sulle postazioni in modo autonomo (per informazioni dettagliate v. sezione [Installazione di Agent Dr.Web](#)).
- Gestione semplificata delle postazioni della rete antivirus attraverso il metodo di gruppi.
- Possibilità di gestire i pacchetti antivirus delle postazioni in modo centralizzato, in particolare, è possibile: rimuovere sia singoli componenti che l'intero Antivirus su postazioni SO Windows; configurare le impostazioni dei componenti dei pacchetti antivirus; assegnare i permessi per configurare e gestire i pacchetti antivirus dei computer protetti agli utenti di questi computer.



- Gestione centralizzata della scansione antivirus delle postazioni, in particolare è possibile: avviare la scansione antivirus in remoto sia secondo un calendario prestabilito che su una richiesta diretta dell'amministratore dal Pannello di controllo; configurare in modo centralizzato le impostazioni di scansione antivirus che vengono trasmesse alle postazioni per il successivo avvio di una scansione locale con queste impostazioni.
- Ottenimento di informazioni statistiche sullo stato delle postazioni protette, di statistiche di virus, di informazioni sullo stato del software antivirus installato, sullo stato dei componenti antivirus in esecuzione, nonché di un elenco degli hardware e dei software della postazione protetta.
- Sistema flessibile di amministrazione del Server di protezione centralizzata e della rete antivirus grazie alla possibilità di delimitare i permessi di diversi amministratori, nonché la possibilità di connettere amministratori attraverso sistemi di autenticazione esterni, come Active Directory, LDAP, RADIUS, PAM.
- Gestione delle licenze di protezione antivirus delle postazioni con un sistema ramificato di assegnazione delle licenze a postazioni e gruppi di postazioni, nonché di trasferimento delle licenze tra diversi Server di protezione centralizzata in caso di una configurazione di rete antivirus con diversi server.
- Ampio set di impostazioni per la configurazione del Server Dr.Web dei suoi singoli componenti, tra l'altro, è possibile: impostare un calendario per la manutenzione; connettere procedure personalizzate; configurare in modo flessibile l'aggiornamento da SAM di tutti i componenti della rete antivirus e la successiva distribuzione degli aggiornamenti alle postazioni; configurare i sistemi di avviso dell'amministratore sugli eventi della rete antivirus con vari metodi di consegna dei messaggi; configurare le relazioni tra i server per una configurazione di rete antivirus con diversi server.



Le informazioni dettagliate sull'utilizzo delle funzioni descritte sopra sono riportate nel **Manuale dell'amministratore**.

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. Il Pannello di controllo mobile supporta le funzionalità di base del Pannello di controllo:

1. Gestione dei componenti antivirus installati su postazioni della rete antivirus:



- avvio di una scansione rapida o completa sulle postazioni selezionate o su tutte le postazioni dei gruppi selezionati;
  - configurazione della reazione di Scanner Dr.Web al rilevamento di oggetti malevoli;
  - visualizzazione e gestione dei file dalla Quarantena sulla postazione selezionata o su tutte le postazioni del gruppo selezionato.
2. Visualizzazione delle statistiche sullo stato della rete antivirus:
    - numero di postazioni registrate sul Server Dr.Web e il loro stato corrente (online/offline);
    - statistiche di infezioni su postazioni protette.
  3. Gestione delle postazioni e dei gruppi:
    - visualizzazione delle impostazioni;
    - visualizzazione e gestione della lista dei componenti del pacchetto antivirus;
    - rimozione di postazioni e gruppi;
    - invio dei messaggi con qualsiasi contenuto sulle postazioni;
    - riavvio delle postazioni SO Windows;
    - aggiunta di postazioni e gruppi alla lista dei preferiti per un rapido accesso.
  4. Visualizzazione e gestione dei messaggi sugli eventi importanti nella rete antivirus tramite le notifiche interattive Push:
    - visualizzazione di tutte le notifiche sul Server Dr.Web;
    - impostazione delle reazioni agli eventi delle notifiche;
    - ricerca delle notifiche secondo i criteri di filtro impostati;
    - eliminazione delle notifiche;
    - esclusione della perdita di notifiche a seguito della cancellazione automatica.
  5. Gestione delle nuove postazioni in attesa di essere collegate al Server Dr.Web:
    - conferma dell'accesso;
    - rigetto delle postazioni.
  6. Gestione delle postazioni su cui un aggiornamento del software antivirus non è riuscito:
    - visualizzazione delle postazioni fallite;
    - aggiornamento dei componenti sulle postazioni fallite.
  7. Gestione del repository di Server Dr.Web:
    - visualizzazione dello stato dei prodotti nel repository;
    - avvio dell'aggiornamento di repository da Sistema di aggiornamento mondiale Dr.Web.
  8. Ricerca di postazioni e gruppi nella rete antivirus per nome, indirizzo o ID.

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 multiplatforma 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.

A seconda del sistema operativo della postazione, vengono fornite le funzioni di protezione corrispondenti, riportate di seguito.

### Postazioni SO Windows

#### *Scansione antivirus*

Scansione del computer on demand e secondo il calendario. Inoltre, è supportata la possibilità di avviare la scansione antivirus delle postazioni su remoto dal Pannello di controllo, compresa la verifica della presenza di rootkit.

#### *Monitoraggio di file*

Scansione continua del file system in tempo reale. Controlla tutti i processi che vengono avviati e file che vengono creati su dischi rigidi e vengono aperti su supporti rimovibili.

#### *Monitoraggio di email*

Scansione di ogni email in entrata e in uscita in client di posta.

Inoltre, è possibile utilizzare il filtro antispam (a condizione che la licenza permetta l'utilizzo di tale funzionalità).

#### *Monitoraggio del traffico web*

Controllo di tutte le connessioni a siti attraverso il protocollo HTTP. Neutralizzazione delle minacce nel traffico HTTP (per esempio, in file inviati o ricevuti), nonché limitazione dell'accesso a risorse sospette o non corrette.



### *Office control*

Controllo dell'accesso a risorse locali e di rete, in particolare, controllo dell'accesso a siti web. Permette di controllare l'integrità dei file importanti da modifiche accidentali o infezioni da virus e vieta ai dipendenti l'accesso alle informazioni indesiderate.

### *Firewall*

Protezione dei computer dall'accesso non autorizzato dall'esterno e prevenzione della fuga di informazioni importanti attraverso internet. Controllo della connessione e del trasferimento di dati attraverso internet e blocco delle connessioni sospette a livello di pacchetti e applicazioni.

### *Quarantena*

Isolamento di oggetti dannosi e sospetti in una directory speciale.

### *Auto-protezione*

Protezione dei file e delle directory di Dr.Web Enterprise Security Suite da rimozione o modifica non autorizzata o accidentale da parte dell'utente, nonché da parte dei programmi malevoli. Con l'auto-protezione attivata l'accesso ai file e alle directory di Dr.Web Enterprise Security Suite è consentito solo ai processi Dr.Web.

### *Protezione preventiva*

Prevenzione di potenziali minacce alla sicurezza. Controllo dell'accesso agli oggetti critici del sistema operativo, controllo del caricamento driver, dell'esecuzione automatica programmi e del funzionamento dei servizi di sistema, nonché monitoraggio dei processi in esecuzione e blocco processi se rilevata attività di virus.

### *Controllo delle applicazioni*

Monitora l'attività di tutti i processi sulle postazioni. Permette all'amministratore della rete antivirus di consentire o vietare l'avvio di determinate applicazioni sulle postazioni protette.

## **Postazioni con SO della famiglia UNIX**

### *Scansione antivirus*

Motore di scansione. Esegue la scansione antivirus dei dati (contenuti nei file, record di avvio delle unità disco, altri dati ricevuti da altri componenti di Dr.Web per UNIX). Organizza una coda di scansione. Esegue la cura delle minacce per le quali tale azione è applicabile.

### *Scansione antivirus, gestione della quarantena*

Componente per la verifica degli oggetti del file system e la gestione della quarantena. Accetta task di scansione file da altri componenti di Dr.Web per UNIX. Monitora le directory del file system in base al task, trasferisce i file al motore di scansione per la verifica. Esegue la rimozione dei file infetti, il loro spostamento in quarantena e il



ripristino dalla quarantena, gestisce le directory di quarantena. Organizza e mantiene aggiornata una cache che memorizza informazioni sui file precedentemente scansionati e un registro delle minacce rilevate.

Viene utilizzato da tutti i componenti che controllano oggetti del file system, come per esempio SpIDer Guard (per Linux, SMB, NSS).

#### *Controllo del traffico web*

Un server ICAP che analizza le richieste e il traffico che passa attraverso i proxy HTTP. Impedisce il trasferimento dei file infetti e l'accesso ai nodi di rete inclusi nelle categorie indesiderate di risorse web e nelle blacklist create dall'amministratore di sistema.

#### *Monitoraggio di file per i sistemi GNU/Linux*

Monitor del file system Linux. Funziona in background e tiene traccia delle operazioni sui file (come per esempio la creazione, l'apertura, la chiusura e l'avvio di un file) nei file system GNU/Linux. Invia al componente della scansione file le richieste per la verifica del contenuto di file nuovi e modificati, nonché di file eseguibili al momento dell'avvio di programmi.

#### *Monitoraggio di file per le directory Samba*

Monitora le directory condivise di Samba. Funziona in background e monitora le operazioni del file system (come per esempio la creazione, l'apertura e la chiusura di un file, nonché le operazioni di lettura e scrittura) nelle directory riservate per l'archiviazione dei file del server SMB Samba. Invia il contenuto di file nuovi e modificati al componente della scansione file per la verifica.

#### *Monitoraggio di file NSS*

Monitor dei volumi NSS (Novell Storage Services). Funziona in background e monitora le operazioni del file system (come per esempio la creazione, l'apertura e la chiusura di un file, nonché le operazioni di scrittura) sui volumi NSS montati in un punto specificato del file system. Invia il contenuto di file nuovi e modificati per la verifica al componente della scansione file.

#### *Controllo delle connessioni di rete*

Componente del controllo del traffico di rete e delle URL. È progettato per eseguire il controllo della presenza di minacce nei dati scaricati sul nodo locale dalla rete e trasferiti da esso alla rete esterna e impedire le connessioni ai nodi di rete inclusi nelle categorie indesiderate di risorse web e nelle blacklist create dall'amministratore di sistema.

#### *Monitoraggio di email*

Componente del controllo dei messaggi email. Analizza i messaggi dei protocolli di posta, scompone i messaggi di posta elettronica e li prepara per il controllo della presenza di minacce. Può funzionare in due modalità:

1. Filtro per server di posta (Sendmail, Postfix, ecc.), che è connesso tramite l'interfaccia Milter, Spamd o Rspamd.



2. Proxy trasparente dei protocolli di posta (SMTP, POP3, IMAP). In questa modalità utilizza SplDer Gate.

## **Postazioni macOS**

### *Scansione antivirus*

Scansione del computer on demand e secondo il calendario. Inoltre, è supportata la possibilità di avviare la scansione antivirus delle postazioni su remoto dal Pannello di controllo.

### *Monitoraggio di file*

Scansione continua del file system in tempo reale. Controlla tutti i processi che vengono avviati e file che vengono creati su dischi rigidi e vengono aperti su supporti rimovibili.

### *Monitoraggio del traffico web*

Controllo di ogni connessione a siti web via HTTP. Neutralizzazione delle minacce nel traffico HTTP (per esempio in file inviati o ricevuti), nonché blocco dell'accesso a siti non attendibili o non corretti.

### *Quarantena*

Isolamento di oggetti dannosi e sospetti in una directory speciale.

## **Dispositivi mobili SO Android**

### *Scansione antivirus*

Scansione del dispositivo mobile on demand e secondo il calendario. Inoltre, è supportata la possibilità di avviare la scansione antivirus delle postazioni su remoto dal Pannello di controllo.

### *Monitoraggio di file*

Scansione continua del file system in tempo reale. Scansione di ogni file al momento quando viene salvato nella memoria del dispositivo mobile.

### *Filtro chiamate ed SMS*

Il filtraggio di messaggi SMS e chiamate consente di bloccare i messaggi e le chiamate indesiderati, per esempio, invii pubblicitari, nonché le chiamate e i messaggi provenienti da numeri sconosciuti.

### *Antifurto*

Rilevamento della posizione o blocco istantaneo delle funzioni del dispositivo mobile in caso di smarrimento o furto.



### *Limitazione dell'accesso a risorse Internet*

Il filtraggio URL consente di proteggere l'utente del dispositivo mobile dalle risorse di Internet indesiderate.

### *Firewall*

Protezione del dispositivo mobile dall'accesso non autorizzato dall'esterno e prevenzione della fuga di informazioni importanti attraverso la rete. Controllo della connessione e del trasferimento di dati attraverso internet e blocco delle connessioni sospette a livello di pacchetti e applicazioni.

### *Aiuto nella risoluzione di problemi*

Diagnostica ed analisi della sicurezza del dispositivo mobile ed eliminazione di problemi e vulnerabilità rilevati.

### *Controllo dell'esecuzione di applicazioni*

Divieto dell'esecuzione sul dispositivo mobile delle applicazioni non incluse nella lista di quelle consentite dall'amministratore.

## **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.

Il Server proxy consente di utilizzare qualsiasi computer che fa parte della rete antivirus per i seguenti scopi:

- Come centro di ritrasmissione degli aggiornamenti per ridurre il carico di rete sul Server Dr.Web e sulla connessione tra il Server Dr.Web e il Server proxy, nonché per ridurre i tempi di ricezione degli aggiornamenti da parte delle postazioni protette attraverso l'uso della funzione di memorizzazione nella cache.
- Come centro di inoltro degli eventi di virus dalle postazioni protette al Server Dr.Web, il che anche riduce il carico di rete e consente di provvedere al lavoro, per esempio, nei casi in cui un gruppo di postazioni si trova in un segmento di rete isolato dal segmento in cui si trova il Server Dr.Web.

### **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 componente aggiuntivo e permette di utilizzare la tecnologia Microsoft Network Access Protection (NAP) per controllare l'operatività del software delle postazioni protette. La sicurezza risultante viene raggiunta tramite la soddisfazione dei requisiti per l'operatività delle postazioni della rete.

### Loader di repository

Il Loader di repository Dr.Web viene fornito come utility aggiuntiva 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	<ul style="list-style-type: none"><li>• in ingresso, in uscita per Server Dr.Web e Server proxy</li><li>• in uscita per Agent Dr.Web</li></ul>	Per la comunicazione dei componenti antivirus con Server Dr.Web e per le connessioni tra server
	UDP	in ingresso, in uscita	Tra l'altro, viene utilizzata da Server proxy per stabilire la



Numeri di porte	Protocolli	Connessioni	Scopo
			connessione con i client
			Per il funzionamento di Scanner di rete
139, 445	TCP	<ul style="list-style-type: none"><li>• in uscita per Server Dr.Web</li><li>• in ingresso per Agent Dr.Web</li></ul>	Per l'installazione remota di Agent Dr.Web
	UDP	in ingresso, in uscita	
9080	HTTP	<ul style="list-style-type: none"><li>• in ingresso per Server Dr.Web</li><li>• in uscita per il computer su cui viene aperto Pannello di controllo</li></ul>	Per il funzionamento di Pannello di controllo della sicurezza Dr.Web
9081	HTTPS		Per il funzionamento dell'utility di diagnostica remota di Server Dr.Web
10101	TCP		
80	HTTP	in uscita	Per la ricezione degli aggiornamenti da SAM
443	HTTPS		
18008	UDP	<ul style="list-style-type: none"><li>• in ingresso, in uscita per Server di scansione</li><li>• in ingresso, in uscita per Agent virtuale Dr.Web</li></ul>	Per il rilevamento di qualsiasi Server di scansione disponibile da parte di Agenti virtuali Dr.Web con l'utilizzo del meccanismo Discovery
7090	TCP	<ul style="list-style-type: none"><li>• in ingresso per Server di scansione</li><li>• in uscita per Agent virtuale Dr.Web</li></ul>	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	<ul style="list-style-type: none"><li>• requisiti minimi: 1 GB;</li><li>• requisiti consigliati: da 2 GB</li></ul>
Spazio su disco rigido	<ul style="list-style-type: none"><li>• 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 <code>var\installers-cache</code> della directory di installazione di Server Dr.Web;</li></ul>



Parametro	Requisiti
	<ul style="list-style-type: none"><li>• fino a 5 GB per il database;</li><li>• indipendentemente dal percorso di installazione di Server Dr.Web, sul disco di sistema in caso di SO Windows o in <code>/var/tmp</code> in caso di SO della famiglia UNIX (o in un'altra directory per file temporanei, se è stata ridefinita):<ul style="list-style-type: none"><li>▫ per installare Server Dr.Web sono necessari almeno 4,3 GB per l'avvio dell'installer e l'estrazione dei file temporanei;</li><li>▫ 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</li></ul></li></ul>
Supporto di ambienti virtuali e cloud	<p>È supportato il funzionamento su sistemi operativi che soddisfano i requisiti sopra elencati in 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><li>• ECP Veil,</li><li>• Rosa Virtualization RV2.1</li></ul>
Altro	<p>Per l'utilizzo del database Oracle è richiesta la libreria <code>Linux kernel AIO access library (libaio)</code>.</p> <p>Le utility di amministrazione, disponibili per il download attraverso il Pannello di controllo, sezione <b>Amministrazione</b> → <b>Utility</b>, devono essere eseguite su un computer che soddisfi i requisiti di sistema per Server Dr.Web</p>



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
<p><i>Per sistemi operativi a 32 bit:</i></p> <ul style="list-style-type: none"><li>• Windows 7,</li><li>• Windows 8,</li></ul>	<ul style="list-style-type: none"><li>• Linux con libreria glibc 2.13 o versioni successive,</li><li>• FreeBSD 11.3 e versioni successive.</li></ul> <p>Inoltre, versioni speciali di distribuzioni Linux:</p>



Windows	UNIX
<ul style="list-style-type: none"><li>• Windows 8.1,</li><li>• Windows 10.</li></ul> <p><i>Per sistemi operativi a 64 bit:</i></p> <ul style="list-style-type: none"><li>• Windows Server 2008 R2,</li><li>• Windows 7,</li><li>• Windows Server 2012,</li><li>• Windows Server 2012 R2,</li><li>• Windows 8,</li><li>• Windows 8.1,</li><li>• Windows 10,</li><li>• Windows 11,</li><li>• Windows Server 2016,</li><li>• Windows Server 2019,</li><li>• Windows Server 2022</li></ul>	<ul style="list-style-type: none"><li>▪ ALT Linux 8,</li><li>▪ ALT Linux 9,</li><li>▪ Astra Linux Special Edition 1.5 (con patch cumulativa 20201201SE15),</li><li>▪ Astra Linux 1.6 (con patch cumulativa 20200722SE16),</li><li>▪ Astra Linux 1.7,</li><li>▪ Astra Linux Common Edition 2.12 Orel,</li><li>▪ ALT 8 SP,</li><li>▪ GosLinux IC6,</li><li>▪ RED OS 7.3 MUROM.</li></ul> <p>In SO ALT 8 SP e GosLinux IC6 l'uso dei livelli di accesso vincolati non è supportato.</p>

## 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
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: <ul style="list-style-type: none"><li>• Internet Explorer 11,</li></ul>



	<ul style="list-style-type: none"><li>• Microsoft Edge 0.10 o versioni successive,</li><li>• Mozilla Firefox 44 o versioni successive,</li><li>• Google Chrome 49 o versioni successive,</li><li>• Opera di ultima versione,</li><li>• Safari di ultima versione,</li><li>• Yandex.Browser di ultima versione</li></ul>
Risoluzione schermo	Risoluzione dello schermo consigliata 1280×1024
Altro	<p>Se viene utilizzato il web browser Windows Internet Explorer, è necessario tenere conto delle seguenti caratteristiche:</p> <ul style="list-style-type: none"><li>• 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;</li><li>• 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;</li><li>• 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;</li><li>• 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;</li><li>• 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;</li><li>• l'uso del Pannello di controllo attraverso il web browser Windows Internet Explorer in modalità di compatibilità non è supportato</li></ul>



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://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	<ul style="list-style-type: none"><li>• Apple iPhone,</li><li>• Apple iPad</li></ul>
Android	Android 5.0-12	–

## NAP Validator

Parametro	Requisiti	
	Per Server Dr.Web	Per Agent Dr.Web
Sistema operativo	SO Windows Server 2008	<ul style="list-style-type: none"><li>• SO Windows XP SP3,</li><li>• SO Windows Vista con SP2</li></ul>
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	<ul style="list-style-type: none"><li>• VMware,</li><li>• Hyper-V,</li><li>• Xen,</li><li>• KVM</li></ul>
Sistema operativo	Linux, FreeBSD.  La lista dei sistemi operativi supportati è analoga a quella per il pacchetto antivirus per SO UNIX



Parametro	Requisiti
Connessioni di rete	Presenza delle connessioni di rete: <ul style="list-style-type: none"><li>• connessione a Server Dr.Web per l'aggiornamento dei database dei virus e dei database dei filtri incorporati;</li><li>• connessione per l'elaborazione delle richieste provenienti dagli agent virtuali</li></ul>

## 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
Sistema operativo	Per sistemi operativi a 32 bit: <ul style="list-style-type: none"><li>• Windows XP con pacchetto di aggiornamento SP2 o successivi;</li><li>• Windows Vista con pacchetto di aggiornamento SP2 o successivi;</li><li>• Windows 7 con pacchetto di aggiornamento SP1 o successivi;</li><li>• Windows 8;</li><li>• Windows 8.1;</li><li>• Windows 10 22H2 o versioni precedenti;</li><li>• Windows Server 2003 con pacchetto di aggiornamento SP1;</li><li>• Windows Server 2008 con pacchetto di aggiornamento SP2 o successivi.</li></ul> Per sistemi operativi a 64 bit: <ul style="list-style-type: none"><li>• Windows Vista con pacchetto di aggiornamento SP2 o successivi;</li><li>• Windows 7 con pacchetto di aggiornamento SP1 o successivi;</li><li>• Windows 8;</li><li>• Windows 8.1;</li><li>• Windows 10 22H2 o versioni precedenti;</li><li>• Windows 11 22H2 o versioni precedenti;</li><li>• Windows Server 2008 con pacchetto di aggiornamento SP2 o successivi;</li></ul>



Parametro	Requisito
	<ul style="list-style-type: none"><li>• Windows Server 2008 R2 con pacchetto di aggiornamento SP1 o successivi;</li><li>• Windows Server 2012;</li><li>• Windows Server 2012 R2;</li><li>• Windows Server 2016;</li><li>• Windows Server 2019;</li><li>• Windows Server 2022</li></ul>
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: <ul style="list-style-type: none"><li>• VMware;</li><li>• Hyper-V;</li><li>• Xen;</li><li>• KVM</li></ul>
Altro	<p>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.</p> <p>Per il plugin Dr.Web per Microsoft Outlook è richiesto un client installato Microsoft Outlook di MS Office:</p> <ul style="list-style-type: none"><li>• Outlook 2000;</li><li>• Outlook 2002;</li><li>• Outlook 2003;</li><li>• Outlook 2007;</li><li>• Outlook 2010 con pacchetto di aggiornamento SP2;</li><li>• Outlook 2013;</li><li>• Outlook 2016;</li><li>• Outlook 2019;</li><li>• Outlook 2021</li></ul>

## UNIX

Componente	Requisito
Piattaforma	<p>Sono supportati i processori delle seguenti architetture e set di istruzioni:</p> <ul style="list-style-type: none"><li>• Intel/AMD: a 32 bit (IA-32, x86); a 64 bit (x86-64, x64, amd64);</li><li>• ARM64;</li><li>• E2K (Elbrus);</li></ul>



Componente	Requisito
	<ul style="list-style-type: none"><li>• IBM POWER (<i>ppc64el</i>)</li></ul>
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	<p>GNU/Linux (basato su un kernel versione 2.6.37 o successive, che utilizza la libreria <code>glibc</code> versione 2.13 o successive, il sistema di inizializzazione <code>systemd</code> versione 209 o successive), FreeBSD. L'elenco delle versioni supportate dei sistemi operativi è riportato di seguito.</p> <p>Il sistema operativo deve supportare il meccanismo di autenticazione PAM</p>
Altro	<p>Presenza della connessione di rete:</p> <ul style="list-style-type: none"><li>• connessione internet per l'aggiornamento dei database dei virus e dei componenti del prodotto antivirus;</li><li>• 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</li></ul>

Piattaforma	Versioni supportate di GNU/Linux
x86_64	<ul style="list-style-type: none"><li>• Astra Linux Special Edition 1.5 (con patch cumulativa 20201201SE15), 1.6 (con patch cumulativa 20200722SE16), 1.7;</li><li>• Astra Linux Common Edition Orel 2.12;</li><li>• Debian 9, 10;</li><li>• Fedora 31, 32;</li><li>• CentOS 7, 8;</li><li>• Ubuntu 18.04, 20.04, 22.04;</li><li>• ALT Workstation 9, 10;</li><li>• ALT Server 9, 10;</li><li>• ALT 8 SP;</li><li>• RED OS 7.2 MUROM, RED OS 7.3 MUROM;</li><li>• GosLinux IC6;</li><li>• SUSE Linux Enterprise Server 12 SP3;</li><li>• Red Hat Enterprise Linux 7, 8</li></ul>
x86	<ul style="list-style-type: none"><li>• CentOS 7;</li><li>• Debian 10;</li><li>• ALT Workstation 9, 10;</li><li>• ALT 8 SP;</li></ul>
ARM64	<ul style="list-style-type: none"><li>• Ubuntu 18.04;</li><li>• CentOS 7, 8;</li></ul>



Piattaforma	Versioni supportate di GNU/Linux
	<ul style="list-style-type: none"><li>• ALT Workstation 9, 10;</li><li>• ALT Server 9, 10;</li><li>• ALT 8 SP;</li><li>• Astra Linux Special Edition (Novorossiysk) 4.7</li></ul>
E2K	<ul style="list-style-type: none"><li>• Astra Linux Special Edition (Leningrad) 8.1 (con patch cumulativa 20200429SE81);</li><li>• ALT 8 SP;</li><li>• Elbrus-D MCST 1.4;</li><li>• Software generale Complesso informatico Elbrus-8.32 TVGI.00311-28</li></ul>
ppc64el	<ul style="list-style-type: none"><li>• CentOS 8;</li><li>• Ubuntu 20.04;</li></ul>



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	<ul style="list-style-type: none"><li>• OS X 10.11 El Capitan;</li><li>• macOS 10.12 Sierra;</li><li>• macOS 10.13 High Sierra;</li><li>• macOS 10.14 Mojave;</li></ul>



Parametro	Requisiti
	<ul style="list-style-type: none"><li>• macOS 10.15 Catalina;</li><li>• macOS 11 Big Sur;</li><li>• macOS 12 Monterey;</li><li>• macOS 13 Ventura.</li></ul>

## 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).  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	<ul style="list-style-type: none"><li>• Windows Server 2008 x64 con pacchetto di aggiornamento installato SP2;</li><li>• Windows Server 2008 R2;</li><li>• Windows Server 2012;</li><li>• Windows Server 2012 R2;</li><li>• Windows Server 2016;</li><li>• Windows Server 2019;</li><li>• Windows Server 2022</li></ul>



Parametro	Requisito
Versione di Microsoft Exchange Server	<ul style="list-style-type: none"><li>• Microsoft Exchange Server 2007 x64 con pacchetto di aggiornamento installato SP1;</li><li>• Microsoft Exchange Server 2010 x64 con pacchetto di aggiornamento installato SP1;</li><li>• Microsoft Exchange Server 2013 con pacchetto di aggiornamento installato SP1 (inoltre, sono richiesti l'installazione di Cumulative Update 5 o l'avvio dello script <a href="#">Exchange2013-KB2938053-Fixit</a>);</li><li>• Microsoft Exchange Server 2016 con Cumulative Update 3 installato (o versioni successive);</li><li>• Microsoft Exchange Server 2019</li></ul>

## 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 256 colori
File system	NTFS o FAT32
Sistema operativo	Per sistemi operativi a 32 bit: <ul style="list-style-type: none"><li>• Windows Server 2008,</li><li>• Windows Server 2008 R2.</li></ul> Per sistemi operativi a 64 bit: <ul style="list-style-type: none"><li>• Windows Server 2008,</li><li>• Windows Server 2008 R2,</li><li>• Windows Server 2012,</li><li>• Windows Server 2012 R2,</li><li>• Windows Server 2016,</li><li>• Windows Server 2019,</li><li>• Windows Server 2022</li></ul>
Altri software	Software Lotus: <ul style="list-style-type: none"><li>• IBM Lotus Domino per Windows versione 8.5 - 9.0.1,</li><li>• IBM Lotus Notes per Windows versione 7.0.2 - 9.0.1,</li></ul>



Parametro	Requisito
	<ul style="list-style-type: none"><li>• IBM Domino per Windows 10.1,</li><li>• IBM Notes per Windows 10.0,</li><li>• HCL Domino per Windows 11.0,</li><li>• HCL Notes per Windows 11.0.</li></ul> Browser per l'utilizzo dell'interfaccia web: <ul style="list-style-type: none"><li>• Internet Explorer 8 o versioni successive,</li><li>• Mozilla Firefox 3 o versioni successive,</li><li>• Opera 9 o versioni successive</li></ul>

## 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-reloader-<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-reloader-windows-<numero_di_bit>.exe`  
Versione console di Loader di repository Dr.Web.
- `drweb-reloader-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: 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 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](#).



## Capitolo 4: Introduzione all'uso

### 4.1. 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 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 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 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 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](#)).

## 4.2. Configurazione delle connessioni di rete

### Informazioni generali

Al Server Dr.Web si connettono i seguenti client:

- Agent Dr.Web.
- Installer di Agent Dr.Web.
- Server Dr.Web adiacenti.
- Server proxy Dr.Web.

Una connessione viene sempre stabilita da parte del client.

Sono possibili i seguenti modi di connessione dei client al Server Dr.Web:

1. Tramite le [connessioni dirette](#).

Questo approccio ha tanti vantaggi, ma non è sempre preferibile (ci sono perfino delle situazioni quando non si deve utilizzarlo).

2. Tramite il [Servizio di rilevamento di Server Dr.Web](#).

Di default (se non diversamente impostato), i client utilizzano questo Servizio.

Questo approccio va utilizzato se è necessaria la riconfigurazione di tutto il sistema, in particolare, se si deve trasferire il Server Dr.Web su altro computer o cambiare l'indirizzo IP del computer su cui è installato il Server Dr.Web.

3. Tramite il [protocollo SRV](#).

Questo approccio permette di cercare il Server Dr.Web per nome del computer e/o del servizio Server Dr.Web sulla base dei record SRV su server DNS.



Se nelle impostazioni della rete antivirus Dr.Web Enterprise Security Suite è indicato l'utilizzo di connessioni dirette, il Servizio di rilevamento di Server Dr.Web può essere disattivato. Per farlo, nella descrizione dei trasporti (**Amministrazione** → **Configurazione del Server Dr.Web** → scheda **Rete** → scheda **Trasporto**) si deve lasciare vuoto il campo **Gruppo multicast**.

## Configurazione del firewall

Per l'interazione dei componenti della rete antivirus è necessario che tutte le porte ed interfacce utilizzate siano aperte su tutti i computer che fanno parte della rete antivirus.

Durante l'installazione di Server Dr.Web l'installer aggiunge automaticamente le porte e le interfacce di Server Dr.Web alle eccezioni del firewall SO Windows.

Se sul computer viene utilizzato un firewall diverso da quello SO Windows, l'amministratore della rete antivirus deve configurarlo manualmente in modo opportuno.

### 4.2.1. Connessioni dirette

#### Configurazione del Server Dr.Web

Nelle impostazioni del Server Dr.Web deve essere indicato l'indirizzo (v. documento **Allegati, Allegato D. Specifica dell'indirizzo di rete**) su cui il Server Dr.Web deve essere "in ascolto" per la ricezione delle connessioni TCP in arrivo.

Questo parametro viene indicato nelle impostazioni del Server Dr.Web **Amministrazione** → **Configurazione del Server Dr.Web** → scheda **Rete** → scheda **Trasporto** → campo **Indirizzo**.

Di default viene impostato che il Server Dr.Web "è in ascolto" con i seguenti parametri:

- **Indirizzo:** valore vuoto — utilizza *tutte le interfacce di rete* per questo computer su cui è installato Server Dr.Web.
- **Porta:** 2193 — utilizza la porta 2193.



La porta 2193 è assegnata a Dr.Web Enterprise Management Service in IANA.

Per il corretto funzionamento di tutto il sistema Dr.Web Enterprise Security Suite, è sufficiente che il Server Dr.Web "sia in ascolto" su almeno una porta TCP che deve essere conosciuta da tutti i client.



## Configurazione dell'Agent Dr.Web

All'installazione di Agent Dr.Web, l'indirizzo di Server Dr.Web (indirizzo IP, il NetBIOS o il nome a dominio del computer su cui è in esecuzione Server Dr.Web) può essere esplicitamente indicato nei parametri di installazione:

```
drwinst /server <Indirizzo_Server_Dr.Web>
```

All'installazione di Agent Dr.Web, come indirizzo di Server Dr.Web è consigliato utilizzare il nome di Server Dr.Web in [formato FQDN](#). Questo semplificherà il processo di configurazione della rete antivirus, relativo alla procedura di reinstallazione di Server Dr.Web su un altro computer. In tale caso, se verrà cambiato l'indirizzo di Server Dr.Web, sarà sufficiente modificarlo nelle impostazioni del server DNS per il nome del computer con Server Dr.Web in modo che tutti gli agent si connettano automaticamente al nuovo server.

Di default, il comando `drwinst` eseguito senza parametri scansiona la rete cercando i Server Dr.Web e tenta di installare l'Agent Dr.Web dal primo Server Dr.Web trovato nella rete (modalità *Multicasting* con l'utilizzo di [Servizio di rilevamento di Server Dr.Web](#)).

In questo modo, l'indirizzo del Server Dr.Web diventa noto all'Agent Dr.Web durante l'installazione.

In seguito, l'indirizzo del Server Dr.Web può essere modificato manualmente nelle impostazioni dell'Agent Dr.Web.

### 4.2.2. Servizio di rilevamento di Server Dr.Web

Con questo schema di connessione il client non conosce in anticipo l'indirizzo del Server Dr.Web. Ogni volta prima di stabilire la connessione, il client cerca il Server Dr.Web nella rete. Per farlo, il client invia nella rete una richiesta broadcast e attende una risposta dal Server Dr.Web in cui è indicato il suo indirizzo. Dopo aver ricevuto la risposta, il client stabilisce una connessione al Server Dr.Web.

Per questo scopo, il Server Dr.Web deve rimanere *in ascolto* di tali richieste sulla rete.

Sono possibili diverse varianti di configurazione di questo schema. È importante che il metodo di ricerca del Server Dr.Web, impostato per i client, sia coerente con le impostazioni della parte di risposta del Server Dr.Web.

In Dr.Web Enterprise Security Suite di default viene utilizzata la modalità *Multicast over UDP*:

1. Il Server Dr.Web viene registrato in un gruppo multicast con l'indirizzo indicato nelle impostazioni del Server Dr.Web.
2. Gli Agent Dr.Web, cercando il Server Dr.Web, inviano nella rete le richieste multicast all'indirizzo di gruppo definito nel punto 1.



Di default per l'ascolto da parte del Server Dr.Web viene impostato l'indirizzo `udp/231.0.0.1:2193` (analogamente alle connessioni dirette).

Questo parametro viene configurato nelle impostazioni del Pannello di controllo:

**Amministrazione** → **Configurazione del Server Dr.Web** → **Rete** → **Trasporto** → **TCP/IP**. Il valore vuoto prescrive di utilizzare l'indirizzo di default indicato sopra.

### 4.2.3. Utilizzo del protocollo SRV

I client con SO Windows supportano il protocollo di rete client *SRV* (la descrizione del formato è riportata in documento **Allegati**, [Allegato D. Specifica dell'indirizzo di rete](#)).

**Un client può connettersi al Server Dr.Web tramite i record SRV nel seguente modo:**

1. Durante l'installazione del Server Dr.Web, viene configurata la registrazione in dominio Active Directory, l'installer inserisce il record SRV corrispondente su server DNS.



Il record SRV viene inserito su server DNS in conformità a RFC2782 (v. <https://datatracker.ietf.org/doc/html/rfc2782>).

2. Quando viene richiesta una connessione al Server Dr.Web, l'utente imposta la comunicazione attraverso il protocollo `srv`.

Per esempio, l'esecuzione dell'installer di Agent Dr.Web:

- con l'esplicita indicazione del nome del servizio `myservice`:  
`drwinst /server "srv/myservice"`
- senza l'esplicita indicazione del nome del servizio. In tale caso nei record SRV verrà cercato il nome di default — `drwcs`:  
`drwinst /server "srv/"`

3. Il client utilizza le funzioni del protocollo SRV in modo trasparente all'utente per la comunicazione con il Server Dr.Web.



Se per la comunicazione il Server Dr.Web non è indicato in modo esplicito, come nome del servizio di default viene utilizzato `drwcs`.

## 4.3. Connessione sicura

### 4.3.1. Cifratura e compressione del traffico dati

La modalità di cifratura viene utilizzata per garantire la sicurezza dei dati trasmessi su un canale non sicuro e permette di evitare l'eventuale divulgazione di informazioni preziose e sostituzione di software caricati sulle postazioni protetti.



La rete antivirus di Dr.Web Enterprise Security Suite utilizza i seguenti strumenti crittografici:

- Firma digitale elettronica (GOST R 34.10-2001).
- Crittografia asimmetrica (VKO GOST R 34.10-2001 — RFC 4357).
- Crittografia simmetrica (GOST 28147-89).
- Funzione di hash crittografica (GOST R 34.11-94).

La rete antivirus di Dr.Web Enterprise Security Suite permette di criptare il traffico tra il Server Dr.Web e i client, a cui appartengono:

- Agent Dr.Web.
- Installer di Agent Dr.Web.
- Server Dr.Web adiacenti.
- Server proxy Dr.Web.

Visto che il traffico tra i componenti, in particolare tra i Server Dr.Web, può essere abbastanza grande, la rete antivirus permette di impostare la compressione di tale traffico. La configurazione del criterio di compressione e la compatibilità di queste impostazioni su vari client sono analoghe alle impostazioni di cifratura.

## Criterio di coordinazione delle impostazioni

Il criterio di utilizzo della cifratura e della compressione viene impostato separatamente su ogni componente della rete antivirus, e le impostazioni degli altri componenti devono essere coerenti con le impostazioni del Server Dr.Web.

Quando vengono coordinate le impostazioni di cifratura e di compressione sul Server Dr.Web e su un client, è necessario tenere presente che alcune combinazioni di impostazioni non sono ammissibili e la scelta delle stesse porterà all'impossibilità di stabilire una connessione tra il Server Dr.Web e il client.

Nella [tabella 4-1](#) sono riportate informazioni su quello con quali impostazioni la connessione tra il Server Dr.Web e il client sarà cifrata/compressa (+), con quali sarà non cifrata/non compressa (–) e quali combinazioni non sono ammissibili (**Errore**).

**Tabella 4-1. Compatibilità delle impostazioni dei criteri di cifratura e di compressione**

Impostazioni del client	Impostazioni del Server Dr.Web		
	Sì	Possibile	No
Sì	+	+	Errore
Possibile	+	+	–
No	Errore	–	–



L'utilizzo della cifratura di traffico dati crea un notevole carico di elaborazione sui computer con le prestazioni vicine al minimo ammissibile per i componenti installati. Se la cifratura di traffico dati non è richiesta per fornire la sicurezza aggiuntiva, è possibile rinunciare all'utilizzo di questa modalità.

Per disattivare la modalità di cifratura, è necessario far passare sequenzialmente il Server Dr.Web e i componenti prima in modalità **Possibile** evitando la formazione di coppie client-server incompatibili.

L'utilizzo della compressione diminuisce il traffico dati, ma aumenta notevolmente il consumo di memoria operativa e il carico di elaborazione sui computer in misura maggiore rispetto alla cifratura.

## Connessione attraverso Server proxy Dr.Web

Quando i client si connettono al Server Dr.Web attraverso il Server proxy Dr.Web, è necessario tenere conto delle impostazioni di cifratura e compressione su tutti i tre componenti. In tale caso:

- Le impostazioni di Server Dr.Web e di Server proxy (qui svolge il ruolo di client) devono concordare secondo la [tabella 4-1](#).
- Le impostazioni di client e di Server proxy (qui svolge il ruolo di Server Dr.Web) devono concordare secondo la [tabella 4-1](#).

La possibilità di stabilire una connessione attraverso il Server proxy dipende dalle versioni di Server Dr.Web e di client che supportano determinate tecnologie di cifratura:

- Se il Server Dr.Web e il client supportano la cifratura TLS, utilizzata nella versione 13.0, allora basta che siano soddisfatte le [condizioni descritte sopra](#) per stabilire una connessione operativa.
- Se uno dei componenti non supporta la cifratura TLS: sul Server Dr.Web e/o sul client è installata la versione 10 e precedenti con la cifratura GOST, viene eseguita una verifica aggiuntiva secondo la [tabella 4-2](#).

**Tabella 4-2. Compatibilità delle impostazioni dei criteri di cifratura e di compressione nell'uso di Server proxy**

Impostazioni della connessione con il client	Impostazioni della connessione con il Server Dr.Web			
	Nulla	Compressione	Cifratura	Tutto
Nulla	Modalità normale	Modalità normale	Errore	Errore
Compressione	Modalità normale	Modalità normale	Errore	Errore
Cifratura	Errore	Errore	Modalità trasparente	Errore



Impostazioni della connessione con il client	Impostazioni della connessione con il Server Dr.Web			
	Nulla	Compressione	Cifratura	Tutto
Tutto	Errore	Errore	Errore	Modalità trasparente

### Segni convenzionali

Impostazioni delle connessioni con il Server Dr.Web e con il client	
Nulla	Non è supportata né la compressione né la cifratura.
Compressione	È supportata solo la compressione.
Cifratura	È supportata solo la cifratura.
Tutto	Sono supportate sia la compressione che la cifratura.

Risultato della connessione	
Modalità normale	La connessione stabilita implica il funzionamento in modalità normale — con l'elaborazione dei comandi e la memorizzazione nella cache.
Modalità trasparente	La connessione stabilita implica il funzionamento in modalità trasparente — senza l'elaborazione dei comandi e la memorizzazione nella cache. Viene selezionata la versione minima del protocollo di cifratura: se uno dei componenti (Server Dr.Web o Agent Dr.Web) è della versione 13 e l'altro è della versione 10, viene impostata la cifratura utilizzata nella versione 10.
Errore	La connessione del Server proxy con il Server Dr.Web e con il client verrà interrotta.

Pertanto, se il Server Dr.Web e l'Agent Dr.Web sono di diverse versioni: uno della versione 13 e l'altro della versione 10 e precedenti, alle connessioni stabilite attraverso il Server proxy si applicano le seguenti limitazioni:

- La memorizzazione dei dati nella cache sul Server proxy è possibile solo se entrambe le connessioni — quella con il Server Dr.Web e quella con il client sono state stabilite senza uso di cifratura.
- La cifratura verrà utilizzata solo se entrambe le connessioni — quella con il Server Dr.Web e quella con il client sono state stabilite con l'uso di cifratura e con gli stessi parametri di compressione (per entrambe le connessioni c'è la compressione o per entrambe non c'è).



## Impostazioni di cifratura e di compressione sul Server Dr.Web

### Per definire le impostazioni di compressione e cifratura del Server Dr.Web

1. Selezionare la voce **Amministrazione** nel menu principale del Pannello di controllo.
2. Nella finestra che si è aperta selezionare la voce del menu di gestione **Configurazione del Server Dr.Web**.
3. Nella scheda **Rete** → **Trasporto** selezionare dalle liste a cascata **Crittografia** e **Compressione** una delle varianti:
  - **Sì** — è obbligatoria la cifratura (o la compressione) del traffico con tutti i client (valore predefinito per la cifratura, se non è stato diversamente specificato durante l'installazione del Server Dr.Web).
  - **Possibile** — la cifratura (o la compressione) viene eseguita per il traffico con i client, le cui impostazioni non lo bloccano.
  - **No** — la cifratura (o la compressione) non è supportata (valore predefinito per la compressione, se non è stato diversamente specificato durante l'installazione del Server Dr.Web).



Quando si impostano la cifratura e la compressione sul lato Server Dr.Web, prestare attenzione alle caratteristiche dei client che si pianifica di connettere a questo Server Dr.Web. Non tutti i client supportano la cifratura e la compressione di traffico.

## Impostazioni di cifratura e di compressione sul Server proxy Dr.Web

### Per definire in modo centralizzato le impostazioni di cifratura e di compressione per il Server proxy



Se il Server proxy non è connesso al Server Dr.Web per la gestione delle impostazioni in remoto, configurare una connessione come descritto in p. [Connessione del Server proxy Dr.Web al Server Dr.Web](#).

1. Aprire il Pannello di controllo per il Server Dr.Web che è il server di gestione per il Server proxy.
2. Selezionare la voce **Rete antivirus** nel menu principale del Pannello di controllo, nella finestra che si è aperta nella lista gerarchica fare clic sul nome del Server proxy di cui si vuole modificare le impostazioni o sul nome del suo gruppo primario se le impostazioni del Server proxy sono ereditate.
3. Nel menu di gestione che si è aperto selezionare la voce **Server proxy Dr.Web**. Si aprirà la sezione delle impostazioni.



4. Passare alla scheda **Ascolto**.
5. Nella sezione **Parametri di connessione con i client** nella lista a cascata **Crittografia** e **Compressione** selezionare la modalità di cifratura e di compressione del traffico per i canali tra il Server proxy e i relativi client: Agent Dr.Web ed installer di Agent Dr.Web.
6. Nella sezione **Parametri di connessione con i Server Dr.Web** viene impostata una lista dei Server Dr.Web su cui verrà reindirizzato il traffico. Selezionare nella lista il Server Dr.Web richiesto e premere il pulsante  sulla barra degli strumenti di questa sezione per modificare i parametri di connessione con il Server Dr.Web selezionato. Nella finestra che si è aperta, nelle liste a cascata **Crittografia** e **Compressione** selezionare la modalità di cifratura e di compressione del traffico per il canale tra il Server proxy e il Server Dr.Web selezionato.
7. Per salvare le impostazioni definite, premere il pulsante **Salva**.

### Per definire localmente le impostazioni di cifratura e di compressione per il Server proxy



Se il Server proxy è connesso al Server Dr.Web di gestione per la configurazione in remoto, il file di configurazione del Server proxy verrà sovrascritto in base alle impostazioni arrivate dal Server Dr.Web. In tale caso, è necessario definire le impostazioni in remoto dal Server Dr.Web o disattivare l'impostazione che permette di accettare configurazioni da questo Server Dr.Web.

La descrizione del file di configurazione `drwcsd-proxy.conf` è riportata in documento **Allegati**, [F4. File di configurazione di Server proxy Dr.Web](#)

1. Sul computer su cui è installato il Server proxy aprire il file di configurazione `drwcsd-proxy.conf`.
2. Modificare le impostazioni di compressione e cifratura per le connessioni con i client e con i Server Dr.Web.
3. Riavviare il Server proxy:
  - In caso di SO Windows:
    - Se il Server proxy è in esecuzione come un servizio di SO Windows, il servizio viene riavviato tramite i mezzi standard del sistema.
    - Se il Server proxy è in esecuzione nella console, per riavviare, premere CTRL+BREAK.
  - In caso di SO della famiglia UNIX:
    - Inviare il segnale `SIGHUP` al daemon Server proxy.
    - Eseguire il seguente comando:

In caso di SO Linux:

```
/etc/init.d/dwcp_proxy restart
```

In caso di SO FreeBSD:

```
/usr/local/etc/rc.d/dwcp_proxy restart
```



## Impostazioni di cifratura e di compressione sulle postazioni

### Per definire in modo centralizzato le impostazioni di cifratura e di compressione delle postazioni

1. Selezionare la voce **Rete antivirus** nel menu principale del Pannello di controllo, nella finestra che si è aperta nella lista gerarchica fare clic sul nome di una postazione o di un gruppo.
2. Nel menu di gestione che si è aperto selezionare la voce **Parametri di connessione**.
3. Nella scheda **Generali** selezionare dalle liste a cascata **Modalità di compressione** e **Modalità di cifratura** una delle varianti:
  - **Sì** — è obbligatoria la cifratura (o la compressione) del traffico con il Server Dr.Web.
  - **Possibile** — la cifratura (o la compressione) viene eseguita per il traffico con il Server Dr.Web se le impostazioni del Server Dr.Web non lo vietano.
  - **No** — la cifratura (o la compressione) non è supportata.
4. Premere **Salva**.
5. Le modifiche diventeranno effettive non appena le impostazioni verranno trasmesse sulle postazioni. Se le postazioni sono disconnesse al momento della modifica delle impostazioni, le modifiche verranno trasmesse non appena le postazioni si connetteranno a Server Dr.Web.

### Agent Dr.Web per Windows

Le impostazioni di cifratura e di compressione possono essere definite durante l'installazione di Agent Dr.Web:

- In caso di installazione in remoto dal Pannello di controllo la modalità di cifratura e compressione viene definita direttamente nelle impostazioni della sezione **Installazione via rete**.
- In caso di installazione locale l'installer grafico non fornisce la possibilità di modificare la modalità di cifratura e di compressione, tuttavia, queste impostazioni possono essere definite tramite le opzioni della riga di comando all'avvio dell'installer (v. documento **Allegati**, [G1. Installer di rete](#)).

Dopo l'installazione di Agent Dr.Web la possibilità di modificare le impostazioni di cifratura e compressione localmente sulla postazione non è fornita. Di default è impostata la modalità **Possibile** (se durante l'installazione non è stato impostato un altro valore), cioè l'utilizzo della cifratura e della compressione dipende dalle impostazioni sul lato Server Dr.Web. Tuttavia, le impostazioni sul lato Agent Dr.Web possono essere modificate attraverso il Pannello di controllo (v. [sopra](#)).



## Antivirus Dr.Web per Android

Antivirus Dr.Web per Android non supporta né la cifratura né la compressione. La connessione non sarà possibile se è impostato il valore **Si** per la cifratura e/o compressione sul lato Server Dr.Web o sul lato Server proxy (nel caso di connessione attraverso il Server proxy).

## Antivirus Dr.Web per Linux

Durante l'installazione dell'antivirus non è possibile modificare la modalità di cifratura e compressione. Di default è impostata la modalità **Possibile**.

Dopo l'installazione dell'antivirus la possibilità di modificare le impostazioni di cifratura e compressione localmente sulla postazione viene fornita solo in modalità console. La modalità di funzionamento console e le relative opzioni della riga di comando vengono descritte in **Manuale dell'utente di Dr.Web per Linux**.

Inoltre, le impostazioni sul lato postazione possono essere modificate attraverso il Pannello di controllo (v. [sopra](#)).

## Antivirus Dr.Web per macOS

La possibilità di modificare le impostazioni di cifratura e compressione localmente sulla postazione non viene fornita. Di default è impostata la modalità **Possibile**, cioè l'utilizzo della cifratura e della compressione dipende dalle impostazioni sul lato Server Dr.Web.

Le impostazioni sul lato postazione possono essere modificate attraverso il Pannello di controllo (v. [sopra](#)).

### 4.3.2. Strumenti per la connessione sicura

Durante l'installazione di Server Dr.Web vengono creati i seguenti strumenti che forniscono una connessione sicura tra i componenti della rete antivirus.

#### 1. Chiave di cifratura privata di Server Dr.Web `drwcsd.pri`.

Viene conservata sul Server Dr.Web e non viene trasmessa ad altri componenti della rete antivirus.

Se la chiave privata viene persa, è necessario ripristinare manualmente la connessione tra i componenti della rete antivirus (ovvero creare tutte le chiavi e tutti i certificati, e inoltre propagarli su tutti i componenti della rete).

La chiave privata viene utilizzata nei seguenti casi:

##### a) Creazione delle chiavi pubbliche e dei certificati.

La chiave di cifratura pubblica e il certificato vengono creati automaticamente dalla chiave privata durante l'installazione di Server Dr.Web. In tale caso è possibile sia creare



una nuova chiave privata che utilizzarne una esistente (per esempio, quella dall'installazione precedente di Server Dr.Web). Inoltre, le chiavi di cifratura e i certificati possono essere creati in qualsiasi momento tramite l'utility di server `drwsign` (v. documento **Allegati**, [H7.1. Utility di generazione delle chiavi e dei certificati digitali](#)).

Informazioni sulle chiavi pubbliche e sui certificati sono riportate di seguito.

*b) Autenticazione di Server Dr.Web.*

L'autenticazione di Server Dr.Web dai client remoti viene effettuata in base alla firma digitale elettronica (una volta nel corso di ciascuna connessione).

Il Server Dr.Web firma digitalmente un messaggio tramite la chiave privata e invia il messaggio al client. Il client verifica la firma del messaggio ricevuto tramite il certificato.

*c) Decifratura dei dati.*

In caso di cifratura del traffico tra il Server Dr.Web e i client, la decifratura dei dati inviati dal client viene effettuata sul Server Dr.Web tramite la chiave privata.

## 2. Chiave di cifratura pubblica di Server Dr.Web \*.pub.

È disponibile per tutti i componenti della rete antivirus. La chiave pubblica può sempre essere generata dalla chiave privata (v. [sopra](#)). A ciascuna generazione da una stessa chiave privata risulta una stessa chiave pubblica.

A partire dalla versione 11 di Server Dr.Web la chiave pubblica viene utilizzata per la comunicazione con i client delle versioni precedenti. Le altre funzionalità sono state trasferite al certificato che, tra le altre cose, contiene la chiave di cifratura pubblica.

## 3. Certificato di Server Dr.Web `drwcsd-certificate.pem`.

È disponibile per tutti i componenti della rete antivirus. Il certificato contiene la chiave di cifratura pubblica. Il certificato può essere generato dalla chiave privata (v. [sopra](#)). A ciascuna generazione da una stessa chiave privata risulta un nuovo certificato.

I client connessi al Server Dr.Web sono legati a un certificato specifico perciò se il certificato viene perso su un client, è possibile ripristinarlo solo se lo stesso certificato viene utilizzato da qualche altro componente della rete: in tale caso il certificato può essere copiato sul client dal Server Dr.Web o dall'altro client.

Il certificato viene utilizzato nei seguenti casi:

*a) Autenticazione di Server Dr.Web.*

L'autenticazione di Server Dr.Web dai client remoti viene effettuata in base alla firma digitale elettronica (una volta nel corso di ciascuna connessione).

Il Server Dr.Web firma digitalmente un messaggio tramite la chiave privata e invia il messaggio al client. Il client verifica la firma del messaggio ricevuto tramite il certificato (in particolare, tramite la chiave pubblica indicata nel certificato). Nelle versioni precedenti di Server Dr.Web per questo scopo veniva utilizzata direttamente la chiave pubblica.

Per questo scopo è necessaria la presenza sul client di uno o più certificati affidabili dai Server Dr.Web a cui il client può connettersi.



b) *Cifratura dei dati.*

In caso di cifratura del traffico tra il Server Dr.Web e i client, la cifratura dei dati viene effettuata dal client tramite la chiave pubblica.

c) *Realizzazione di una sessione TLS tra il Server Dr.Web e i client remoti.*

d) *Autenticazione di Server proxy.*

L'autenticazione dei Server proxy Dr.Web dai client remoti viene effettuata in base alla firma digitale elettronica (una volta nel corso di ciascuna connessione).

Il Server proxy firma i suoi certificati con la chiave privata e il certificato del Server Dr.Web. Un client che si fida del certificato del Server Dr.Web si fiderà automaticamente dei certificati con esso firmati.

#### 4. Chiave privata di web server.

Viene conservata sul Server Dr.Web e non viene trasmessa ad altri componenti della rete antivirus. I dettagli di utilizzo sono indicati di seguito.

#### 5. Certificato di web server.

È disponibile per tutti i componenti della rete antivirus.

Viene utilizzato per la realizzazione di una sessione TLS tra il web server e il browser (attraverso HTTPS).

All'installazione di Server Dr.Web viene generato sulla base della chiave privata di web server un certificato auto-firmato che non verrà accettato dai browser in quanto non è stato rilasciato da note autorità di certificazione.

Affinché una connessione sicura (HTTPS) sia disponibile, è necessario eseguire una delle seguenti azioni:

- Aggiungere il certificato auto-firmato a quelli attendibili o alle eccezioni per tutte le postazioni e i browser su cui si apre il Pannello di controllo.
- Ottenere un certificato firmato da una nota autorità di certificazione.

### 4.3.3. Connessione dei client al Server Dr.Web

Per la possibilità di connessione al Server Dr.Web, sul lato client deve essere presente un certificato di Server Dr.Web, a prescindere da quello se verrà cifrato il traffico tra il Server Dr.Web e il client.

Al Server Dr.Web possono connettersi i seguenti client:

- **Agent Dr.Web.**

Per il funzionamento degli Agent Dr.Web in modalità centralizzata con la connessione al Server Dr.Web, è necessaria la presenza sulla postazione di uno o più certificati affidabili dai Server Dr.Web a cui può connettersi l'Agent Dr.Web.



Il certificato utilizzato per l'installazione e inoltre i certificati ottenuti attraverso le impostazioni centralizzate dal Server Dr.Web vengono conservati nel registro, ma i file di certificati stessi non vengono utilizzati.

Un file di certificato in un unico esemplare può essere aggiunto tramite un'opzione della riga di comando alla directory di installazione di Agent Dr.Web (ma non al registro) e alla lista generale dei certificati utilizzati. Tale certificato verrà utilizzato, tra l'altro, per la possibilità di connessione al Server Dr.Web per il caso di un errore nelle impostazioni centralizzate.

Nel caso di certificato assente o certificato non valido, l'Agent Dr.Web non potrà connettersi al Server Dr.Web, ma continuerà il funzionamento e l'aggiornamento in Modalità mobile, se tale modalità è consentita per questa postazione.

- **Installer di Agent Dr.Web.**

Quando viene eseguita un'installazione di Agent Dr.Web , sulla postazione, insieme al file di installazione selezionato, deve essere presente un certificato di Server Dr.Web.

Se viene avviato un pacchetto di installazione creato nel Pannello di controllo, il certificato fa parte del pacchetto di installazione e non è richiesto indicare in aggiunta il file del certificato.

Dopo l'installazione di Agent Dr.Web i dati del certificato vengono inseriti nel registro, il file di certificato stesso in seguito non viene utilizzato.

Nel caso di certificato assente o certificato non valido, l'installer non potrà installare Agent Dr.Web (questo riguarda tutti i tipi di file di installazione di Agent Dr.Web).

- **Server Dr.Web adiacenti.**

Quando viene configurata una connessione tra Server Dr.Web adiacenti versione 11 e successive, su ciascuno dei Server Dr.Web configurati è necessario indicare il certificato del Server Dr.Web con cui viene stabilita la relazione (v. **Manuale dell'amministratore**, p. [Configurazione delle relazioni tra i Server Dr.Web](#)).

Se almeno un certificato è assente o invalido, la connessione tra i server non potrà essere stabilita.

- **Server proxy Dr.Web.**

Per connettere un Server proxy al Server Dr.Web con la possibilità di configurazione in remoto attraverso il Pannello di controllo, è necessaria la presenza di un certificato sulla postazione con il Server proxy installato. Il Server proxy potrà anche supportare la cifratura.

Se il certificato è assente, il Server proxy continuerà a funzionare, però non saranno disponibili la gestione remota e inoltre la cifratura e la memorizzazione nella cache.



In caso di un aggiornamento regolare dell'intera rete antivirus da una versione precedente che utilizzava chiavi pubbliche a una versione nuova che utilizza certificati, non sono richieste alcune azioni aggiuntive.



Non è consigliabile installare un Agent Dr.Web fornito con un Server Dr.Web versione 11 connettendolo a un Server Dr.Web versione 10 e viceversa.

## 4.4. Integrazione di Dr.Web Enterprise Security Suite con Active Directory

Se nella rete locale protetta viene utilizzato il servizio Active Directory, è possibile configurare l'integrazione dei componenti di Dr.Web Enterprise Security Suite con questo servizio.



Tutti i seguenti metodi sono indipendenti l'uno dall'altro e possono essere utilizzati sia singolarmente che in combinazione.

L'integrazione di Dr.Web Enterprise Security Suite con Active Directory viene effettuata sulla base dei seguenti metodi:

### 1. Registrazione del Server Dr.Web nel dominio Active Directory per l'accesso al Server Dr.Web tramite il protocollo SRV

Durante l'installazione del Server Dr.Web è fornita la possibilità di registrare il Server Dr.Web nel dominio Active Directory tramite gli strumenti dell'installer. Nel corso della registrazione sul server DNS viene creato un record SRV corrispondente al Server Dr.Web. In seguito i client possono accedere al Server Dr.Web attraverso questo record SRV.

Per maggiori informazioni v. [Installazione di Server Dr.Web per SO Windows](#) e [Utilizzo del protocollo SRV](#).

### 2. Sincronizzazione della struttura della rete antivirus con il dominio Active Directory

È possibile configurare la sincronizzazione automatica della struttura della rete antivirus con le postazioni nel dominio Active Directory. In tale caso i container di Active Directory che contengono computer diventano gruppi della rete antivirus in cui vengono messe le postazioni.

Per questo scopo è fornito il task **Sincronizzazione con Active Directory** nel calendario di Server Dr.Web. L'amministratore deve creare questo task in autonomo tramite Scheduler di Server Dr.Web.

Per maggiori informazioni v. **Manuale dell'amministratore**, [Configurazione di calendario del Server Dr.Web](#).

### 3. Autenticazione degli utenti di Active Directory sul Server Dr.Web come amministratori

È fornita la possibilità di autenticazione sul Server Dr.Web degli utenti con gli account di Active Directory per la gestione della rete antivirus. Per questo scopo è necessario utilizzare uno dei seguenti metodi:



- Autenticazione LDAP/AD. È disponibile per i Server Dr.Web su tutti i sistemi operativi supportati. L'accesso al Server Dr.Web viene configurato per gli utenti in base agli attributi di Active Directory corrispondenti tramite il Pannello di controllo. L'accesso diretto al controller di dominio e allo snap-in di Active Directory non è richiesto — non viene effettuata alcuna configurazione aggiuntiva da parte di Active Directory.
- Microsoft Active Directory. È disponibile solo per i Server Dr.Web SO Windows inclusi nel dominio di destinazione. Gli utenti e i gruppi di utenti che hanno accesso a Server Dr.Web vengono configurati direttamente nello snap-in di Active Directory. È richiesta la configurazione iniziale tramite le utility aggiuntive. I pacchetti `drweb-<versione_pacchetto>-<build>-esuite-modify-ad-schema-<versione_SO>.exe` e `drweb-<versione_pacchetto>-<build>-esuite-aduac-<versione_SO>.msi` sono disponibili nel repository di Server Dr.Web nei **Prodotti aziendali Dr.Web**.

La scelta del metodo dipende dal sistema operativo di Server Dr.Web e dal modo di configurazione degli utenti autorizzati.

Per maggiori informazioni v. **Manuale dell'amministratore**, [Autenticazione degli amministratori](#).

#### 4. Installazione remota di Agent Dr.Web su una postazione nel dominio Active Directory

È possibile installare Agent Dr.Web in remoto su una postazione nel dominio Active Directory. Per questo scopo è necessario:

- a) Eseguire l'installazione amministrativa sulla risorsa condivisa di destinazione utilizzando l'installer di Agent Dr.Web speciale per Active Directory. Il pacchetto `drweb-<versione_pacchetto>-<build>-esuite-agent-activedirectory.msi` è disponibile nel repository di Server Dr.Web nei **Prodotti aziendali Dr.Web**.
- b) Configurare i criteri di Active Directory corrispondenti per l'installazione automatica del pacchetto sulle postazioni nel dominio.

Per maggiori informazioni v. [Installazione di Agent Dr.Web con utilizzo del servizio Active Directory](#).

#### 5. Ricerca delle postazioni del dominio Active Directory

È fornita la possibilità di cercare le postazioni del dominio Active Directory attraverso Scanner di rete. In tale caso è possibile determinare la presenza di Agent Dr.Web sulle postazioni trovate, e se è assente, installare Agent Dr.Web in remoto tramite il Pannello di controllo.

Questo approccio all'installazione remota di Agent Dr.Web può essere utilizzato insieme all'installazione automatica dei pacchetti tramite criteri di Active Directory, descritta in p. 4.

Per maggiori informazioni v. **Manuale dell'amministratore**, [Scanner di rete](#).

#### 6. Ricerca degli utenti del dominio Active Directory

È fornita la possibilità di cercare gli utenti del dominio Active Directory per creare i loro profili personali e per mettere a punto Office control e Controllo delle applicazioni.



Per maggiori informazioni vedi **Guida alla gestione delle postazioni per Windows**.



## Capitolo 5: Installazione dei componenti di Dr.Web Enterprise Security Suite

Prima di iniziare a installare i componenti Dr.Web Enterprise Security Suite, leggere la sezione [Creazione della rete antivirus](#).

### 5.1. Installazione di Server Dr.Web

L'installazione di Server Dr.Web è il primo passo della creazione di una rete antivirus. Fino a quando non verrà installato il Server, non può essere installato nessun altro componente della rete antivirus.

L'avanzamento del processo di installazione di Server Dr.Web dipende dalla versione (quella per SO Windows o quella per SO della famiglia UNIX) che viene installata.



Tutti i parametri che vengono impostati durante l'installazione possono essere modificati in seguito dall'amministratore della rete antivirus nel processo di funzionamento del Server Dr.Web.

---

Se il software Server Dr.Web è già installato, consultare rispettivamente le sezioni [Aggiornamento di Server Dr.Web per SO Windows](#) o [Aggiornamento di Server Dr.Web per SO della famiglia UNIX](#).



Se prima dell'installazione del software Server Dr.Web è stato rimosso un Server Dr.Web installato in precedenza, nel processo di installazione verranno cancellati i contenuti del repository e ne verrà installata una versione nuova. Se per qualche motivo è stato salvato il repository della versione precedente, è necessario cancellarne manualmente tutti i contenuti prima di installare la nuova versione di Server Dr.Web e aggiornare il repository completamente dopo l'installazione del Server Dr.Web.

---

Il nome della directory in cui viene installato il Server Dr.Web deve essere impostato nella stessa lingua che è indicata nelle impostazioni di lingua di SO Windows per i programmi che non utilizzano Unicode. Altrimenti, l'installazione del Server Dr.Web non verrà completata.

L'eccezione è la lingua inglese nel nome della directory di installazione.

Insieme al Server Dr.Web viene installato automaticamente il Pannello di controllo della sicurezza Dr.Web che si usa per gestire la rete antivirus e configurare il Server Dr.Web.

Di default, dopo l'installazione il Server Dr.Web si avvia automaticamente, se è la versione per SO Windows, e richiede un avvio manuale, se è la versione per i SO della famiglia UNIX.



### 5.1.1. Installazione di Server Dr.Web per SO Windows

Di seguito viene descritta l'installazione di Server Dr.Web per SO Windows.

**Prima di installare il Server Dr.Web, si consiglia di prestare attenzione alle seguenti informazioni:**



Il file del pacchetto e gli altri file richiesti durante l'installazione del programma devono essere situati su dischi locali del computer su cui viene installato il software Server Dr.Web. I permessi di accesso devono essere configurati in modo che questi file siano disponibili per l'utente **LOCALSYSTEM**.

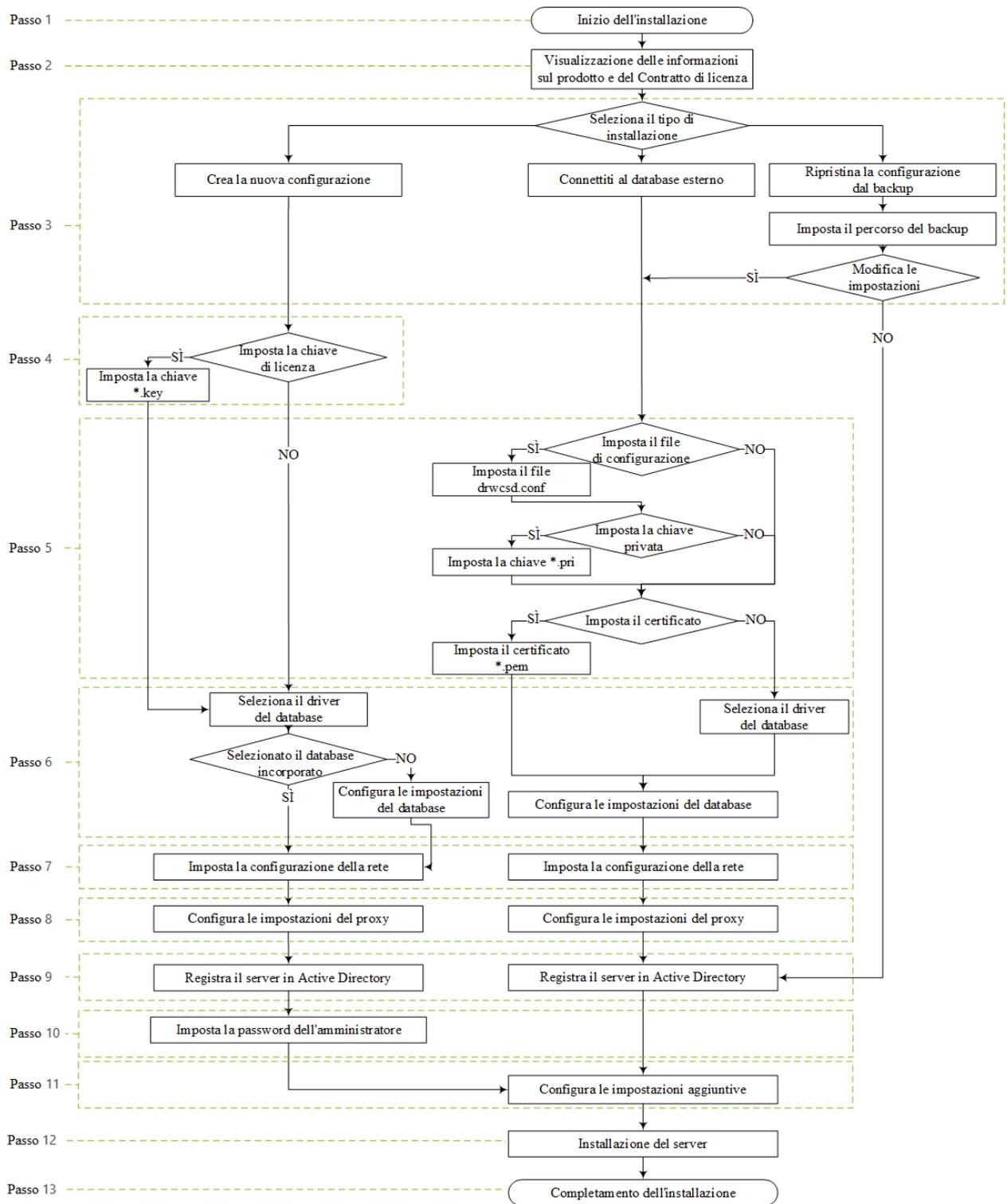
---

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



Dopo l'installazione di Server Dr.Web è necessario aggiornare tutti i componenti di Dr.Web Enterprise Security Suite (v. **Manuale dell'amministratore**, p. [Aggiornamento del repository di Server Dr.Web manualmente](#)).

In [Immagine 5-1](#) è riportato uno schema a blocchi del processo di installazione di Server Dr.Web tramite il programma di installazione. I passi di installazione dello schema corrispondono alla dettagliata descrizione della procedura riportata [sotto](#).



**Immagine 5-1. Schema a blocchi del processo di installazione di Server Dr.Web (Premere un blocco dello schema per passare alla descrizione)**

### Per installare Server Dr.Web su un computer con SO Windows

1. Avviare il file del pacchetto. Durante l'installazione viene controllata la presenza di una versione del pacchetto più nuova su SAM.



Di default, come lingua dell'installer viene selezionata la lingua del sistema operativo. Se necessario, si può cambiare la lingua di installazione in qualsiasi passo, selezionando la voce corrispondente nell'angolo superiore destro della finestra di installer.

2. Si apre una finestra con informazioni sul prodotto che viene installato e un link al testo del contratto di licenza. Dopo aver letto le condizioni del contratto di licenza, per continuare l'installazione, premere il pulsante **Avanti**.
3. Nella finestra successiva selezionare il tipo di installazione di Server Dr.Web:
  - **Crea nuova configurazione** — con questo tipo di installazione verrà creata una nuova configurazione del Server con le impostazioni predefinite. L'uso di qualsiasi impostazione delle installazioni Server precedenti non è fornito. Per questo tipo di installazione viene inizializzato un nuovo database, indipendentemente dal tipo di database selezionato durante la configurazione. Premere **Avanti**. Andare al passaggio 4.
  - **Connettiti al database esterno** — questo tipo di installazione prevede la connessione al database esterno esistente del Server. Per questo tipo di installazione viene aggiornato il database esterno esistente da un'installazione precedente del Server. Premere **Avanti**. Andare al passaggio 5.



Se viene utilizzato un database esterno, è necessario creare preventivamente un database e configurare il driver corrispondente (v. documento **Allegati**, [Allegato A. Impostazioni per l'utilizzo dei DBMS. Parametri dei driver dei DBMS](#)).

- **Recupera la configurazione da copia di backup** — tutte le impostazioni verranno ripristinate dalla copia di backup da un'installazione precedente del Server. Impostare il percorso della copia di backup. Per questo tipo di installazione viene importato e aggiornato il dump del database da una copia di backup.
    - Se necessario, è possibile modificare manualmente le impostazioni prese dalla copia di backup. Per fare ciò, premere il pulsante **Modifica le impostazioni** — diventano disponibili le impostazioni nei passaggi 5-8.
    - Se non è necessario modificare le impostazioni manualmente, premere **Avanti**. L'uso della configurazione presa dal backup avviene automaticamente. Dal backup verranno estratti la chiave di cifratura privata e il certificato. Per continuare l'installazione, è obbligatoria la presenza del file di configurazione. Se la Procedura guidata non può ripristinare determinate impostazioni dalla copia di backup, viene visualizzata una finestra per la definizione manuale di queste impostazioni. Andare al passaggio 9.
4. Se nel passaggio 3 è stata selezionata l'opzione **Crea una nuova configurazione**, nella finestra **Licenza** configurare le impostazioni di licenza:
    - Selezionare l'opzione **Configura la licenza in un secondo momento** per continuare l'installazione del Server senza una chiave di licenza. Notare: per organizzare la protezione antivirus delle postazioni, è necessaria la disponibilità di una licenza. Le chiavi di licenza devono essere aggiunte dopo l'installazione del Server attraverso [Gestione licenze](#) oppure il numero richiesto di licenze deve essere trasferito attraverso la comunicazione inter-server da un Server adiacente.



- Selezionare l'opzione **Imposta il percorso della chiave di licenza** per impostare il file della chiave di licenza di Agent Dr.Web nel processo di installazione di Server.

Per provare il prodotto, si possono utilizzare i file della chiave demo. Premere il pulsante **Richiedi chiave demo** per andare sul sito web della società Doctor Web e per ottenere dei file della chiave demo (v. [File della chiave demo](#)).

5. Se nel passaggio 3 è stata selezionata l'opzione **Connettiti al database esterno**, o se è stata selezionata la voce **Modifica impostazioni** durante il ripristino della configurazione dal backup, nella finestra **Configurazione del Server Dr.Web** è possibile configurare le seguenti impostazioni:
  - **File di configurazione di Server Dr.Web** — percorso del file di configurazione con le impostazioni del Server da un'installazione precedente (`drwcsd.conf`).
  - **Chiave di cifratura privata di Server Dr.Web** — percorso del file con la chiave di cifratura privata del Server da un'installazione precedente. Verranno automaticamente creati un file con la chiave pubblica (il contenuto della chiave pubblica corrisponderà al contenuto della chiave pubblica precedente) e un certificato, se non specificato nel campo sottostante (ogni volta quando un certificato viene generato da una stessa chiave privata, è un nuovo certificato).
  - Se viene utilizzata la chiave di cifratura privata esistente, nel campo **Utilizza il certificato esistente di Server Dr.Web** è possibile impostare il file di certificato precedentemente utilizzato. Questo consentirà agli Agent Dr.Web già installati di connettersi al nuovo Server in quanto i client connessi a un Server sono associati a un certificato specifico (ogni volta quando un certificato viene generato da una stessa chiave privata, è un nuovo certificato). Nel caso contrario, dopo l'installazione sarà necessario copiare il nuovo certificato su tutte le postazioni su cui gli Agent Dr.Web erano precedentemente installati.



Il certificato deve corrispondere alla chiave di cifratura privata.

Se non sono specificati i percorsi dei file, verranno create nuove chiavi di cifratura, un certificato e un file di configurazione con le impostazioni predefinite.

6. Nella finestra **Driver del database** vengono configurati i parametri del database in uso che dipendono dal tipo di installazione:
  - Se nel passaggio 3 è stata selezionata l'opzione **Crea nuova configurazione**, selezionare il tipo di driver che deve essere utilizzato:
    - **Le varianti SQLite (database incorporato)** e IntDB (database incorporato) prescrivono che vengano utilizzati gli strumenti incorporati del Server Dr.Web. Non è richiesto configurare parametri aggiuntivi.
    - Le altre varianti comportano l'utilizzo del database esterno corrispondente. In tale caso è necessario indicare i parametri corrispondenti per configurare l'accesso al database. Le impostazioni dei parametri di DBMS sono descritte in dettaglio in allegati (v. documento **Allegati**, [Allegato A. Impostazioni per l'utilizzo dei DBMS. Parametri dei driver dei DBMS](#)).



- Se nel passaggio 3 è stata selezionata l'opzione **Connettiti al database esterno** o spuntato il flag **Modifica impostazioni** per l'opzione **Connettiti al database esterno**:
  - Se nel passaggio 5 è stato impostato il percorso del file di configurazione del Server, i dati da esso verranno presi automaticamente. Se necessario, modificarli.
  - Se nel passaggio 5 non è stato impostato il percorso del file di configurazione del Server, selezionare il driver del database esterno e configurare le impostazioni del database esterno a cui si conetterà il Server.
- 7. Se nel passaggio 3 è stata selezionata l'opzione **Crea nuova configurazione** o **Connettiti al database esterno** o spuntato il flag **Modifica impostazioni** per l'opzione **Connettiti al database esterno**, si aprirà la finestra **Configurazione della rete**. In questa finestra viene impostato il protocollo di rete per il funzionamento del Server (è consentito impostare solo un protocollo di rete; è possibile configurare ulteriori protocolli in seguito).
  - Nei campi **Interfaccia** e **Porta** impostare i rispettivi valori per le connessioni al Server.



Di default viene utilizzata la porta 2193.

Gli indirizzi vengono impostati nel formato di indirizzo di rete riportato in documento **Allegati**, [Allegato D. Specifica dell'indirizzo di rete](#).

- Spuntare il flag **Attiva il servizio di rilevamento di Server Dr.Web** se si vuole che il Server risponda alle richieste broadcast e multicast degli altri Server secondo l'indirizzo IP e il nome di servizio impostati nei rispettivi campi sotto.
8. Se nel passaggio 3 è stata selezionata l'opzione **Crea nuova configurazione** o **Connettiti al database esterno** o spuntato il flag **Modifica impostazioni** per l'opzione **Connettiti al database esterno**, si aprirà la finestra **Server proxy** per la configurazione dei parametri di utilizzo del server proxy per la connessione al Server Dr.Web.

Affinché le connessioni al Server vengano effettuate attraverso il server proxy, spuntare il flag **Utilizza server proxy**.



Il flag **Utilizza server proxy** sarà disponibile solo se la directory di installazione del Server non contiene i file di configurazione di un'installazione precedente.

Impostare i seguenti parametri della connessione al server proxy:

- **Indirizzo del server proxy** — l'indirizzo IP o il nome DNS del server proxy (è un campo obbligatorio),
  - **Nome utente, Password** — il nome utente e la password per l'accesso al server proxy se il server proxy supporta la connessione con l'autenticazione.
  - Dalla lista a cascata **Metodo di autenticazione** selezionare il richiesto metodo di autenticazione sul server proxy se il server proxy supporta la connessione con l'autenticazione.
9. Se il computer su cui viene installato il Server fa parte di un dominio Active Directory, nella finestra successiva verrà offerto di registrare il Server Dr.Web nel dominio Active Directory. Nel corso della registrazione nel dominio Active Directory, sul server DNS viene creato un



record SRV corrispondente al Server Dr.Web. In seguito i client possono accedere al Server Dr.Web attraverso questo record SRV.

Per la registrazione, impostare i seguenti parametri:

- Spuntare il flag **Registra il Server Dr.Web in Active Directory**.
  - Nel campo **Dominio** indicare il nome del dominio Active Directory in cui verrà registrato il Server. Se nessun dominio è indicato, viene utilizzato il dominio in cui è registrato il computer su cui viene eseguita l'installazione.
  - Nei campi **Nome utente** e **Password** indicare le credenziali dell'amministratore del dominio Active Directory.
  - Gli indirizzi di **Server DNS** vengono inseriti automaticamente e il loro numero dipende dai server DNS impostati.
10. Se nel passaggio 3 è stata selezionata l'opzione **Crea una nuova configurazione**, si aprirà la finestra **Password dell'amministratore**. Impostare la password dell'amministratore della rete antivirus, creato di default con il nome utente **admin** e con i completi permessi di gestione della rete antivirus.

Per gli altri tipi di installazione la password dell'amministratore principale verrà presa dal database della installazione precedente del Server.

11. Nella finestra successiva la Procedura guidata informa che è pronta a installare il Server Dr.Web. Se necessario, si possono configurare parametri di installazione aggiuntivi. Per farlo, premere la voce **Avanzate** nella parte inferiore della finestra e configurare le seguenti impostazioni:

- Nella scheda **Generali**:
  - Dalla lista a cascata **Lingua dell'interfaccia del Pannello di controllo della sicurezza Dr.Web** scegliere la lingua predefinita dell'interfaccia di Pannello di controllo della sicurezza Dr.Web.
  - Dalla lista a cascata **Lingua dell'interfaccia di Agent Dr.Web** scegliere la lingua predefinita dell'interfaccia di Agent Dr.Web e dei componenti del pacchetto antivirus che vengono installati su postazioni.
  - Spuntare il flag **Condividi la directory di installazione di Agent Dr.Web** per modificare la modalità di utilizzo e il nome della risorsa condivisa per la directory di installazione di Agent Dr.Web (di default viene impostato il nome nascosto della risorsa condivisa).
  - Spuntare il flag **Avvia Server Dr.Web dopo la fine dell'installazione** per avviare il Server Dr.Web automaticamente dopo l'installazione.
  - Spuntare il flag **Aggiorna repository dopo la fine dell'installazione** per aggiornare automaticamente il repository di Server Dr.Web subito dopo il completamento dell'installazione.
  - Spuntare il flag **Limita l'accesso a Server Dr.Web**, per limitare l'accesso locale al Server. L'accesso verrà negato per gli installer di Agent Dr.Web, gli Agent Dr.Web e gli altri Server (nel caso di una rete antivirus già esistente costruita tramite Dr.Web Enterprise Security Suite). In seguito, queste impostazioni potranno essere modificate



tramite il menu del Pannello di controllo **Amministrazione**, voce **Configurazione del Server Dr.Web**, scheda **Moduli**.

- Spuntare il flag **Invia le statistiche all'azienda Doctor Web** per consentire l'invio delle statistiche di eventi di virus a Doctor Web.
- Nella scheda **Percorso**:
  - Nel campo **Directory di installazione di Server Dr.Web** viene impostata la directory in cui viene installato il Server Dr.Web. Per modificare la directory predefinita, premere il pulsante **Sfoglia** e selezionare la directory richiesta.
  - Nel campo **Directory per il backup di Server Dr.Web** viene impostata la directory in cui verranno salvati i backup dei dati critici del Server Dr.Web secondo il calendario dei task del Server. Per modificare la directory predefinita, premere il pulsante **Sfoglia** e selezionare la directory richiesta.
- Nella scheda **Log** è possibile configurare le impostazioni del log di funzionamento di Server Dr.Web.

Dopo aver finito di configurare i componenti aggiuntivi, premere il pulsante **OK** per accettare le modifiche apportate o il pulsante **Annulla** se nessuna modifica è stata apportata o per rifiutare le modifiche apportate.

12. Premere il pulsante **Installa** per iniziare il processo di installazione. Le azioni successive del programma di installazione non richiedono l'intervento dell'utente.

13. Dopo il completamento dell'installazione, premere il pulsante **Finito**.

Generalmente, il Server Dr.Web viene gestito tramite il Pannello di controllo che funge da interfaccia esterna per il Server Dr.Web.

Durante l'installazione di Server Dr.Web nel menu principale di SO Windows **Programmi** viene collocata la directory **Dr.Web Server** contenente i seguenti elementi che consentono di effettuare la configurazione e la gestione di base del Server Dr.Web:

- La directory **Gestione del server** contiene i comandi di avvio, riavvio e arresto di Server Dr.Web, nonché i comandi di configurazione del log e altri comandi di Server Dr.Web descritti in modo più dettagliato in documento **Allegati**, [G3. Server Dr.Web](#).
- La voce **Interfaccia web** — per aprire il Pannello di controllo e connettersi al Server Dr.Web installato su questo computer (sull'indirizzo <https://localhost:9081>).
- La voce **Documentazione** — per aprire la documentazione dell'amministratore in formato HTML.

La struttura della directory di installazione di Server Dr.Web è descritta in **Manuale dell'amministratore**, sezione [Server Dr.Web](#).

## 5.1.2. Installazione di Server Dr.Web per SO della famiglia UNIX



Tutte le azioni di installazione devono essere eseguite dalla console dall'account di superutente (**root**).



## Per installare il Server Dr.Web per i SO della famiglia UNIX

1. Per avviare l'installazione del pacchetto Server Dr.Web, eseguire il seguente comando:

```
./<file_del_pacchetto>.tar.gz.run
```



Per eseguire il pacchetto di installazione, è possibile utilizzare le opzioni della riga di comando. I parametri del comando di esecuzione sono riportati in documento **Allegati, G6. Installer di Server Dr.Web per SO della famiglia UNIX.**

---

Il nome dell'amministratore della rete antivirus predefinito è **admin**.

2. In seguito viene riportato il testo del contratto di licenza. Per continuare l'installazione, si deve accettare il contratto di licenza.
3. Per utilizzare le impostazioni di un'installazione precedente salvate in un backup, indicare il percorso della directory in cui è archiviato il backup (o premere il tasto INVIO per utilizzare la directory di default — /var/tmp/drwcs). Per installare Server Dr.Web senza utilizzare le impostazioni precedenti, inserire 0.
4. Se nel sistema è stato rilevato un pacchetto supplementare (extra), verranno visualizzate le informazioni sulla necessità di rimuovere il pacchetto supplementare prima di iniziare a installare il pacchetto Server Dr.Web. Non è possibile continuare l'installazione senza rimuovere il pacchetto supplementare.
5. In seguito viene eseguita l'installazione del software durante la quale il programma di installazione potrebbe richiedere di confermare le proprie azioni sotto l'account dell'amministratore.
6. Durante l'installazione viene generata una password casuale per l'amministratore principale. Dopo il completamento dell'installazione questa password viene restituita attraverso la console nei risultati dell'installazione del Server Dr.Web.



Durante l'installazione del software sotto SO **FreeBSD** viene creato uno script `rc /usr/local/etc/rc.d/drwcsd`.

Utilizzare i comandi:

- `/usr/local/etc/rc.d/drwcsd stop` — per l'arresto manuale del Server Dr.Web;
- `/usr/local/etc/rc.d/drwcsd start` — per l'avvio manuale del Server Dr.Web.



Notare che durante l'installazione del Server Dr.Web non viene impostata la chiave di licenza. Le chiavi di licenza devono essere aggiunte dopo l'installazione del Server Dr.Web attraverso [Gestione licenze](#).



## Configurazione di Astra Linux versione 1.6 per l'installazione di Server Dr.Web in modalità ambiente software chiuso

Nel caso di installazione di Server Dr.Web nell'ambiente del sistema operativo Astra Linux versione 1.6 in modalità ambiente software chiuso, può essere rifiutato l'avvio del programma di installazione a causa di assenza della chiave di cifratura pubblica di Server Dr.Web nella lista delle chiavi affidabili. In questo caso è necessario riconfigurare la modalità ambiente software chiuso, dopodiché avviare di nuovo il programma di installazione.

### Per riconfigurare la modalità ambiente software chiuso

1. Installare il pacchetto `astra-digsig-oldkeys` dal disco di installazione del sistema operativo, se non è ancora installato.
2. Collocare la chiave di cifratura pubblica di Server Dr.Web nella directory `/etc/digsig/keys/legacy/keys` (se la directory è mancante, deve essere creata).
3. Eseguire il seguente comando:

```
# update-initramfs -k all -u
```

4. Riavvia il sistema.

## Configurazione di Astra Linux Special Edition con PostgreSQL in caso di uso di livelli di accesso vincolati

Per configurare PostgreSQL per il funzionamento con la considerazione di privilegi di accesso vincolati, nel file `/etc/postgresql/<versione_database>/main/postgresql.conf` impostare il valore del parametro `ac_ignore_socket_maclabel` a `false`. Dopo l'impostazione del parametro, il server di DBMS controllerà il flag di sicurezza della connessione in entrata e trasmetterà solo le informazioni con un flag non superiore al flag della connessione in entrata.

```
ac_ignore_socket_maclabel = false
```

## 5.2. Installazione di Agent Dr.Web



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

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).



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.

### Agent Dr.Web può essere installato su una postazione in uno dei seguenti modi:

#### 1. [Localmente](#).

L'installazione locale di Agent Dr.Web viene eseguita direttamente sul computer o sul dispositivo mobile dell'utente. Può essere eseguita sia dall'amministratore che dall'utente.

#### 2. [In remoto](#).

L'installazione remota viene eseguita nel Pannello di controllo attraverso la rete locale. Viene eseguita dall'amministratore della rete antivirus. L'intervento dell'utente in tale caso non è richiesto.

### Installazione di Agent Dr.Web sopra il prodotto antivirus Dr.Web standalone per le postazioni SO Windows

In presenza sulla postazione SO Windows di un prodotto standalone Dr.Web versione 7.x-12.x, l'installazione di Agent Dr.Web per Dr.Web Enterprise Security Suite versione 13.0 avviene secondo il seguente schema:

- Se l'installer o il pacchetto di installazione di Agent Dr.Web viene avviato in modalità GUI su una postazione con un prodotto standalone installato versione 7.x-12.x, verrà avviato l'installer del prodotto installato. Quindi all'utente verrà chiesto di immettere il codice di conferma delle azioni e rimuovere il prodotto. Dopo il riavvio del sistema operativo verrà avviata la versione GUI dell'installer che è stato avviato inizialmente per l'installazione di Agent Dr.Web per Dr.Web Enterprise Security Suite versione 13.0.
- Se l'installer di Agent Dr.Web viene avviato in modalità background su una postazione con un prodotto standalone installato versione 7.x-12.x, questo non porterà all'esecuzione di alcuna azione. In caso di [installazione remota](#), l'installer restituirà al Pannello di controllo un messaggio sulla presenza di prodotti standalone di versioni precedenti. In tale caso, è necessario rimuovere manualmente il prodotto standalone e installare Agent Dr.Web per Dr.Web Enterprise Security Suite versione 13.0 in qualsiasi dei modi possibili.
- Se l'installer di Agent Dr.Web in caso di installazione sia locale che remota viene avviato su una postazione con un prodotto standalone versione 13.0 installato, la modalità del prodotto installato verrà cambiata da standalone a protezione centralizzata. Dopo la connessione e l'autenticazione sul Server Dr.Web possono essere ricevuti aggiornamenti, nuove impostazioni e una lista di componenti da installare a seconda di cui può essere richiesto un riavvio del computer.



### Quando gli Agent Dr.Web vengono installati sui server della LAN e sui computer del cluster, si deve tenere presente che:

- Nel caso di installazione su computer che svolgono il ruolo di terminal server (in SO Windows sono installati i servizi **Terminal Services**), per assicurare il funzionamento degli Agent Dr.Web nelle sessioni utente terminale, si consiglia di eseguire l'installazione degli Agent Dr.Web localmente tramite la procedura guidata di installazione e di eliminazione dei programmi nel **Pannello di controllo** SO Windows. L'installazione remota in questo caso può portare a errori nel funzionamento del protocollo Remote Desktop.
- Sui server che svolgono le funzioni di rete critiche (controller di dominio, server di distribuzione licenze ecc.) non è consigliabile installare i componenti SpIDer Gate, Office control, SpIDer Mail e Firewall Dr.Web per evitare eventuali conflitti dei servizi di rete e dei componenti interni dell'antivirus Dr.Web.
- L'installazione di Agent Dr.Web su cluster deve essere eseguita separatamente su ciascun nodo del cluster.
- I principi di funzionamento di Agent Dr.Web e dei componenti del pacchetto antivirus su un nodo del cluster sono analoghi a quelli su un server LAN normale, pertanto, non è consigliabile installare sui nodi del cluster i componenti SpIDer Gate, SpIDer Mail e Firewall Dr.Web.
- Se l'accesso alla risorsa quorum del cluster è strettamente limitato, si consiglia di escluderla dal controllo tramite il monitor SpIDer Guard e limitarsi a controlli regolari della risorsa tramite Scanner avviato in modo programmato o manuale.

## 5.2.1. File di installazione

### Pacchetti di installazione

#### Pacchetto di installazione individuale

Quando viene creato un nuovo account di postazione, nel Pannello di controllo viene generato un pacchetto di installazione individuale per l'installazione di Agent Dr.Web. Il pacchetto di installazione individuale include l'installer di Agent Dr.Web e un set di parametri per la connessione e l'autenticazione della postazione su Server Dr.Web.

I pacchetti di installazione individuali sono disponibili per le postazioni protette con tutti i sistemi operativi supportati da Dr.Web Enterprise Security Suite. I pacchetti di installazione individuali vengono generati nel Pannello di controllo sulla base di [installer](#) di Agent Dr.Web. I parametri di connessione e autenticazione della postazione sul Server Dr.Web sono inclusi direttamente nel pacchetto di installazione individuale.



Per ottenere i pacchetti di installazione individuali per i sistemi operativi diversi da SO Windows, dopo l'installazione di Server Dr.Web è necessario scaricare i prodotti aziendali



Dr.Web corrispondenti dai server SAM nel repository.

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

Un link per il download del pacchetto di installazione individuale di Agent Dr.Web per una determinata postazione è disponibile:

1. Subito dopo la creazione di una nuova postazione (v. passaggio **11** nella sezione [Creazione del nuovo account di postazione](#)).
2. In qualsiasi momento dopo la creazione di una postazione:
  - nella sezione delle proprietà della postazione,
  - nella sezione **Oggetti selezionati** quando la postazione viene selezionata nella lista gerarchica.

## Pacchetto di installazione di gruppo

Il pacchetto di installazione di gruppo di Agent Dr.Web viene generato nel Pannello di controllo per l'installazione sulle postazioni di un determinato gruppo custom. In tale caso è prevista l'installazione di Agent Dr.Web su tutte le postazioni con lo stesso SO dallo stesso pacchetto di installazione di gruppo.

Il pacchetto di installazione di gruppo include l'installer di Agent Dr.Web, i parametri di connessione al Server Dr.Web, nonché l'identificatore e la password del gruppo custom in cui verrà inclusa la postazione dopo l'installazione di Agent Dr.Web. Tuttavia, i parametri di autenticazione della postazione sul Server Dr.Web e i componenti antivirus stessi non fanno parte del pacchetto di installazione di gruppo.

Un link per il download del pacchetto di installazione di gruppo è disponibile nella sezione delle proprietà del gruppo custom.

## Installer

L'installer di Agent Dr.Web è diverso dal pacchetto di installazione in quanto non include i parametri di connessione e autenticazione della postazione sul Server Dr.Web.

Sono disponibili i seguenti installer di Agent Dr.Web:

- Per le postazioni SO Windows sono disponibili due tipi di installer:
  - *L'installer di rete* `drwinst.exe` installa direttamente l'Agent Dr.Web. Dopo essere stato connesso al Server Dr.Web, l'Agent Dr.Web scarica e installa i componenti necessari del pacchetto antivirus. È possibile sia l'installazione locale che quella remota di Agent tramite l'installer di rete.  
L'installer di rete di Agent Dr.Web `drwinst.exe` si trova nella directory `webmin/install/windows` (di default è una risorsa condivisa nascosta) della directory



di installazione di Server Dr.Web. L'accessibilità via rete della risorsa viene configurata al [passaggio 12](#) dell'installazione di Server Dr.Web. In seguito, è possibile modificare questa risorsa a propria discrezione.

- *L'installer completo* `drweb-<versione_agent>-<build>-esuite-agent-full-windows.exe` installa contemporaneamente l'Agent Dr.Web e il pacchetto antivirus.
- Per le postazioni SO Android, Linux, macOS è disponibile un installer di Agent Dr.Web simile all'installer della versione standalone.

Gli installer per l'installazione di Agent Dr.Web sono disponibili sulla [pagina di installazione](#) del Pannello di controllo della sicurezza Dr.Web.



Per ottenere gli installer per i sistemi operativi diversi da SO Windows, nonché il pacchetto completo dell'installer per SO Windows, dopo l'installazione di Server Dr.Web è necessario scaricare i prodotti aziendali Dr.Web corrispondenti dai server SAM nel repository.

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

## Pagina di installazione

Subito dopo l'installazione di Server Dr.Web, sulla pagina di installazione del Pannello di controllo della sicurezza Dr.Web è possibile scaricare:

1. Installer di Agent Dr.Web per Windows.
2. Certificato di Server Dr.Web `drwcsd-certificate.pem`.

Dopo che si effettua una [piccola configurazione](#), sulla pagina sarà inoltre disponibile una serie di installer aggiuntivi. Gli installer per postazioni protette sotto tutti i sistemi operativi supportati da Dr.Web Enterprise Security Suite si trovano nelle directory con i nomi corrispondenti al nome del sistema operativo.

La pagina di installazione è disponibile su qualsiasi computer che abbia l'accesso di rete al Server Dr.Web, sull'indirizzo:

```
http://<Indirizzo_Server_Dr.Web>:<numero_porta>/install/
```

dove come `<Indirizzo_Server_Dr.Web>` indicare l'indirizzo IP o il nome a dominio del computer su cui è installato il Server Dr.Web. Come `<numero_porta>` indicare il numero di porta 9080 (o 9081 per https).

### Per configurare la lista dei prodotti disponibili sulla pagina di installazione

1. Selezionare la voce **Amministrazione** nel menu principale, dopodiché nel menu di gestione selezionare la sezione **Configurazione generale del repository**.
2. Andare alla scheda **Pacchetti di installazione Dr.Web** → **Prodotti aziendali Dr.Web**.



3. Fare clic sulla freccia a sinistra del nome del prodotto richiesto e precisare il sistema operativo e il numero di bit. Dopo aver spuntato i flag di fronte a tutti i prodotti necessari, premere **Salva**.
4. Aggiornare il repository attraverso la sezione **Stato del repository** nel menu di gestione.
5. Dopo il caricamento da SAM e l'aggiornamento del repository sulla pagina di installazione saranno disponibili gli installer dei prodotti selezionati.

## 5.2.2. Installazione locale di Agent Dr.Web

L'installazione locale di Agent Dr.Web viene eseguita direttamente sul computer o sul dispositivo mobile dell'utente. Può essere eseguita sia dall'amministratore che dall'utente.



Prima della prima installazione degli Agent Dr.Web, è necessario aggiornare il repository di Server Dr.Web (v. **Manuale dell'amministratore**, p. [Aggiornamento del repository di Server Dr.Web manualmente](#), p. **Verifica disponibilità aggiornamenti**).

### Postazioni SO Android, SO Linux, macOS

Per l'installazione locale di Agent Dr.Web sulle postazioni Android, Linux, macOS sono disponibili i seguenti strumenti:

- [Pacchetto di installazione individuale](#) creato nel Pannello di controllo.
- [Pacchetto di installazione di gruppo](#) creato nel Pannello di controllo.
- [Installer di](#) Agent Dr.Web.

Scegliendo il tipo di pacchetto da installare, prestare attenzione alle seguenti caratteristiche:

- a) In caso di creazione del pacchetto di installazione individuale, sono forniti l'installer di Agent Dr.Web, nonché i parametri di connessione al Server Dr.Web e i parametri di autenticazione della postazione sul Server Dr.Web.
- b) In caso di installazione di Agent Dr.Web tramite l'installer, i parametri di connessione al Server Dr.Web e i parametri di autenticazione della postazione sul Server Dr.Web non sono forniti.

### Postazioni SO Windows

Per l'installazione locale di Agent Dr.Web sulle postazioni SO Windows sono disponibili i seguenti strumenti:

- [Pacchetto di installazione individuale](#) creato nel Pannello di controllo  
`drweb_es_<SO>_<postazione>.exe`.
- [Pacchetto di installazione di gruppo](#) creato nel Pannello di controllo  
`drweb_es_<SO>_<gruppo>.exe`.
- [Installer completo](#) di Agent Dr.Web `drweb-<versione_agent>-<build>-esuite-agent-full-windows.exe`.



- [Installer di rete](#) di Agent Dr.Web `drwinst.exe`.

Scegliendo il tipo di pacchetto da installare, prestare attenzione alle seguenti caratteristiche:

- In caso di installazione dal pacchetto di installazione individuale, i parametri di connessione al Server Dr.Web e i parametri di autenticazione della postazione sul Server Dr.Web sono inclusi nel pacchetto di installazione individuale. L'installazione tramite il pacchetto di installazione individuale viene eseguita sulla base dell'installer di rete da cui viene installato direttamente l'Agent Dr.Web. Dopo essere stato connesso al Server Dr.Web, l'Agent Dr.Web scarica e installa i componenti del pacchetto antivirus.
- In caso di installazione dal pacchetto di installazione di gruppo, i parametri di connessione al Server Dr.Web, nonché l'identificatore e la password del gruppo custom in cui verrà inclusa la postazione dopo l'installazione di Agent Dr.Web, fanno parte del pacchetto di installazione. Tuttavia, i parametri di autenticazione della postazione sul Server Dr.Web e i componenti antivirus stessi non sono inclusi nel pacchetto di installazione di gruppo. Dopo l'installazione di Agent Dr.Web viene eseguita la connessione di Agent Dr.Web a Server Dr.Web nel processo della quale viene determinata la presenza di postazioni libere nel gruppo custom di cui il pacchetto di installazione di gruppo è stato utilizzato. Se sono disponibili postazioni libere, i parametri di autenticazione della postazione sul Server Dr.Web vengono forniti automaticamente.
- In caso di installazione tramite l'installer di rete, solo l'Agent viene installato. Dopo essere stato connesso al Server Dr.Web, l'Agent Dr.Web scarica e installa i componenti corrispondenti del pacchetto antivirus. I parametri di connessione al Server Dr.Web e i parametri di autenticazione della postazione sul Server Dr.Web non vengono forniti.
- In caso di installazione tramite il pacchetto completo, vengono installati contemporaneamente l'Agent Dr.Web e il pacchetto antivirus. I parametri di connessione al Server Dr.Web e i parametri di autenticazione della postazione sul Server Dr.Web non vengono forniti.

### Caratteristiche comparative dei file di installazione

File di installazione		Installazione di Agent Dr.Web	Installazione del pacchetto antivirus	Parametri di connessione al Server Dr.Web	Parametri di autenticazione sul Server Dr.Web
Pacchetto di installazione	Individuale	+	-	+	+
	Di gruppo	+	-	+	-
Installer	Di rete	+	-	-	-
	Completo	+	+	-	-



Per ottenere gli installer e i pacchetti di installazione per sistemi operativi diversi da SO Windows, nonché il pacchetto completo dell'installer per SO Windows, è necessario scaricare i **Prodotti aziendali Dr.Web** nel repository dai server SAM in aggiunta dopo l'installazione di Server Dr.Web.

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



Inoltre, è possibile eseguire tutti i tipi di file di installazione di Agent Dr.Web dalla riga di comando con utilizzo delle opzioni riportate in documento **Allegati**, [G1. Installer di rete](#).

### 5.2.2.1. Installazione di Agent Dr.Web attraverso il pacchetto di installazione individuale

#### Per installare Agent Dr.Web sulle postazioni protette attraverso il pacchetto di installazione individuale

1. Tramite il Pannello di controllo [creare un account](#) di nuova postazione sul Server Dr.Web.
2. Inviare all'utente il link del pacchetto di installazione di Agent Dr.Web individuale per il sistema operativo corrispondente del computer o del dispositivo mobile, se il software Agent Dr.Web verrà installato dall'utente in autonomo.



Per il più comodo trasferimento del file di installazione e del file di configurazione, è possibile utilizzare la funzione **Invio dei file di installazione** (maggiori informazioni sono riportate nel **Manuale dell'amministratore**, p. [Invio dei file di installazione](#)) per inviare email con i file corrispondenti.

3. Installare Agent Dr.Web sulla postazione.



L'installazione locale di Agent Dr.Web su postazioni è descritta nel **Manuale dell'utente** per il sistema operativo corrispondente.



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

---

Se sulla postazione è già installato un software antivirus, il pacchetto di installazione individuale cercherà di rimuoverlo prima di iniziare l'installazione. Se tale tentativo non va a buon fine, l'utente dovrà rimuovere il software antivirus utilizzato sulla postazione.

4. Per le postazioni macOS [configurare i parametri di connessione](#) al Server Dr.Web localmente.



Nel caso di installazione di Agent Dr.Web tramite un pacchetto di installazione individuale per altri sistemi supportati, non è richiesta alcuna configurazione aggiuntiva. I parametri di connessione al Server Dr.Web e i parametri di autenticazione della postazione sul Server Dr.Web sono inclusi direttamente nel pacchetto di installazione individuale. Dopo che Agent Dr.Web viene installato, la postazione si conetterà al Server Dr.Web in modo automatico.

## Creazione del nuovo account di postazione

Per creare uno o più account di nuove postazioni, utilizzare il Pannello di controllo della sicurezza Dr.Web.



Quando si crea un account di postazione, prestare attenzione al nome di Server Dr.Web impostato nelle seguenti sezioni del Pannello di controllo:

1. **Amministrazione** → **Configurazione del web server** → campo **Indirizzo di Server Dr.Web**. Il valore di questo parametro viene utilizzato nel generare il link del pacchetto di installazione di Agent Dr.Web.

Se il valore di questo parametro non è impostato in nessun posto, come nome di Server Dr.Web per la generazione del link al download del pacchetto di installazione individuale di Agent Dr.Web viene impostato il nome DNS (se disponibile) o l'indirizzo IP del computer su cui è aperto il Pannello di controllo.

2. **Amministrazione** → **Configurazione del Server Dr.Web** → Scheda **Rete** → scheda **Download** → campo **Indirizzo di Server Dr.Web**. Il valore di questo parametro viene trascritto nei pacchetti di installazione di Agent Dr.Web e determina a quale Server Dr.Web si conetterà l'Agent Dr.Web dopo l'installazione.

Se il valore di questo parametro non è impostato in nessun posto, nel corso della creazione del pacchetto di installazione di Agent Dr.Web, in esso viene trascritto l'indirizzo di Server Dr.Web su cui è connesso il Pannello di controllo. In questo caso, la connessione del Pannello di controllo al Server Dr.Web deve essere effettuata sull'indirizzo IP per il dominio in cui viene creato l'account (l'indirizzo di Server Dr.Web non deve essere impostato come loopback — 127.0.0.1).

### Per creare un nuovo account di postazione tramite il Pannello di controllo della sicurezza Dr.Web

1. Selezionare la voce **Rete antivirus** nel menu principale del Pannello di controllo.
2. Nella barra degli strumenti premere il pulsante **+ Aggiungi oggetto della rete** → **+ Crea postazione**. Nella parte destra della finestra del Pannello di controllo si apre la barra di creazione di un account postazione.
3. Nel campo **Numero** indicare il numero di account che si vuole creare.
4. Nel campo **Identificatore** viene generato automaticamente l'identificatore univoco della postazione che viene creata. Se necessario, è possibile modificarlo.
5. Nel campo **Nome** impostare il nome di postazione che verrà visualizzato nella lista gerarchica della rete antivirus. In seguito, dopo che la postazione si connette al Server



Dr.Web, questo nome può essere sostituito automaticamente con il nome impostato localmente sulla postazione.

6. Nei campi **Password** e **Confermare la password** è possibile impostare una password di accesso della postazione al Server Dr.Web. Se la password non è indicata, verrà generata automaticamente.



Quando vengono creati più di un account, i campi **Identificatore**, **Nome** e **Password** (**Confermare la password**) verranno impostati automaticamente e non possono essere modificati durante la creazione di postazioni.

7. Nel campo **Descrizione** inserire informazioni supplementari sulla postazione. Questo parametro non è obbligatorio.
8. Nella sezione **Gruppi** vengono impostati i gruppi di cui farà parte la postazione che viene creata.
  - Nella lista **Appartenenza** si può configurare una lista di gruppi custom di cui farà parte la postazione.

Di default, la postazione fa parte del gruppo **Everyone**. Se ci sono gruppi personalizzati, è possibile includere in essi la postazione che viene creata, senza limitazioni al numero di gruppi in cui è inclusa la postazione. Per farlo, premere **Modifica** , spuntare i flag di fronte ai gruppi personalizzati desiderati nella lista **Appartenenza** e premere **Applica**.



Non si può escludere la postazione dal gruppo **Everyone** e dal gruppo primario.

Per impostare il gruppo primario per la postazione che viene creata, premere sull'icona del gruppo desiderato nella sezione **Appartenenza**. In questo caso sull'icona del gruppo appare **1**.

- Nella lista **Criterio** è possibile impostare un criterio da cui verranno prese le impostazioni della postazione che viene creata.

La lista viene visualizzata se nella sezione **Amministrazione** → **Configurazione del Server Dr.Web** sulla scheda **Generali** è spuntato il flag **Usa criteri**.

Di default, nessun criterio è assegnato. Per assegnare un criterio, premere , spuntare il flag di fronte al criterio richiesto e premere **Applica**. La postazione eredita le impostazioni dalla versione corrente di questo criterio. Non è possibile assegnare più di un criterio a una postazione.

- Nella lista **Profilo** è possibile impostare un profilo del componente Controllo delle applicazioni, il quale verrà applicato alla postazione che viene creata.

Di default il profilo viene ereditato dal gruppo padre della postazione. Per selezionare un profilo per la postazione, premere **Modifica** , spuntare il flag di fronte al profilo richiesto e premere **Applica**. A una postazione possono essere assegnati più profili.

9. Nella sezione **Server proxy Dr.Web** vengono configurate le impostazioni del Server proxy Dr.Web associato a questa postazione.



Se si vuole installare un Server proxy sulla postazione che viene creata, spuntare il flag **Crea Server proxy Dr.Web associato** e impostare i parametri del Server proxy Dr.Web. I parametri sono analoghi ai parametri di [creazione del Server proxy Dr.Web](#).



Durante la creazione dell'account di postazione verrà creato un account di Server proxy Dr.Web nel Pannello di controllo. Dopo la trasmissione delle impostazioni alla postazione il Server proxy Dr.Web verrà installato su questa postazione in modalità background. L'Agent Dr.Web si conetterà al Server Dr.Web solo attraverso il Server proxy Dr.Web installato. L'uso del Server proxy Dr.Web sarà trasparente per l'utente.

10. Se necessario, compilare la sezione **Sicurezza**. La descrizione delle impostazioni di questa sezione è riportata nel **Manuale dell'amministratore** sezione [Sicurezza](#).
11. Se necessario, compilare la sezione **Posizione**.
12. Premere il pulsante **Salva** nell'angolo superiore destro. Si apre una finestra che informa che la nuova postazione è stata creata e che inoltre riporta il numero di identificazione e i seguenti link:
  - Nella voce **File di installazione** — un link per il download del pacchetto di installazione individuale di Agent Dr.Web.
  - Nella voce **File di configurazione** — un link per il download del file con le impostazioni di connessione al Server Dr.Web per le postazioni con Android, macOS e SO Linux.



Subito dopo la creazione della nuova postazione fino al momento quando verrà impostato il sistema operativo della postazione, nella sezione download del pacchetto vengono forniti separatamente i link per tutti i sistemi operativi supportati da Dr.Web Enterprise Security Suite.

---

I link per il download del pacchetto di installazione individuale di Agent Dr.Web e del file di configurazione sono inoltre disponibili:

- nelle proprietà della postazione dopo la creazione,
- nella sezione **Oggetti selezionati** quando la postazione creata viene selezionata nella lista gerarchica.

---

Per ottenere i pacchetti di installazione individuali per i sistemi operativi diversi da SO Windows, dopo l'installazione di Server Dr.Web è necessario scaricare i prodotti aziendali Dr.Web corrispondenti dai server SAM nel repository.

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

- Nella voce **Password** viene riportata la password di accesso di questa postazione al Server Dr.Web. Per visualizzare la password, premere
- Nella voce **Password del Server proxy** è riportata la password di accesso del Server proxy Dr.Web al Server Dr.Web, se la postazione veniva creata con un Server proxy Dr.Web associato (v. passaggio 9).



- Il pulsante **Installa** è progettato per l'[installazione remota di Agent Dr.Web tramite il Pannello di controllo della sicurezza Dr.Web](#).
13. Le azioni di installazione di Agent Dr.Web su postazione sono riportate nel **Manuale dell'utente** per il sistema operativo corrispondente.

## Impostazioni di connessione al Server Dr.Web per la postazione macOS

1. Nel menu dell'applicazione Antivirus Dr.Web premere la voce **Preferenze** e selezionare la sezione **Modalità**.
2. Spuntare il flag **Attiva la modalità di protezione centralizzata**.
3. Le impostazioni di connessione al Server Dr.Web, quali l'indirizzo IP e i parametri di autenticazione sul Server Dr.Web, vengono definite automaticamente dal file di configurazione `install.cfg` situato all'interno del pacchetto di installazione individuale.  
Per utilizzare il file:
  - a) Nella Gestione licenze premere sul link **Altri tipi di attivazione**.
  - b) Trascinare il file di configurazione nella finestra che si è aperta o fare clic sull'area circondata da linea punteggiata per aprire una finestra per selezionare il file.Dopo la connessione del file i campi di inserimento dei parametri di connessione al Server Dr.Web verranno compilati automaticamente.

### 5.2.2.2. Installazione di Agent Dr.Web attraverso il pacchetto di installazione di gruppo

#### Per installare Agent Dr.Web sulle postazioni protette attraverso il pacchetto di installazione di gruppo

1. Attraverso il Pannello di controllo creare un nuovo gruppo custom sul Server Dr.Web (una descrizione dettagliata della procedura di creazione gruppi è riportata nel **Manuale dell'amministratore**, p. [Creazione ed eliminazione di gruppi](#)). Inoltre, si può utilizzare un gruppo già disponibile, creato in precedenza.
2. Se necessario, nella Gestione licenze assegnare al gruppo una chiave di licenza individuale. Altrimenti, il gruppo erediterà la chiave di licenza dal suo gruppo padre.
3. Attraverso il Pannello di controllo [creare account](#) di nuove postazioni sul Server Dr.Web. Includere i nuovi account di postazioni nel gruppo custom dal passaggio 1 e rendere questo gruppo primario per essi. In un gruppo custom è possibile creare tante postazioni, quante licenze sono disponibili per questo gruppo.
4. Nelle impostazioni del gruppo sarà disponibile un link di un pacchetto di installazione di gruppo. I pacchetti di installazione saranno divisi per sistema operativo: un pacchetto di installazione per ciascuno sistema operativo.
5. Inviare agli utenti il link del pacchetto di installazione di gruppo di Agent Dr.Web per il sistema operativo corrispondente del computer o del dispositivo mobile, se il software



Agent Dr.Web verrà installato dagli utenti in autonomo. A tutti gli utenti viene inviato lo stesso pacchetto di installazione di gruppo per il sistema operativo corrispondente.

6. Installare Agent Dr.Web sulla postazione.



L'installazione locale di Agent Dr.Web su postazioni è descritta nel **Manuale dell'utente** per il sistema operativo corrispondente.



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

Se sulla postazione è già installato un software antivirus, l'installer cercherà di rimuoverlo prima di iniziare l'installazione. Se tale tentativo non va a buon fine, l'utente dovrà rimuovere in autonomo il software antivirus utilizzato sulla postazione.

7. Dopo l'installazione dell'Agent Dr.Web, viene effettuata la connessione dell'Agent Dr.Web al Server Dr.Web indicato nel pacchetto di installazione di gruppo. Nel corso della prima connessione al Server Dr.Web viene determinata la presenza di postazioni libere nel gruppo custom di cui il pacchetto di installazione di gruppo è stato utilizzato per installare l'Agent Dr.Web. Il numero di postazioni libere viene determinato in base al numero di account in questo gruppo di cui il periodo di ammissione non è ancora scaduto. Ad ogni connessione del pacchetto di installazione di gruppo il numero di postazioni libere viene ricalcolato per fornire informazioni attuali.
- Se sono disponibili postazioni libere, i parametri di autenticazione della postazione per la connessione al Server Dr.Web vengono forniti automaticamente. Questa procedura viene eseguita in modo trasparente per l'amministratore e non richiede un intervento aggiuntivo.
  - Se non ci sono postazioni libere in questo gruppo, l'installazione viene interrotta con un relativo messaggio all'utente.

### 5.2.2.3. Installazione di Agent Dr.Web attraverso installer

A differenza del pacchetto di installazione, l'Installer di Agent Dr.Web non include i parametri di connessione al Server Dr.Web e i parametri di autenticazione della postazione sul Server Dr.Web.

Gli installer per l'installazione di Agent Dr.Web sono disponibili sulla [pagina di installazione](#) del Pannello di controllo della sicurezza Dr.Web.



Per ottenere gli installer per sistemi operativi diversi da SO Windows, nonché il pacchetto completo dell'installer per SO Windows, è necessario scaricare i **Prodotti aziendali Dr.Web** nel repository dai server SAM in aggiunta dopo l'installazione di Server Dr.Web.

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



## Installazione locale su postazioni Android, Linux, macOS

Per le postazioni SO Android, Linux, macOS è disponibile un installer di Agent Dr.Web simile all'installer della versione standalone.



L'installazione locale di Agent Dr.Web su postazioni è descritta nel **Manuale dell'utente** per il sistema operativo corrispondente.

Se il software viene installato attraverso l'installer senza il file di configurazione, è necessario indicare manualmente sulla postazione l'indirizzo del Server Dr.Web per la connessione della postazione.

I parametri di autenticazione possono essere impostati manualmente o si può omettere di impostarli. Sono possibili le seguenti varianti di connessione al Server Dr.Web:

Variante del task	Parametri di autenticazione
Viene impostato manualmente	La postazione cerca di autenticarsi automaticamente secondo i parametri di autenticazione impostati.
Non viene impostato	Il principio di autenticazione sul Server Dr.Web dipende dalle impostazioni del Server Dr.Web per la connessione di nuove postazioni (per maggiori informazioni v. <b>Manuale dell'amministratore</b> , p. <a href="#">Criteri di approvazione delle postazioni</a> ).



Per impostare i parametri di autenticazione manualmente, è necessario prima creare un nuovo account di postazione nel Pannello di controllo. In tale caso sarà disponibile un [pacchetto di installazione](#) che include un file di configurazione con i parametri di connessione e autenticazione. Si consiglia di utilizzare il pacchetto di installazione invece dell'installer.

## Installazione locale su postazioni SO Windows

Sono disponibili i seguenti tipi di installer di Agent Dr.Web:

- *l'installer di rete* `drwinst.exe` installa solo l'Agent Dr.Web. Dopo la connessione al Server Dr.Web, l'Agent Dr.Web scarica e installa i componenti corrispondenti del pacchetto antivirus.
- *l'installer completo* `drweb-<versione_agent>-<build>-esuite-agent-full-windows.exe` installa contemporaneamente l'Agent Dr.Web e il pacchetto antivirus.

Nelle installazioni attraverso questi installer è possibile non impostare i parametri di connessione al Server Dr.Web e di autenticazione o impostarli manualmente.



Per impostare i parametri di autenticazione manualmente, è necessario prima creare un nuovo account di postazione nel Pannello di controllo. In tale caso sarà disponibile un [pacchetto di installazione](#). Se non è necessario installare attraverso il pacchetto completo o l'installer di rete, si consiglia di utilizzare il pacchetto di installazione invece dell'installer.

Sono possibili le seguenti varianti di connessione al Server Dr.Web:

Variante del task	Indirizzo del Server Dr.Web	Parametri di autenticazione
Viene impostato manualmente	La postazione si connette direttamente al Server Dr.Web impostato.	La postazione cerca di autenticarsi automaticamente secondo i parametri di autenticazione impostati.
Non viene impostato	Agent Dr.Web cerca Server Dr.Web nella rete tramite il <i>Servizio di rilevamento di Server Dr.Web</i> . Viene effettuato un tentativo di connessione al primo Server Dr.Web trovato.	Il principio di autenticazione sul Server Dr.Web dipende dalle impostazioni del Server Dr.Web per la connessione di nuove postazioni (per maggiori informazioni v. <b>Manuale dell'amministratore</b> , p. <a href="#">Criteri di approvazione delle postazioni</a> ).



Nel **Manuale dell'utente** per SO Windows sono descritte le varianti di installazione di Agent Dr.Web tramite l'installer completo e tramite il pacchetto di installazione.

Si consiglia che l'installazione tramite l'installer di rete venga eseguita dall'amministratore della rete antivirus.

## Installazione locale tramite l'installer di rete in SO Windows

L'installer di rete di Agent Dr.Web `drwinst.exe` è fornito per l'installazione di Agent Dr.Web solo in SO Windows.

Se l'installer di rete viene avviato in modalità di installazione standard (cioè senza l'opzione `/instMode remove`) su una postazione su cui è già stata eseguita un'installazione, nessuna azione verrà eseguita. L'installer termina l'operazione e visualizza una finestra con la lista delle opzioni disponibili.

L'installazione tramite l'Installer di rete è disponibile in due modalità principali:

1. *Modalità background* — si avvia se è stata impostata l'opzione della modalità background.
2. *Modalità grafica* — la modalità predefinita. Si avvia se non è stata impostata l'opzione della modalità background.

Tramite l'installer di rete è inoltre possibile installare Agent Dr.Web su una postazione su remoto, utilizzando il Pannello di controllo (v. p. [Installazione remota di Agent Dr.Web](#)).



## Per installare Agent Dr.Web su una postazione in modalità background

1. Dal computer su cui verrà installato il software antivirus accedere alla directory di rete di installazione di Agent Dr.Web (nel caso di installazione di Server Dr.Web questa è la sottodirectory `webmin/install/windows` della directory di installazione di Server Dr.Web, in seguito può essere spostata) o scaricare dalla [pagina di installazione](#) del Pannello di controllo il file eseguibile dell'installer `drwinst.exe` e il certificato `drwcsd-certificate.pem`. Eseguire il file `drwinst.exe` con l'opzione di modalità background `/silent yes`.

Di default il file `drwinst.exe`, avviato senza i parametri di connessione al Server Dr.Web, utilizza la modalità *Multicast* per cercare nella rete i Server Dr.Web attivi e tenta di installare l'Agent Dr.Web dal primo Server Dr.Web trovato nella rete.



Quando viene utilizzata la modalità *Multicast* per la ricerca dei Server Dr.Web attivi, l'Agent Dr.Web verrà installato dal primo Server Dr.Web trovato. Se la chiave di cifratura pubblica disponibile non corrisponde alla chiave di cifratura del Server Dr.Web, l'installazione fallisce. In questo caso, indicare esplicitamente l'indirizzo del Server Dr.Web all'avvio dell'installer (v. sotto).

Se l'Agent Dr.Web deve essere installato sullo stesso computer su cui è installato Server Dr.Web, è necessario impostare direttamente l'indirizzo di Server Dr.Web nei parametri di avvio dell'installer in quanto Server Dr.Web può essere non rilevato tramite la ricerca attraverso una richiesta multicast.

Inoltre, il file `drwinst.exe` può essere avviato con parametri della riga di comando aggiuntivi:

- Nel caso in cui la modalità *Multicast* non viene utilizzata, all'installazione di Agent Dr.Web si consiglia di indicare esplicitamente il nome di Server Dr.Web (preventivamente registrato nel servizio DNS):

```
drwinst /silent yes /server <nome_DNS_Server_Dr.Web>
```



Come indirizzo di Server Dr.Web è consigliato utilizzare il nome di Server Dr.Web in formato FQDN, preventivamente registrato nel servizio DNS. Questo semplificherà il processo di configurazione della rete antivirus, relativo alla procedura di reinstallazione di Server Dr.Web su un altro computer. In tale caso, se verrà cambiato l'indirizzo di Server Dr.Web, sarà sufficiente modificarlo nelle impostazioni del server DNS per il nome del computer con Server Dr.Web in modo che tutti gli agent si connettano automaticamente al nuovo server.

1. Se nella rete funziona un server DNS locale, è necessario creare in esso un nome separato per Server Dr.Web, nonché per Server proxy Dr.Web (per esempio, `drwebes.company.lan`).
2. Nelle impostazioni di Agent Dr.Web, deve essere indicato il nome di Server Dr.Web in formato FQDN.



- Oltre al nome in formato FQDN, nelle impostazioni di Agent Dr.Web è consigliato aggiungere anche l'indirizzo di Server Dr.Web e mantenere aggiornato questo indirizzo in caso di sua modifica. In questo caso, se è impossibile utilizzare il nome di server, l'agent effettuerà il tentativo di connessione in base all'indirizzo di server.

- Inoltre, è possibile utilizzare l'indicazione esplicita dell'indirizzo di Server Dr.Web, per esempio:

```
drwinst /silent yes /server 192.168.1.3
```

- L'utilizzo dell'opzione `/regagent yes` consente di registrare nel corso dell'installazione l'Agent Dr.Web nella lista di aggiunta e rimozione dei programmi.



La lista completa dei parametri dell'Installer di rete è riportata in documento **Allegati, G1. Installer di rete.**

- Al termine del funzionamento dell'installer, sul computer verrà installato il software Agent Dr.Web (ma non il pacchetto antivirus).
- Dopo la conferma della postazione sul Server Dr.Web (se lo richiedono le impostazioni del Server Dr.Web), viene automaticamente installato il pacchetto antivirus.
- Riavviare il computer su richiesta di Agent Dr.Web.

### Per installare Agent Dr.Web su una postazione in modalità grafica

Dal computer su cui verrà installato il software antivirus accedere alla directory di rete di installazione di Agent Dr.Web (nel caso di installazione di Server Dr.Web questa è la sottodirectory `webmin/install/windows` della directory di installazione di Server Dr.Web, in seguito può essere spostata) o scaricare dalla [pagina di installazione](#) del Pannello di controllo il file eseguibile dell'installer `drwinst.exe` e il certificato `drwcsd-certificate.pem`. Eseguire il file `drwinst.exe`.

Si apre la finestra dell'installazione guidata di Agent Dr.Web. Le azioni successive di installazione di Agent Dr.Web su postazione in modalità grafica dell'installer di rete sono analoghe alle azioni di installazione tramite il pacchetto di installazione, ma senza le impostazioni di connessione al Server Dr.Web, se non sono state definite nella relativa opzione della riga di comando.



L'installazione di Agent Dr.Web su postazioni è descritta in manuale **Agent Dr.Web per Windows. Manuale dell'utente.**

### 5.2.3. Installazione remota di Agent Dr.Web

Dr.Web Enterprise Security Suite fornisce la possibilità di rilevare i computer su cui non è ancora installata la protezione antivirus Dr.Web Enterprise Security Suite, e in alcuni casi, di installare tale protezione in remoto.



L'installazione remota è possibile:

- [Tramite il Pannello di controllo.](#)
- [Con l'uso del servizio Active Directory](#), se nella rete locale protetta viene utilizzato questo servizio.



L'installazione remota di Agent Dr.Web è possibile solo su postazioni con SO Linux e SO della famiglia Windows (v. [Requisiti di sistema](#)), ad eccezione delle edizioni Starter e Home.

Per installare l'Agent Dr.Web in remoto su postazioni, è necessario avere i privilegi di amministratore delle postazioni corrispondenti.

### 5.2.3.1. Installazione di Agent Dr.Web con utilizzo del Pannello di controllo della sicurezza Dr.Web

- [Installazione remota di Agent Dr.Web per SO Windows](#)
- [Installazione remota di Agent Dr.Web per SO UNIX](#)

#### 5.2.3.1.1. Installazione remota di Agent Dr.Web per SO Windows

**Sono possibili i seguenti modi di installazione remota degli Agent Dr.Web sulle postazioni della rete:**

1. [Installazione tramite Scanner di rete.](#)

Consente di cercare prima dell'installazione i computer della rete che non sono protetti e di installare su di essi gli Agent Dr.Web.

2. [Installazione tramite lo strumento Installazione via rete.](#)

Questo metodo è adatto se si conosce in anticipo l'indirizzo della postazione o del gruppo di postazioni su cui verranno installati gli Agent Dr.Web.

3. [Installazione sulle postazioni con gli ID specificati.](#)

Consente di installare su postazioni o gruppi di postazioni gli Agent Dr.Web per gli account selezionati (anche per tutti i nuovi account presenti) con ID e password di accesso al Server Dr.Web specificati.



Per la corretta operatività di Scanner di rete e dello strumento **Installazione via rete** nel browser Windows Internet Explorer, l'indirizzo IP e/o il nome DNS del computer su cui è installato il Server Dr.Web devono essere aggiunti ai siti attendibili del browser in cui il Pannello di controllo viene aperto per l'installazione remota.



## Utilizzo di Scanner di rete

Nella lista gerarchica della rete antivirus nel Pannello di controllo vengono visualizzati i computer già inclusi nella rete antivirus. Dr.Web Enterprise Security Suite consente inoltre di rilevare i computer che non sono protetti tramite il software antivirus Dr.Web Enterprise Security Suite, e di installare i componenti antivirus su remoto.

Per installare velocemente il software Agent Dr.Web su postazioni, si consiglia di utilizzare Scanner di rete (v. **Manuale dell'amministratore**, p. [Scanner di rete](#)), il quale cerca computer per indirizzo IP.



L'installazione via rete è disponibile solo per gli amministratori con il permesso **Visualizzazione delle proprietà dei gruppi di postazioni**, concesso per tutta la rete antivirus (per maggiori informazioni sui permessi degli amministratori v. **Manuale dell'amministratore**, [Permessi degli amministratori](#)).

### Per installare Agent Dr.Web utilizzando Scanner di rete

1. Aprire Scanner di rete. Per farlo, selezionare la voce **Amministrazione** nel menu principale del Pannello di controllo, nella finestra che si è aperta selezionare la voce del menu di gestione **Scanner di rete**. Si apre una finestra con lo stesso nome con dati non caricati.
2. Configurare i parametri per la ricerca di postazioni nella rete. Le impostazioni sono descritte dettagliatamente nel **Manuale dell'amministratore**, p. [Scanner di rete](#).
3. Premere il pulsante **Scansiona**. Nella finestra viene caricata una directory (lista gerarchica) dei computer in cui è indicato su quali di essi il software antivirus è installato e su quali no.
4. Espandere gli elementi della directory corrispondenti ai gruppi di lavoro (domini). Tutti gli elementi della directory, corrispondenti ai gruppi di lavoro e a singole postazioni, sono contrassegnati da varie icone, il cui significato è riportato di seguito.

**Tabella 5-1. Possibili tipi di icone**

Icona	Descrizione
<b>Gruppi di lavoro</b>	
	Gruppi di lavoro che, tra gli altri computer, comprendono computer su cui si può installare Dr.Web Enterprise Security Suite.
	Altri gruppi che comprendono computer con il software antivirus installato o computer non disponibili via rete.
<b>Postazioni</b>	
	Postazione attiva con il software antivirus installato.
	Postazione attiva con lo stato del software antivirus non confermato: sul computer non è installato il software antivirus o la presenza del software non è stata verificata.



Gli elementi della directory corrispondenti alle postazioni con l'icona  possono essere espansi ulteriormente per visualizzare la lista dei componenti installati.

5. Nella finestra di **Scanner di rete** selezionare un computer non protetto (oppure più computer non protetti, utilizzando i tasti CTRL o MAIUSCOLO).
6. Nella barra degli strumenti premere il pulsante  **Installa Agent Dr.Web**.
7. Si apre la finestra **Installazione via rete** per la creazione di un task di installazione di Agent Dr.Web.
8. Nel campo **Indirizzi delle postazioni** impostare gli indirizzi IP o i nomi DNS dei computer su cui verrà installato Agent Dr.Web. Se vengono impostate diverse postazioni, utilizzare ";" o "," come separatore (non importa il numero di spazi che incorniciano il separatore).

Quando il software viene installato sui computer trovati mediante Scanner di rete, nel campo **Indirizzi delle postazioni** sarà già indicato l'indirizzo della postazione o di più postazioni sulle quali verrà eseguita l'installazione.



Gli indirizzi vengono impostati nel formato di indirizzo di rete riportato in documento **Allegati**, [Allegato D. Specifica dell'indirizzo di rete](#).

9. Di default nel campo **Server Dr.Web** è visualizzato l'indirizzo IP o il nome DNS del Server Dr.Web a cui è connesso il Pannello di controllo. Se necessario, indicare in questo campo l'indirizzo del Server Dr.Web da cui verrà installato il software antivirus. Quando vengono impostati più Server Dr.Web, utilizzare ";" o "," come separatore (non importa il numero di spazi che fiancheggiano il separatore). Lasciare vuoto il campo affinché venga utilizzato il servizio di rilevamento di Server Dr.Web (modalità *Multicast*).



L'installazione remota di Agent Dr.Web non è disponibile sul computer con il Server Dr.Web installato da cui viene avviato il processo di installazione.



Gli indirizzi vengono impostati nel formato di indirizzo di rete riportato in documento **Allegati**, [Allegato D. Specifica dell'indirizzo di rete](#).

All'installazione di Agent Dr.Web, come indirizzo di Server Dr.Web è consigliato utilizzare il nome di Server Dr.Web in [formato FQDN](#).

10. Nel campo **Numero di installazioni simultanee** impostare il numero massimo di postazioni su cui può essere eseguita l'installazione remota che viene lanciata.
11. Spuntare il flag **Installa software Agent Dr.Web per Windows** per configurare le impostazioni specifiche per l'installazione remota sui sistemi operativi Windows.
12. Di default, il software Agent Dr.Web verrà installato sulla postazione nella directory %ProgramFiles%\DrWeb. Se necessario, indicare un altro percorso nel campo **Directory di installazione di Agent Dr.Web**.

Si consiglia di impostare il percorso completo per determinare in maniera univoca la posizione della directory di installazione. Nell'impostare del percorso è ammissibile utilizzare le variabili di ambiente.



13. Dalla lista a cascata **Lingua** selezionare la lingua di interfaccia per Antivirus Dr.Web che verrà installato sulle postazioni.
14. Nel campo **Time-out dell'installazione (s)** impostare il tempo massimo in secondi di attesa del completamento dell'installazione di Agent Dr.Web. Valori ammissibili: 1–600. Di default, è impostato il valore di 180 secondi. In caso di capacità bassa del canale di comunicazione tra il Server Dr.Web e l'Agent Dr.Web, si consiglia di aumentare il valore di questo parametro.



Nel caso di una grande quantità di dati il tempo di installazione può superare la durata della sessione. Se la sessione scade prima del completamento dell'installazione, il processo verrà terminato automaticamente, e l'Agent Dr.Web non verrà installato.

15. Se necessario, spuntare il flag **Registra Agent Dr.Web nella lista dei programmi installati**.
16. Nella sezione **Componenti da installare** selezionare i componenti del pacchetto antivirus che verranno installati sulla postazione.
17. Nelle sezioni **Compressione** e **Crittografia** impostare i parametri di compressione e di cifratura del traffico dati, utilizzati da Installer di rete durante l'installazione dell'Agent Dr.Web e del pacchetto antivirus. Queste impostazioni verranno inoltre utilizzate dall'Agent Dr.Web per l'interazione con il Server Dr.Web dopo l'installazione.
18. Nella sezione **Autenticazione sul computer remoto** indicare i parametri di autenticazione per l'accesso ai computer remoti su cui verrà installato l'Agent Dr.Web:
  - **Utente** — nome utente per l'autenticazione sulle postazioni su cui verrà eseguita l'installazione remota. Per gli utenti di dominio è necessario indicare il nome del dominio nel formato `<dominio>\<utente>` o `<utente>@<dominio>`. Per gli utenti locali è necessario indicare il nome della postazione o il nome del gruppo di lavoro nel formato `<postazione>\<utente>` o `<gruppo>\<utente>`.
  - **Password** — password dell'utente sul computer remoto.

Si possono impostare diversi account amministratore. Per aggiungere un altro account, premere il pulsante  e compilare i campi con le impostazioni di autenticazione. Fare lo stesso per ciascun account nuovo.

Nel corso dell'installazione dell'Agent Dr.Web prima viene utilizzato il primo account dalla lista. Se l'installazione con questo account non è riuscita, viene utilizzato l'account successivo e così via.
19. Nella sezione **Parametri di riavvio** spuntare il flag **Riavvia la postazione** e impostare l'ora o il periodo del riavvio nella lista a cascata (anche immediatamente dopo l'installazione di Agent Dr.Web).
  - **Subito dopo l'installazione** — la postazione verrà riavviata immediatamente dopo l'installazione di Agent Dr.Web.
  - **All'ora impostata** — in conformità all'ora del sistema in cui l'amministratore ha avviato il browser e configurato l'impostazione.
  - **Nel periodo impostato** — in conformità all'ora locale della postazione.
20. Dopo aver inserito tutti i parametri necessari, premere **Installa**.



Per avviare l'installazione del software antivirus viene utilizzato un servizio incorporato.

Per avviare l'installazione, vengono utilizzati l'installer di rete del Server Dr.Web corrente situato nella directory `webmin\install\windows` della directory di installazione di Server Dr.Web e il certificato SSL `drwcsd-certificate.pem` situato nella directory `etc` della directory di installazione di Server Dr.Web.

Se nel repository di Server Dr.Web sono assenti i pacchetti di installazione per l'installazione remota di Agent Dr.Web, contattare il servizio di supporto tecnico Doctor Web: <https://support.drweb.com/>.

21. L'Agent Dr.Web verrà installato sulle postazioni indicate. Dopo la conferma della postazione sul Server Dr.Web (se lo richiedono le impostazioni del Server Dr.Web, v. inoltre **Manuale dell'amministratore** p. [Criteri di approvazione delle postazioni](#)), il pacchetto antivirus verrà installato automaticamente.

22. Riavviare il computer su richiesta di Agent Dr.Web. **Utilizzo dello strumento Installazione via rete**

Quando la rete antivirus in sostanza è già stata creata ed è necessario installare il software Agent Dr.Web su determinati computer, si consiglia di utilizzare **Installazione via rete**.



L'installazione via rete è disponibile solo per gli amministratori con il permesso **Visualizzazione delle proprietà dei gruppi di postazioni**, concesso per tutta la rete antivirus (per maggiori informazioni sui permessi degli amministratori v. **Manuale dell'amministratore**, [Permessi degli amministratori](#)).

### Per installare Agent Dr.Web via rete

1. Nel menu principale selezionare la voce **Amministrazione**, dopodiché nel menu di gestione selezionare **Installazione via rete**.
2. I passaggi successivi di installazione sono simili ai passaggi **8–22** della procedura [sopra](#).

## Installazione per account con gli ID specificati

### Se viene creato un nuovo account di postazione:

1. Creare un nuovo account o diversi nuovi account di postazioni (v. p. [Creazione di nuovo account](#)).
2. Subito dopo la creazione del nuovo account, nella parte destra della finestra principale si apre un pannello con l'intestazione **Creazione della postazione**. Premere il pulsante **Installa**.
3. Si apre la finestra di Scanner di rete.
4. I passaggi successivi di installazione sono simili ai passaggi **2–22** della procedura [sopra](#).



5. Dopo la fine dell'installazione, controllare se nella lista gerarchica sono cambiate le [icone](#) delle postazioni corrispondenti.

### Se viene utilizzato un account di postazione già esistente:

1. Nella lista gerarchica della rete antivirus selezionare una nuova postazione o un gruppo di postazioni su cui non sono ancora stati installati gli Agent Dr.Web, o selezionare il gruppo **New** (per installare su tutti i nuovi account disponibili).
2. Nella barra degli strumenti premere il pulsante  **Installa Agent Dr.Web**.
3. Si apre la finestra di Scanner di rete.
4. I passaggi successivi di installazione sono simili ai passaggi **2–22** della procedura [sopra](#).
5. Dopo la fine dell'installazione, controllare se nella lista gerarchica sono cambiate le [icone](#) delle postazioni corrispondenti.



L'installazione di Agent Dr.Web su postazioni con ID selezionati è disponibile anche per l'amministratore di gruppi.



Se vengono restituiti degli errori nel corso dell'installazione remota, consultare la sezione degli **Allegati** [Diagnostica dei problemi di installazione remota](#).

## Impostazioni aggiuntive

- Se le postazioni fanno parte del dominio e per l'installazione viene utilizzato l'account amministratore di dominio, sulle postazioni deve essere attivata la condivisione di file e stampanti. Per la posizione dell'impostazione per diverse versioni di SO Windows v. la [tabella](#).
- Se le postazioni della rete non fanno parte del dominio o per l'installazione viene utilizzato l'account locale, per alcune versioni del sistema operativo Windows è necessaria la configurazione aggiuntiva delle postazioni.

### Configurazione aggiuntiva nel caso di installazione remota su una postazione fuori dominio o con l'utilizzo dell'account locale



Le impostazioni indicate possono abbassare la sicurezza dei computer della rete. Si consiglia vivamente di conoscere lo scopo delle impostazioni indicate prima di apportare modifiche al sistema, o rinunciare all'installazione remota e installare l'Agent Dr.Web [in maniera manuale](#).

---

Dopo aver configurato la postazione della rete, si consiglia di ripristinare tutte le impostazioni modificate ai valori che erano impostati prima della modifica per non violare i criteri di sicurezza di base del sistema operativo.



Se l'Agent Dr.Web viene installato in remoto su una postazione fuori dominio e/o con l'utilizzo dell'account locale, sul computer su cui verrà installato in remoto l'Agent Dr.Web, è necessario eseguire le seguenti azioni:

SO	Impostazione	
Windows XP	Configurare la modalità di accesso ai file condivisi	Stile nuovo: <b>Start → Impostazioni → Pannello di controllo → Aspetto e temi → Proprietà cartelle → Scheda Aspetto → togliere il flag Utilizza condivisione file semplice (scelta consigliata)</b>
		Stile classico: <b>Start → Impostazioni → Pannello di controllo → Proprietà cartelle → Scheda Aspetto → togliere il flag Utilizza condivisione file semplice (scelta consigliata)</b>
	Impostare autenticazione a livello di rete nei criteri locali	Stile nuovo: <b>Start → Impostazioni → Pannello di controllo → Prestazioni e manutenzione → Amministrazione → Criteri di protezione locali → Impostazioni di protezione → Criteri locali → Impostazioni di protezione → Accesso di rete: modello di condivisione e protezione per gli account locali → Classico: gli utenti locali effettuano l'autenticazione di se stessi.</b>
		Stile classico: <b>Start → Impostazioni → Pannello di controllo → Amministrazione → Criteri di protezione locali → Impostazioni di protezione → Criteri di protezione locali → Impostazioni di protezione → Accesso di rete: modello di condivisione e protezione per gli account locali → Classico: gli utenti locali effettuano l'autenticazione di se stessi.</b>
	Disattivare Windows Firewall sulla postazione prima di eseguire l'installazione remota.	
Windows Server 2003	Disattivare Windows Firewall sulla postazione prima di eseguire l'installazione remota.	
Windows Vista  Windows Server 2008	Attivare Condivisione di file	Stile nuovo: <b>Start → Impostazioni → Pannello di controllo → Rete e Internet → Centro connessioni di rete e condivisione → Condivisione e individuazione → Condivisione di file → Attiva.</b>
		Stile classico: <b>Start → Impostazioni → Pannello di controllo → Centro connessioni di rete e condivisione → Condivisione e individuazione → Condivisione di file → Attiva.</b>



SO	Impostazione	
	Impostare autenticazione a livello di rete nei criteri locali	<p>Stile nuovo:</p> <p><b>Start → Impostazioni → Pannello di controllo → Sistema e manutenzione → Amministrazione → Criteri di protezione locali → Impostazioni di protezione → Criteri di protezione locali → Impostazioni di protezione → Accesso di rete: modello di condivisione e protezione per gli account locali → Classico: gli utenti locali effettuano l'autenticazione di se stessi.</b></p> <p>Stile classico:</p> <p><b>Start → Pannello di controllo → Amministrazione → Criteri di protezione locali → Impostazioni di protezione → Criteri di protezione locali → Impostazioni di protezione → Accesso di rete: modello di condivisione e protezione per gli account locali → Classico: gli utenti locali effettuano l'autenticazione di se stessi.</b></p>
	<p>Creare la chiave <b>LocalAccountTokenFilterPolicy</b>:</p> <p>a) Nell'editor del registro di sistema, aprire il ramo <b>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System</b>. Se il record <b>LocalAccountTokenFilterPolicy</b> non esiste, nel menu <b>Modifica</b> selezionare <b>Nuovo</b> ed impostare il valore <b>DWORD</b>. Immettere il valore <b>LocalAccountTokenFilterPolicy</b> e premere <b>INVIO</b>.</p> <p>b) Nel menu contestuale della voce <b>LocalAccountTokenFilterPolicy</b> selezionare <b>Modifica</b>.</p> <p>c) Nel campo <b>Valore</b> impostare il valore <b>1</b> e fare clic su <b>OK</b>.</p> <p>Il riavvio non è richiesto.</p>	
Windows 7 Windows Server 2008 R2	Attivare Condivisione file e stampanti	<p>Stile nuovo:</p> <p><b>Start → Pannello di controllo → Rete e Internet → Centro connessioni di rete e condivisione → Modifica impostazioni di condivisione avanzate → Condivisione file e stampanti → Attivare Condivisione file e stampanti.</b></p> <p>Stile classico:</p> <p><b>Start → Pannello di controllo → Centro connessioni di rete e condivisione → Modifica impostazioni di condivisione avanzate → Condivisione file e stampanti → Attivare Condivisione file e stampanti.</b></p>
	Impostare autenticazione a livello di rete nei criteri locali	<p>Stile nuovo:</p> <p><b>Start → Pannello di controllo → Sistema e sicurezza → Amministrazione → Criteri di protezione locali → Impostazioni di protezione → Criteri di protezione locali → Impostazioni di protezione → Accesso di rete: modello di condivisione e</b></p>



SO	Impostazione	
		<p><b>protezione per gli account locali</b> → <b>Classico: gli utenti locali effettuano l'autenticazione di se stessi.</b></p>
		<p>Stile classico:</p> <p><b>Start</b> → <b>Pannello di controllo</b> → <b>Amministrazione</b> → <b>Criteri di protezione locali</b> → <b>Impostazioni di protezione</b> → <b>Criteri di protezione locali</b> → <b>Impostazioni di protezione</b> → <b>Accesso di rete: modello di condivisione e protezione per gli account locali</b> → <b>Classico: gli utenti locali effettuano l'autenticazione di se stessi.</b></p>
	<p>Creare la chiave <b>LocalAccountTokenFilterPolicy</b>:</p> <p>a) Nell'editor del registro di sistema, aprire il ramo <b>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System</b>. Se il record <b>LocalAccountTokenFilterPolicy</b> non esiste, nel menu <b>Modifica</b> selezionare <b>Nuovo</b> ed impostare il valore <b>DWORD</b>. Immettere il valore <b>LocalAccountTokenFilterPolicy</b> e premere INVIO.</p> <p>b) Nel menu contestuale della voce <b>LocalAccountTokenFilterPolicy</b> selezionare <b>Modifica</b>.</p> <p>c) Nel campo <b>Valore</b> impostare il valore <b>1</b> e fare clic su <b>OK</b>.</p> <p>Il riavvio non è richiesto.</p>	
Windows 8 Windows 8.1 Windows Server 2012	Attivare Condivisione file e stampanti	<p>Stile nuovo:</p> <p><b>Impostazioni</b> → <b>Pannello di controllo</b> → <b>Rete e Internet</b> → <b>Centro connessioni di rete e condivisione</b> → <b>Modifica impostazioni di condivisione avanzate</b> → <b>Condivisione file e stampanti</b> → <b>Attivare Condivisione file e stampanti.</b></p>
Windows Server 2012 R2 Windows 10		<p>Stile classico:</p> <p><b>Impostazioni</b> → <b>Pannello di controllo</b> → <b>Centro connessioni di rete e condivisione</b> → <b>Modifica impostazioni di condivisione avanzate</b> → <b>Condivisione file e stampanti</b> → <b>Attivare Condivisione file e stampanti.</b></p>
	Impostare autenticazione a livello di rete nei criteri locali	<p>Stile nuovo:</p> <p><b>Impostazioni</b> → <b>Pannello di controllo</b> → <b>Sistema e sicurezza</b> → <b>Amministrazione</b> → <b>Criteri di protezione locali</b> → <b>Impostazioni di protezione</b> → <b>Criteri di protezione locali</b> → <b>Impostazioni di protezione</b> → <b>Accesso di rete: modello di condivisione e protezione per gli account locali</b> → <b>Classico: gli utenti locali effettuano l'autenticazione di se stessi.</b></p>
		<p>Stile classico:</p>



SO	Impostazione
	<p><b>Impostazioni → Pannello di controllo → Amministrazione → Criteri di protezione locali → Impostazioni di protezione → Criteri di protezione locali → Impostazioni di protezione → Accesso di rete: modello di condivisione e protezione per gli account locali → Classico: gli utenti locali effettuano l'autenticazione di se stessi.</b></p>
	<p>Creare la chiave <b>LocalAccountTokenFilterPolicy</b>:</p> <p>a) Nell'editor del registro di sistema, aprire il ramo <b>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System</b>. Se il record <b>LocalAccountTokenFilterPolicy</b> non esiste, nel menu <b>Modifica</b> selezionare <b>Nuovo</b> ed impostare il valore <b>DWORD</b>. Immettere il valore <b>LocalAccountTokenFilterPolicy</b> e premere INVIO.</p> <p>b) Nel menu contestuale della voce <b>LocalAccountTokenFilterPolicy</b> selezionare <b>Modifica</b>.</p> <p>c) Nel campo <b>Valore</b> impostare il valore <b>1</b> e fare clic su <b>OK</b>.</p> <p>Il riavvio non è richiesto.</p>

Se per l'account sulla postazione della rete è impostata una password vuota, impostare nei criteri locali il criterio di accesso con una password vuota: **Pannello di controllo → Amministrazione → Criteri di protezione locali → Impostazioni di protezione → Criteri di protezione locali → Impostazioni di protezione → Account: limitare l'uso locale di account con password vuote all'accesso alla console → Disattiva**.

### 5.2.3.1.2. Installazione remota di Agent Dr.Web per SO UNIX

#### Prima di iniziare l'installazione:

1. Configurare l'accesso tramite SSH dal computer su cui è installato il Server Dr.Web al computer su cui verrà installato l'Agent Dr.Web (l'installazione remota viene effettuata tramite SSH).
2. Nella sezione di Pannello di controllo **Configurazione generale del repository** impostare per il caricamento nel repository di Server Dr.Web i pacchetti di Agent Dr.Web per UNIX corrispondenti. Per farlo, nel menu principale selezionare la voce **Amministrazione**, dopodiché nel menu di gestione selezionare **Configurazione generale del repository**. Nella sezione **Pacchetti di installazione Dr.Web** selezionare la scheda **Prodotti aziendali Dr.Web**, quindi **Dr.Web per Linux**. Selezionare la piattaforma richiesta.



Caricare i pacchetti solo per le piattaforme che sono necessarie e utilizzate. Il caricamento di tutti i pacchetti richiederà molto tempo e ulteriore spazio su disco.

3. Caricare i pacchetti di Agent Dr.Web per UNIX nel repository. Due volte all'ora essi vengono caricati autonomamente secondo il calendario di Scheduler di Server Dr.Web. Se no,



aggiornare forzatamente il repository. Per fare questo, nel menu principale selezionare la voce **Amministrazione**, dopodiché nel menu di gestione selezionare **Stato del repository**, quindi **Verifica aggiornamenti**.

Per controllare se i pacchetti di Agent Dr.Web per UNIX sono caricati, nel menu principale selezionare la voce **Amministrazione**, dopodiché nel menu di gestione selezionare **Prodotti aziendali**.

Dopo questo si può iniziare l'installazione.

Per l'installazione remota del software Agent Dr.Web sui computer con i sistemi operativi della famiglia UNIX, utilizzare lo strumento Installazione via rete nel Pannello di controllo della sicurezza Dr.Web.



Durante l'installazione dell'Agent Dr.Web, sulla postazione viene creata una directory con il pacchetto e il log di installazione. Il percorso di questa directory viene indicato nell'interfaccia web all'avvio dell'installazione (parametro **Directory dei file temporanei**).

### Per installare Agent Dr.Web via rete

1. Nel menu principale selezionare la voce **Amministrazione**, dopodiché nel menu di gestione selezionare **Installazione via rete**.
2. Nel campo **Indirizzi delle postazioni** impostare gli indirizzi IP o i nomi DNS dei computer su cui verrà installato Agent Dr.Web. Se vengono impostate diverse postazioni, utilizzare ";" o "," come separatore (non importa il numero di spazi che incorniciano il separatore).



Gli indirizzi vengono impostati nel formato di indirizzo di rete riportato in documento **Allegati**, [Allegato D. Specifica dell'indirizzo di rete](#).

3. Nel campo **Server Dr.Web** di default è visualizzato l'indirizzo IP o il nome DNS del Server Dr.Web a cui è connesso il Pannello di controllo. Se necessario, indicare in questo campo l'indirizzo del Server Dr.Web da cui verrà installato il software antivirus. Quando vengono impostati più Server Dr.Web, utilizzare ";" o "," come separatore (non importa il numero di spazi che fiancheggiano il separatore). Lasciare vuoto il campo affinché venga utilizzato il servizio di rilevamento di Server Dr.Web (modalità *Multicast*).



L'installazione remota di Agent Dr.Web non è disponibile sul computer con il Server installato da cui viene avviato il processo di installazione.



Gli indirizzi vengono impostati nel formato di indirizzo di rete riportato in documento **Allegati**, sezione [Allegato D. Specifica dell'indirizzo di rete](#).

All'installazione di Agent Dr.Web, come indirizzo di Server Dr.Web è consigliato utilizzare il nome di Server Dr.Web in [formato FQDN](#).



4. Nel campo **Numero di installazioni simultanee** impostare il numero massimo di postazioni su cui può essere eseguita l'installazione remota che viene lanciata.
5. Spuntare il flag **Installa software Agent Dr.Web per UNIX** per configurare le impostazioni specifiche per l'installazione remota sui sistemi operativi della famiglia UNIX.
6. Nel campo **Timeout di connessione e autenticazione (s)** impostare il tempo massimo in secondi di attesa del stabilimento della connessione e dell'autenticazione sulle postazioni remote.
7. Nel campo **Timeout di trasmissione dei pacchetti di installazione (s)** indicare il tempo massimo in secondi di attesa del completamento del processo di trasmissione dei pacchetti di installazione.
8. Nel campo **Timeout di installazione dei pacchetti (s)** indicare il tempo massimo in secondi di attesa del completamento dell'installazione dei pacchetti.



Nel caso di una grande quantità di dati il tempo di installazione può superare la durata della sessione. Se la sessione scade prima del completamento dell'installazione, il processo verrà terminato automaticamente, e i pacchetti non verranno installati.

9. Se è necessario installare il prodotto Dr.Web per file server UNIX invece di Agent Dr.Web, spuntare il flag **Installa Dr.Web per file server UNIX**.
10. Nella sezione **Connessione a postazioni remote via SSH tramite password** indicare i parametri di autenticazione per l'accesso ai computer remoti su cui verrà installato l'Agent Dr.Web:
  - **Utente** — nome utente per l'autenticazione sulle postazioni su cui verrà eseguita l'installazione remota. Per gli utenti di dominio è necessario indicare il nome del dominio nel formato `<dominio>\<utente>` o `<utente>@<dominio>`. Per gli utenti locali è necessario indicare il nome della postazione o il nome del gruppo di lavoro nel formato `<postazione>\<utente>` o `<gruppo>\<utente>`.
  - **Password** — password dell'utente sul computer remoto.È possibile impostare contemporaneamente più account per l'autenticazione. Per aggiungere un altro account, premere il pulsante  e compilare i campi con le impostazioni di autenticazione.

Nel corso dell'installazione di Agent Dr.Web verranno utilizzati in sequenza gli account dalla lista. Se l'installazione con un account non è riuscita, viene utilizzato l'account successivo e così via.
11. Nella sezione **Connessione a postazioni remote via SSH tramite chiavi SSH** è possibile configurare le impostazioni di autenticazione alternativa sui computer remoti con utilizzo delle chiavi di cifratura:
  - **Utente** — nome utente per l'autenticazione sulle postazioni su cui verrà eseguita l'installazione remota. Per gli utenti di dominio è necessario indicare il nome del dominio nel formato `<dominio>\<utente>` o `<utente>@<dominio>`. Per gli utenti locali è necessario indicare il nome della postazione o il nome del gruppo di lavoro nel formato `<postazione>\<utente>` o `<gruppo>\<utente>`.
  - **Chiave pubblica SSH** — percorso del file della chiave pubblica SSH.



- **Chiave privata SSH** — percorso del file della chiave privata SSH.
- **Password della chiave privata SSH** — password della chiave privata SSH (opzionale).

Come nella sezione **Connessione a postazioni remote via SSH tramite password**, c'è la possibilità di specificare contemporaneamente più account, per questo scopo è necessario premere il pulsante  e compilare i campi corrispondenti.



Se sono compilati i parametri di autenticazione in entrambe le sezioni **Connessione a postazioni remote via SSH tramite password** e **Connessione a postazioni remote via SSH tramite chiavi SSH**, per primi per l'installazione di Agent Dr.Web verranno utilizzati i parametri di autenticazione tramite chiavi di cifratura.

12. La sezione **Permessi di superutente** contiene impostazioni studiate per elevare i permessi utente sul computer remoto al livello necessario per l'installazione di Agent Dr.Web.
  - Spuntare il flag **Utilizza il comando sudo** o **Utilizza il comando su** per elevare i permessi a livello dell'utente *root* per il tempo dell'installazione di Agent Dr.Web.
  - Nel campo **Timeout di inserimento della password (s)** indicare il tempo massimo in secondi di attesa dell'inserimento della password per l'utilizzo del comando *su* o *sudo*.
  - Nel campo **Password su/sudo** inserire la password per l'utilizzo del comando *su* o *sudo*. Premendo il pulsante , si possono indicare diverse password che verranno selezionate in modo alternato. Se si lascia il campo vuoto, ma allo stesso tempo sarà impostata la password utente nella sezione **Connessione a postazioni remote via SSH tramite password**, verrà effettuato un tentativo di eseguire il comando con la password specificata.
13. Nel campo **Porta** della sezione **Parametri di connessione** indicare il numero di porta SSH sui computer che verrà utilizzato per l'installazione remota di Agent Dr.Web. Tramite il pulsante  è possibile elencare diverse porte.
14. Dopo aver indicato tutti i parametri necessari, premere **Installa**.
15. L'Agent Dr.Web verrà installato sulle postazioni indicate. Dopo la conferma della postazione sul Server Dr.Web (se lo richiedono le impostazioni del Server Dr.Web, v. inoltre **Manuale dell'amministratore** [Criteri di approvazione delle postazioni](#)), verrà automaticamente installato il pacchetto antivirus.
16. Riavviare i computer remoti su richiesta di Agent Dr.Web.

### 5.2.3.2. Installazione di Agent Dr.Web con utilizzo del servizio Active Directory

Se nella rete locale protetta viene utilizzato il servizio **Active Directory**, è possibile installare Agent Dr.Web sulle postazioni in remoto.



L'installazione di Agent tramite il servizio Active Directory è inoltre possibile in caso di utilizzo di un file system distribuito DFS (v. documento **Allegati**, [Utilizzo di DFS per l'installazione di Agent Dr.Web tramite Active Directory](#)).



## Installazione di Agent Dr.Web

### Per installare Agent Dr.Web utilizzando il servizio Active Directory

1. Scaricare l'installer di Agent Dr.Web per le reti con **Active Directory** dalla [pagina di installazione](#).
2. Sul server della rete locale che supporta il servizio **Active Directory** eseguire l'installazione amministrativa di Agent Dr.Web. L'installazione può essere eseguita sia in modalità riga di comando **(A)** che in modalità grafica del programma di installazione **(B)**.



Quando si aggiorna il Server Dr.Web, non è necessario aggiornare l'installer di Agent Dr.Web per le reti con Active Directory. In seguito all'aggiornamento del software Server Dr.Web, gli Agent Dr.Web e il software antivirus sulle postazioni verranno aggiornati automaticamente dopo l'installazione.

### (A) Configurazione dei parametri di installazione di Agent Dr.Web in modalità riga di comando

Avviare il seguente comando con tutti i parametri necessari e con il parametro obbligatorio di disattivazione della modalità grafica /qn:

```
msiexec /a <nome_pacchetto>.msi /qn [<parametri>]
```

L'opzione /a avvia la distribuzione del pacchetto amministrativo.

#### Nome pacchetto

Il nome del pacchetto di installazione di Agent Dr.Web per le reti con **Active Directory** di solito ha il seguente formato:

```
drweb-<versione_pacchetto>-<build>-esuite-agent-activedirectory.msi
```

#### Parametri

/qn — il parametro di disattivazione della modalità grafica. Quando viene utilizzata questa opzione, è necessario impostare i seguenti parametri obbligatori:

- `ESERVERADDRESS=<nome_DNS>` — l'indirizzo del Server Dr.Web a cui si conatterà l'Agent Dr.Web. Per i formati possibili v. documento **Allegati**, [Allegato D. Specifica dell'indirizzo di rete](#).
- `ESERVERPATH=<nome_completo_file>` — il percorso completo del certificato del Server Dr.Web e il nome del file (di default, è il file `drwcsd-certificate.pem` nella sottodirectory `webmin/install` della directory di installazione del Server Dr.Web).
- `TARGETDIR` — la directory di rete per l'immagine di Agent Dr.Web (pacchetto di installazione modificato di Agent Dr.Web), la quale viene selezionata attraverso l'editor



Criteri di gruppo per l'installazione stabilita. Tale directory deve avere accesso in lettura e scrittura. Il percorso della directory deve essere indicato nel formato di indirizzi di rete, anche se è disponibile localmente; la directory deve essere obbligatoriamente accessibile dalle postazioni di destinazione.



Prima dell'installazione amministrativa, nella directory di destinazione per l'immagine di Agent Dr.Web (v. parametro TARGETDIR) non è necessario mettere manualmente i file per l'installazione. L'Installer di Agent Dr.Web per le reti con Active Directory (<nome\_pacchetto>.msi) e gli altri file necessari per l'installazione degli Agent Dr.Web su postazioni verranno messi nella directory di destinazione automaticamente nel corso dell'installazione amministrativa. Se questi file sono presenti nella directory di destinazione prima dell'inizio dell'installazione amministrativa, per esempio, sono rimasti da installazioni precedenti, i file con i nomi uguali verranno sovrascritti.

Se è necessario eseguire l'installazione amministrativa da Server Dr.Web diversi, si consiglia di impostare directory di destinazione diverse per ciascuno dei Server Dr.Web.



Dopo la distribuzione del pacchetto amministrativo nella directory <directory\_di\_destinazione>\Program Files\DrWeb deve esserci solo il file README.txt.

## Esempi

```
msiexec /a ES_Agent.msi /qn ESSERVERADDRESS=servername.net ESSERVERPATH=\win_serv\drwcs_inst\drwcsd-certificate.pem TARGETDIR=\\comp\share
```

```
msiexec /a ES_Agent.msi /qn ESSERVERADDRESS=192.168.14.1 ESSERVERPATH="C:\Program Files\DrWeb Server\webmin\install\drwcsd-certificate.pem" TARGETDIR=\\comp\share
```

Si possono impostare gli stessi parametri in modalità grafica dell'installer.

In seguito è necessario ordinare l'installazione del pacchetto sul server della rete locale su cui è installato il software di gestione di Active Directory (v. procedura [sotto](#)).

## (B) Configurazione dei parametri di installazione di Agent Dr.Web in modalità grafica



Prima dell'installazione amministrativa, assicurarsi che la directory di destinazione dell'immagine Agent Dr.Web non contenga l'installer di Agent Dr.Web per le reti con **Active Directory** (<nome\_pacchetto>.msi).



Dopo che il pacchetto amministrativo è stato distribuito, nella directory `<directory_di_destinazione>\Program Files\DrWeb` deve esserci solo il file `README.txt`.

1. Per avviare il programma di installazione in modalità grafica eseguire il comando:

```
msiexec /a <percorso_installer>\<nome_pacchetto>.msi
```

2. Si apre la finestra **InstallShield Wizard** con informazioni sul prodotto che viene installato. Premere il pulsante **Avanti**.



L'installer di Agent Dr.Web utilizza la lingua impostata nelle configurazioni di lingua del computer.

3. Nella nuova finestra indicare il nome DNS o l'indirizzo IP del Server Dr.Web (v. documento **Allegati**, [Allegato D. Specifica dell'indirizzo di rete](#)). Indicare il percorso del certificato di Server Dr.Web (`drwcsd-certificate.pem`). Premere il pulsante **Avanti**.
4. Nella finestra successiva indicare la directory di rete in cui verrà scritto l'immagine di Agent Dr.Web. Il percorso della directory deve essere scritto nel formato di indirizzi di rete, anche se la directory è disponibile localmente; la directory deve essere obbligatoriamente accessibile dalle postazioni di destinazione. Premere il pulsante **Installa**.
5. Dopo la fine dell'installazione viene automaticamente richiamata la finestra di configurazione attraverso cui si può ordinare l'installazione dei pacchetti sui computer della rete.

## Configurazione dell'installazione del pacchetto su postazioni selezionate

1. Nel **Pannello di controllo** (o nel menu **Start** in caso di SO Windows 2003/2008/2012/2012R2 Server, nel menu **Start** → **Programmi** in caso di SO Windows 2000 Server), selezionare **Amministrazione** → **Active Directory — utenti e computer** (in modalità grafica di installazione di Agent Dr.Web questa finestra delle impostazioni viene invocata in maniera automatica).
2. Nel dominio che include i computer su cui si vuole installare Agent Dr.Web, creare una nuova **Unità** (in caso di SO Windows 2000 Server — **Unità organizzativa**) con il nome, come esempio, **ESS**. Per fare questo, dal menu contestuale del dominio selezionare **Nuovo** → **Unità**. Nella finestra che si è aperta, immettere il nome della nuova unità e premere **OK**. Includere nell'unità creata i computer su cui si vuole installare Agent Dr.Web.
3. Aprire la finestra di modifica dei criteri di gruppo. Per farlo:
  - a) in caso del SO Windows 2000/2003 Server: dal menu contestuale dell'unità creata **ESS** selezionare la voce **Proprietà**. Nella finestra di proprietà che si è aperta passare alla scheda **Criteri di gruppo**.
  - b) in caso del SO Windows 2008/2012/2012R2 Server: **Start** → **Amministrazione** → **Gestione Criteri di gruppo**.
4. All'unità creata assegnare un criterio di gruppo. Per farlo:



- a) Nel SO Windows 2000/2003 Server: premere il pulsante **Aggiungi** e creare un elemento dell'elenco con il nome Criteri di gruppo **ESS**. Fare doppio click su di esso.
  - b) Nel SO Windows 2008/2012/2012R2 Server: dal menu contestuale dell'unità **ESS** creata selezionare la voce **Crea un oggetto Criteri di gruppo in questo dominio e crea qui un collegamento**. Nella finestra che si è aperta digitare il nome del nuovo oggetto Criteri di gruppo e premere il pulsante **OK**. Dal menu contestuale del nuovo criterio di gruppo selezionare la voce **Modifica**.
5. Nella finestra che si è aperta **Editor Gestione Criteri di gruppo** configurare il criterio di gruppo creato nel punto 4. Per farlo:
    - a) Nel SO Windows 2000/2003 Server: nella lista gerarchica selezionare l'elemento **Configurazione computer** → **Impostazioni del software** → **Installazione software**.
    - b) Nel SO Windows 2008/2012/2012R2 Server: nella lista gerarchica selezionare l'elemento **Configurazione computer** → **Criteri** → **Impostazioni del software** → **Installazione software**.
  6. Dal menu contestuale dell'elemento **Installazione software** selezionare la voce **Nuovo** → **Pacchetto**.
  7. Quindi assegnare il pacchetto di installazione Agent Dr.Web. Per farlo, indicare l'indirizzo della risorsa di rete condivisa (l'immagine di Agent Dr.Web creata nel corso dell'installazione amministrativa). Il percorso della directory con il pacchetto deve essere scritto nel formato di indirizzi di rete, anche se la directory è disponibile localmente.
  8. Si apre la finestra **Distribuire software**. Selezionare l'opzione **Assegnato**. Fare clic su **OK**.
  9. Nella finestra dell'editor Gestione Criteri di gruppo compare la voce **Agent Dr.Web**. Dal menu contestuale di questa voce selezionare **Proprietà**.
  10. Nella finestra di proprietà pacchetto che si è aperta passare alla scheda **Distribuzione**. Premere il pulsante **Avanzate**.
  11. Si apre la finestra **Impostazioni avanzate di distribuzione**.
    - Spuntare il flag **Non usare le impostazioni di lingua per la distribuzione**.
    - Se si intende installare l'Agent Dr.Web tramite un pacchetto msi configurabile su sistemi operativi a 64 bit, spuntare il flag **Rendi questa applicazione a 32 bit disponibile per computer x64**.
  12. Fare doppio click su **OK**.
  13. L'Agent Dr.Web verrà installato sui computer scelti quando si registreranno prossimamente nel dominio.

## Utilizzo dei criteri con considerazione di installazioni precedenti di Agent Dr.Web

Quando vengono assegnati i criteri di Active Directory per l'installazione di Agent Dr.Web, è necessario tenere in considerazione che l'Agent Dr.Web potrebbe già essere installato sulla postazione. Sono possibili tre varianti:

1. **Sulla postazione non c'è l'Agent Dr.Web.**



Dopo che sono stati assegnati i criteri, l'Agent viene installato in conformità alle regole generali.

## 2. Sulla postazione è già stato installato un Agent Dr.Web senza utilizzo del servizio Active Directory.

Dopo che è stato assegnato il criterio di Active Directory, l'Agent Dr.Web installato rimane sulla postazione.



In questa situazione, l'Agent Dr.Web è installato sulla postazione, ma Active Directory considera l'Agent Dr.Web non installato. Pertanto, dopo ogni caricamento della postazione, verrà ripetuto un tentativo non riuscito di installazione di Agent Dr.Web tramite Active Directory.

Per installare Agent Dr.Web tramite Active Directory, è necessario eliminare manualmente (o tramite il Pannello di controllo) l'Agent Dr.Web installato ed assegnare di nuovo i criteri di Active Directory a tale postazione.

## 3. Sulla postazione è già stato installato un Agent Dr.Web con utilizzo del servizio Active Directory.

Il criterio non viene assegnato nuovamente alla postazione con un Agent Dr.Web installato tramite il servizio Active Directory.

Pertanto, l'assegnazione di criteri non cambierà lo stato del software antivirus sulla postazione.

## 5.3. Installazione di Server di scansione Dr.Web



Server di scansione può essere installato solo su sistemi operativi della famiglia Linux e FreeBSD.

Server di scansione e le macchine virtuali con Agent Dr.Web installato che si connettono ad esso devono essere collocati nei limiti dello stesso hypervisor.

1. Scaricare dalla [pagina di installazione](#) il pacchetto di installazione di Server di scansione sulla postazione che si intende nominare Server di scansione.
2. Scaricare il certificato del Server Dr.Web a cui si conatterà Server di scansione. Per fare ciò, nel menu di gestione del Pannello di controllo nella sezione **Amministrazione** selezionare la voce **Chiavi di crittografia**. Spuntare il flag accanto all'oggetto **Certificato** e premere **Esporta**. Caricare il certificato sulla postazione che si intende nominare Server di scansione.



Il certificato può essere scaricato anche dalla pagina di installazione. Si trova nella stessa directory del pacchetto di installazione di Server di scansione.

3. Passare alla directory in cui è stato scaricato il file del pacchetto di installazione e consentirne l'esecuzione:

```
# chmod +x <nome_file>.run
```



4. Quindi avviare la procedura di installazione:

```
# ./<nome_file>.run
```

5. Accettare le condizioni del Contratto di licenza.
6. Al termine dell'installazione connettere la postazione che si intende nominare Server di scansione a Server Dr.Web eseguendo il comando:

```
# drweb-ctl esconnect <indirizzo di Server Dr.Web> --Certificate <percorso del file del certificato>
```



Come indirizzo di Server Dr.Web è consigliato utilizzare il nome di server [in formato FQDN](#).

Dopo l'esecuzione di questo comando la connessione deve essere approvata automaticamente o dall'amministratore della rete antivirus a seconda delle impostazioni di Server Dr.Web.

La connessione a Server Dr.Web può essere effettuata anche in un altro modo: [creare un account di una postazione](#) che si intende nominare Server di scansione, dopodiché si ottengono il login (ID della postazione) e la password per la connessione. Quindi eseguire il comando:

```
# drweb-ctl esconnect <indirizzo di Server Dr.Web> --login <ID della postazione> --password <password> --Certificate <percorso del file del certificato>
```

7. Se la connessione va a buon fine, la postazione verrà contrassegnata nell'albero della rete antivirus con l'icona  che indica che Server di scansione è attivo e pronto a funzionare.



Sulla postazione che svolge le funzioni di Server di scansione non è necessario installare in aggiunta Agent Dr.Web.

8. Assicurarsi che Server di scansione sia in ascolto sulle porte 7090 e 18008, eseguendo il seguente comando:

```
# netstat -l
```

L'output di questo comando deve contenere le seguenti stringhe:

```
tcp 0 0 0.0.0.0:7090 0.0.0.0:* LISTEN
udp 0 0 0.0.0.0:18008 0.0.0.0:*
```



Le informazioni dettagliate sulla configurazione di Server di scansione e la connessione ad esso delle postazioni sono contenute nel **Manuale dell'amministratore di Dr.Web Enterprise Security Suite**, nella sezione [Connessione delle postazioni a Server di scansione](#).



## 5.4. Installazione di NAP Validator

Dr.Web NAP Validator serve per controllare l'operatività del software antivirus delle postazioni protette.

Questo componente viene installato su un computer con il server NAP configurato.

### Per installare NAP Validator

1. Avviare il file del pacchetto. Si apre la finestra di scelta della lingua per la successiva installazione del prodotto. Selezionare **Italiano** e premere il pulsante **Avanti**.
2. Si apre la finestra **InstallShield Wizard** con informazioni sul prodotto che viene installato. Premere il pulsante **Avanti**.
3. Si apre la finestra con il testo del Contratto di licenza. Dopo aver letto i termini del Contratto di licenza, nel gruppo di pulsanti di scelta indicare **Accetto i termini del Contratto di licenza** e premere il pulsante **Avanti**.
4. Nella finestra che si è aperta, nei campi **Indirizzo** e **Porta**, impostare rispettivamente l'indirizzo IP e la porta del Server Dr.Web. Premere il pulsante **Avanti**.
5. Premere il pulsante **Installa**. Le azioni successive del programma di installazione non richiedono l'intervento dell'utente.
6. Dopo il completamento dell'installazione, premere il pulsante **Finito**.

Dopo aver installato Dr.Web NAP Validator, è necessario inserire il Server Dr.Web nel gruppo di server affidabili NAP. Per farlo:

1. Aprire il componente di configurazione del server NAP (comando `nps.msc`).
2. Nella sezione **Gruppi di server di correzione** premere il pulsante **Aggiungi**.
3. Nella finestra di dialogo che si è aperta, indicare il nome del server di correzione e l'indirizzo IP del Server Dr.Web.
4. Per salvare le modifiche apportate, premere il pulsante **OK**.

## 5.5. Installazione del Server proxy Dr.Web

La rete antivirus può includere uno o più Server proxy Dr.Web.

Quando viene selezionato il computer su cui verrà installato il Server proxy Dr.Web, il criterio principale è l'accessibilità del Server proxy Dr.Web da tutte le reti/segmenti di reti tra cui esso reindirizza le informazioni.



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



È possibile installare il Server proxy Dr.Web in SO Windows in uno dei seguenti modi:

- [In modo automatico durante l'installazione di Agent Dr.Web per Windows](#)

L'installazione viene effettuata tramite un pacchetto di installazione individuale di Agent Dr.Web in cui durante la sua creazione sono state definite le impostazioni di installazione di un Server proxy Dr.Web associato. In questo caso l'installazione di Server proxy Dr.Web viene eseguita automaticamente in modalità background.

- [In modo automatico su una postazione con installato Agent Dr.Web per Windows](#)

Configurare nel Pannello di controllo la creazione di un Server proxy Dr.Web associato per la postazione selezionata. Server proxy Dr.Web verrà installato sulla postazione automaticamente in modalità background.

- [Manualmente tramite l'installer grafico](#)

L'installazione viene effettuata dall'amministratore manualmente su qualsiasi postazione adatta della rete. Nessun altro componente della rete antivirus può essere installato su questa postazione.

L'installazione di Server proxy Dr.Web nei sistemi operativi della famiglia UNIX viene effettuata solo [manualmente tramite l'installer](#).

### 5.5.1. Creazione dell'account del Server proxy Dr.Web



Gli account di Server proxy Dr.Web devono essere creati dall'amministratore su ciascun Server Dr.Web a cui si conetterà il Server proxy Dr.Web (su cui verrà reindirizzato il traffico).

#### Per creare un account di Server proxy Dr.Web tramite il Pannello di controllo della sicurezza Dr.Web

1. Per il gruppo padre in cui si prevede la creazione di un Server proxy Dr.Web definire le impostazioni, come descritto in **Manuale dell'amministratore** sezione [Configurazione del Server proxy in remoto](#). In questo caso il Server proxy Dr.Web erediterà le impostazioni definite al momento della connessione. È anche possibile definire queste impostazioni (sia per il gruppo padre in caso di ereditarietà che individualmente per il Server proxy Dr.Web stesso) dopo la creazione dell'account di Server proxy Dr.Web, ma prima della connessione del Server proxy Dr.Web all'account che viene creato.



Se le impostazioni non sono state definite prima della connessione del Server proxy Dr.Web, il file di configurazione non verrà scaricato. Le impostazioni correnti verranno utilizzate dal Server proxy Dr.Web fino a quando non verranno definite le impostazioni sul Server Dr.Web connesso, a condizione che ad esso sia consentita la gestione della configurazione.

2. Selezionare la voce **Rete antivirus** nel menu principale del Pannello di controllo.



3. Le azioni necessarie per la creazione di un Server proxy Dr.Web dipenderanno da quello se si vuole installare il Server proxy Dr.Web su una postazione esistente con Agent Dr.Web o installare il Server proxy Dr.Web separatamente:

N	Azioni	Installare con Agent Dr.Web	Installare separatamente
a)	<ol style="list-style-type: none"><li>1. Nell'albero della rete antivirus selezionare una postazione per l'installazione di un Server proxy Dr.Web associato.</li><li>2. Nella barra delle proprietà della postazione selezionata passare alla sezione <b>Server proxy</b>.</li></ol>	+	-
b)	<ol style="list-style-type: none"><li>1. Nell'albero della rete antivirus selezionare una postazione per l'installazione di un Server proxy Dr.Web associato.</li><li>2. Nella barra degli strumenti selezionare l'opzione  <b>Aggiungi oggetto della rete</b> →  <b>Crea Server proxy</b>.</li></ol>	+	+
c)	<ol style="list-style-type: none"><li>1. Assicurarsi che nell'albero della rete antivirus non sia selezionata una postazione.</li><li>2. Nella barra degli strumenti selezionare l'opzione  <b>Aggiungi oggetto della rete</b> →  <b>Crea Server proxy</b>.</li></ol>	+	+



Se viene creato un account di un Server proxy Dr.Web che verrà installato su una postazione con Agent Dr.Web, l'installazione stessa del Server proxy Dr.Web verrà eseguita automaticamente attraverso l'Agent in modalità background subito dopo la creazione dell'account del Server proxy (v. inoltre [Installazione di Server proxy Dr.Web durante l'installazione di Agent Dr.Web per Windows](#)).

Se viene creato un account di un Server proxy Dr.Web che verrà installato separatamente (senza relazione ad Agent Dr.Web), l'installazione del Server proxy Dr.Web deve essere effettuata dall'amministratore manualmente tramite il pacchetto di installazione fornito insieme al pacchetto di Server Dr.Web.

4. Nel campo **Identificatore** viene generato automaticamente l'identificatore univoco dell'account che viene creato. Se necessario, è possibile modificarlo.
5. Nel campo **Nome** impostare il nome di Server proxy Dr.Web, che verrà visualizzato nell'albero della rete antivirus.



Il nome indicato durante la configurazione verrà automaticamente sostituito con il nome del computer dopo la connessione del Server proxy Dr.Web al Server Dr.Web.

6. Nei campi **Password** e **Confermare la password** è possibile impostare una password di accesso del Server proxy al Server Dr.Web. Se la password non è indicata, verrà generata automaticamente.



L'identificatore e la password di Server proxy Dr.Web vengono utilizzati in un unico esemplare. Su tutti i Server Dr.Web a cui si connette il Server proxy Dr.Web devono essere



creati account di Server proxy Dr.Web con dati di autenticazione uguali (v. [Connessione del Server proxy Dr.Web al Server Dr.Web](#)).

Dopo la creazione dell'account di Server proxy Dr.Web la modifica dell'identificatore non sarà possibile.

7. Ai passaggi 3.b) e 3.c) nel campo **Postazione** viene impostata una postazione esistente con Agent Dr.Web installato, a cui sarà associato questo Server proxy Dr.Web.

Al passaggio 3.b) al campo **Postazione** verrà aggiunto automaticamente l'identificatore della postazione selezionata.

Al passaggio 3.c) il campo **Postazione** sarà vuoto.

- Per impostare la postazione su cui verrà installato il Server proxy Dr.Web, fare clic su  e nella finestra che si è aperta selezionare una postazione esistente dall'albero della rete antivirus.
- Lasciare vuoto il campo **Postazione** per non associare il Server proxy Dr.Web a nessuna postazione e per connettere il Server proxy Dr.Web installato manualmente. Se il campo **Postazione** è già compilato, fare clic su  per rimuovere la postazione associata.

8. Nella sezione **Appartenenza** viene impostato il gruppo in cui sarà incluso il Server proxy Dr.Web che viene creato. Per modificare il gruppo, spuntare il flag di fronte al gruppo richiesto nella lista riportata.

Un Server proxy può rientrare in solo un gruppo.

È possibile selezionare il gruppo predefinito **Proxies** e i relativi sottogruppi.

9. Premere il pulsante **Salva**.

Si aprirà una finestra di creazione riuscita di un account di Server proxy Dr.Web, in cui sarà inoltre indicata la password di accesso al Server Dr.Web. Per visualizzare la password, fare clic su .



L'identificatore e la password di un account di Server proxy Dr.Web creato attraverso il Pannello di controllo sono necessari per l'amministratore per connettere il Server proxy Dr.Web al Server Dr.Web:

- [Durante l'installazione del Server proxy attraverso l'installer grafico.](#)
- [Manualmente dopo l'installazione del Server proxy \(solo in SO della famiglia UNIX\).](#)

## 5.5.2. Installazione di Server proxy Dr.Web durante l'installazione di Agent Dr.Web per Windows

### Per installare Server proxy Dr.Web insieme ad Agent Dr.Web per Windows

1. Definire le impostazioni del Server proxy Dr.Web nel Pannello di controllo, come descritto in **Manuale dell'amministratore** p. [Configurazione del Server proxy in remoto](#). Le impostazioni devono essere definite per il gruppo in cui si prevede di creare il Server proxy.



In questo caso esso erediterà le impostazioni definite al momento della creazione. È anche possibile definire queste impostazioni (sia per il gruppo in caso di ereditarietà che individualmente per il Server proxy Dr.Web stesso) dopo la creazione del Server proxy, ma prima della connessione del Server proxy Dr.Web all'account che viene creato.



Se le impostazioni non sono state definite prima della connessione del Server proxy Dr.Web, verranno utilizzate le impostazioni trasmesse al Server proxy Dr.Web dall'installer. Queste impostazioni implicano la connessione solo al Server Dr.Web da cui è stata effettuata l'installazione.

2. Creare un account di postazione tramite il Pannello di controllo, come descritto nella sezione [Installazione di Agent Dr.Web attraverso il pacchetto di installazione individuale](#). Durante la creazione della postazione spuntare il flag **Crea un Server proxy associato** e definire le impostazioni proposte. In particolare, indicare il gruppo per il Server proxy Dr.Web, di cui le impostazioni sono state definite nel passaggio 1.



L'identificatore di Server proxy Dr.Web può essere modificato solo durante la creazione dell'account.

3. Avviare sulla postazione l'installazione di Agent Dr.Web dal pacchetto di installazione individuale che è stato creato nel passaggio 2.
4. Dopo l'installazione l'Agent Dr.Web scaricherà automaticamente dal Server Dr.Web l'installer di Server proxy Dr.Web e lo eseguirà in modalità background sulla stessa postazione. Il certificato e l'indirizzo del Server Dr.Web, nonché i dati di autenticazione per la connessione al Server Dr.Web verranno automaticamente inseriti nei relativi file di configurazione del Server proxy Dr.Web. Nelle impostazioni di Server proxy Dr.Web per il reindirizzamento del traffico verrà indicato solo il Server Dr.Web da cui è stata effettuata l'installazione.
5. Dopo l'installazione il Server proxy Dr.Web si conetterà al Server Dr.Web da cui è stata effettuata l'installazione per ottenere un file di configurazione completo. Se sul Server Dr.Web non sono state definite le impostazioni nel passaggio 1, il file di configurazione non verrà scaricato. La configurazione impostata dall'installer verrà utilizzata fino a quando non verrà impostata una configurazione sul Server Dr.Web connesso.
6. L'Agent Dr.Web si conetterà al Server Dr.Web solo attraverso il Server proxy Dr.Web installato. L'uso del Server proxy Dr.Web sarà trasparente per l'utente.

### 5.5.3. Installazione del Server proxy Dr.Web tramite l'installer



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



## Installazione del Server proxy Dr.Web in SO Windows

1. Creare un account di Server proxy Dr.Web tramite il Pannello di controllo, come descritto nella sezione [Creazione dell'account del Server proxy Dr.Web](#).
2. Scaricare l'installer di Server proxy Dr.Web dalla [pagina di installazione](#).
3. Copiare il certificato del Server Dr.Web a cui si conetterà il Server proxy Dr.Web (v. [Connessione del Server proxy Dr.Web al Server Dr.Web](#)) e l'installer sulla postazione su cui si intende effettuare l'installazione.
4. Avviare l'installer di Server proxy Dr.Web. Si apre la finestra **Installazione di Server proxy Dr.Web** con informazioni sul prodotto che viene installato. Premere il pulsante **Avanti**.
5. Nella finestra delle impostazioni generali di Server proxy Dr.Web nella sezione **Impostazioni di ascolto della rete** configurare i seguenti parametri principali:
  - Nel campo **Indirizzo per l'ascolto** impostare l'indirizzo IP su cui il Server proxy Dr.Web "è in ascolto". Di default "è in ascolto" su tutte le interfacce.



Gli indirizzi vengono impostati nel formato di indirizzo di rete riportato in documento **Allegati**, sezione [Allegato D. Specifica dell'indirizzo di rete](#).

- Nel campo **Porta** impostare il numero di porta su cui il Server proxy Dr.Web "è in ascolto". Di default è la porta 2193.
- Spuntare il flag **Attiva rilevamento** per attivare la modalità di simulazione del Server Dr.Web. Questa modalità consente ai client di rilevare il Server proxy Dr.Web come Server Dr.Web nel processo di sua ricerca attraverso le richieste broadcast.
- Spuntare il flag **Attiva trasmissione multicast** affinché il Server proxy Dr.Web risponda alle richieste broadcast indirizzate al Server Dr.Web.
  - Nel campo **Indirizzo di gruppo multicast** impostare l'indirizzo IP del gruppo multicast di cui farà parte il Server proxy Dr.Web. Sull'interfaccia indicata il Server proxy Dr.Web sarà in ascolto per interagire con i client che cercano i Server Dr.Web attivi. Se il campo viene lasciato vuoto, il Server proxy Dr.Web non farà parte di nessuno dei gruppi multicast. Di default il gruppo multicast di cui fa parte il Server Dr.Web è 231.0.0.1.

Nella sezione **Impostazioni di connessione client**:

- Dalla lista a cascata **Modalità di compressione** selezionare la modalità di compressione del traffico per i canali tra il Server proxy Dr.Web e i relativi client: Agent Dr.Web ed installer di Agent Dr.Web. Dalla lista a cascata **Livello** selezionare un livello di compressione (da 1 a 9).
- Dalla lista a cascata **Modalità di cifratura** selezionare la modalità di cifratura del traffico per i canali tra il Server proxy Dr.Web e i relativi client: Agent Dr.Web ed installer di Agent Dr.Web.

Informazioni dettagliate sulla cifratura e sulla compressione sono riportate nella sezione [Cifratura e compressione del traffico dati](#).

Premere il pulsante **Avanti**.



6. Configurare le impostazioni di reindirizzamento delle connessioni:

- Inserire l'indirizzo del Server Dr.Web su cui verranno reindirizzate le connessioni stabilite dal Server proxy Dr.Web e premere . Dopo l'installazione il Server proxy Dr.Web si conetterà a questo Server Dr.Web per ricevere la configurazione. Il certificato di questo Server Dr.Web è stato copiato sulla postazione nel passaggio 3.



Gli indirizzi vengono impostati nel formato di indirizzo di rete riportato in documento **Allegati**, sezione [Allegato D. Specifica dell'indirizzo di rete](#).

- Dalla lista a cascata **Crittografia** selezionare la modalità di cifratura del traffico per i canali di comunicazione tra il Server proxy Dr.Web e il Server Dr.Web impostato.
- Dalla lista a cascata **Compressione** selezionare la modalità di compressione del traffico per i canali di comunicazione tra il Server proxy Dr.Web e il Server Dr.Web impostato. Dalla lista a cascata **Livello** selezionare un livello di compressione (da 1 a 9).

Per aggiungere un altro Server Dr.Web alla lista di reindirizzamento traffico, inserire il suo indirizzo nel campo, premere il pulsante  e definire per esso le impostazioni di cifratura e compressione.

Per rimuovere l'ultimo indirizzo di Server Dr.Web aggiunto dalla lista di reindirizzamento traffico, premere il pulsante .



Al termine dell'installazione il Server proxy Dr.Web si conetterà al primo Server Dr.Web impostato in questa sezione per ricevere le impostazioni.

Se sul Server Dr.Web è definita la configurazione del Server proxy Dr.Web, tutte le impostazioni definite nell'installer verranno sovrascritte con la nuova configurazione ricevuta dal Server Dr.Web.

Dopo aver finito di modificare le impostazioni di reindirizzamento, premere il pulsante **Avanti**.

7. Si apre la finestra di configurazione della connessione con il Server Dr.Web per la gestione in remoto.

La connessione avverrà al primo Server Dr.Web specificato nel passaggio 6 per il reindirizzamento traffico.

- Nel campo **Certificato Server** impostare il file di certificato copiato sulla postazione nel passaggio 3. Per selezionare il file, premere il pulsante **Sfoggia**.
- Nei campi **Identificatore** e **Password** impostare le credenziali dell'account creato sul Server Dr.Web nel passaggio 1.

Premere **Avanti**.

8. Nella finestra **Impostazioni di memorizzazione nella cache** configurare le impostazioni di memorizzazione nella cache del Server proxy Dr.Web:

Spuntare il flag **Abilita la memorizzazione nella cache** per memorizzare nella cache i dati trasmessi dal Server proxy Dr.Web ed impostare i seguenti parametri:



- Nel campo **Periodo di rimozione delle revisioni (minuti)** impostare la periodicità di rimozione delle vecchie revisioni dalla cache nel caso in cui il loro numero ha superato il numero massimo consentito di revisioni conservate. Il valore viene impostato in minuti. Di default è di 60 minuti.
  - Nel campo **Numero di revisioni da conservare** impostare il numero massimo di revisioni di ciascun prodotto che rimarranno nella cache dopo una pulizia. Di default vengono conservate le ultime 3 revisioni, le revisioni più vecchie vengono rimosse.
- Nel campo **Periodo di scaricamento da memoria dei file inutilizzati (minuti)** impostare l'intervallo di tempo in minuti tra gli scaricamenti di file inutilizzati dalla memoria operativa. Di default è di 10 minuti.

Dopo aver configurato le impostazioni di memorizzazione nella cache, premere il pulsante **Avanti**.

9. Si apre una finestra che avvisa che il Server proxy Dr.Web è pronto per l'installazione. Se è necessario modificare i parametri di installazione aggiuntivi, in particolare, la directory di installazione di Server proxy Dr.Web e il percorso per il collocamento dei file utilizzati da Server proxy Dr.Web, premere **Parametri aggiuntivi**.  
Per iniziare l'installazione del Server proxy Dr.Web, premere il pulsante **Installa**.
10. Dopo il completamento del processo di installazione premere il pulsante **Esci**.
11. Dopo l'installazione il Server proxy Dr.Web si conatterà al Server Dr.Web indicato come primo nel passaggio 6 per ottenere un file di configurazione completo. Se sul Server Dr.Web non sono state definite le impostazioni, il file di configurazione non verrà scaricato. La configurazione impostata dall'installer verrà utilizzata fino a quando non verrà impostata una configurazione sul Server Dr.Web connesso.

## Installazione di Server proxy in SO della famiglia UNIX

1. Scaricare l'installer di Server proxy Dr.Web dalla [pagina di installazione](#).
2. Avviare l'installer di Server proxy Dr.Web tramite il seguente comando:  

```
./<file_del_pacchetto>.tar.gz.run
```
3. Per continuare l'installazione, accettare il contratto di licenza.
4. Indicare il percorso del certificato di Server Dr.Web. Il certificato può anche essere aggiunto dopo l'installazione di Server proxy Dr.Web (v. [Connessione del Server proxy Dr.Web al Server Dr.Web](#)).
5. Se necessario, possono essere utilizzati i file di configurazione da un'installazione precedente di Server proxy Dr.Web:
  - Per utilizzare una copia di backup memorizzata di default nella directory `/var/tmp/drwcsd-proxy`, premere INVIO.
  - Per utilizzare una copia di backup da un'altra directory, inserire manualmente il percorso della copia di backup.



- È inoltre possibile installare Server proxy Dr.Web con le impostazioni predefinite, senza utilizzare una copia di backup della configurazione da un'installazione precedente. Per fare ciò, premere 0.
6. Dopo l'installazione di Server proxy Dr.Web, se necessario, è possibile modificare manualmente i file di configurazione corrispondenti (v. [Connessione del Server proxy Dr.Web al Server Dr.Web](#)).

## Avvio e arresto

Nel corso dell'installazione del software sotto il sistema operativo **FreeBSD** viene creato uno script `rc /usr/local/etc/rc.d/dwcp_proxy`. Utilizzare i comandi:

- `/usr/local/etc/rc.d/dwcp_proxy stop` — per arrestare manualmente Server proxy Dr.Web;
- `/usr/local/etc/rc.d/dwcp_proxy start` — per avviare manualmente Server proxy Dr.Web.

Nel processo di installazione del software in SO **Linux** verrà creato uno script `init` per l'avvio e l'arresto di Server proxy Dr.Web `/etc/init.d/dwcp_proxy`.

## 5.5.4. Connessione del Server proxy Dr.Web al Server Dr.Web

A partire dalla versione 11 è fornita la possibilità di connessione di Server proxy Dr.Web a Server Dr.Web per la gestione remota delle impostazioni e il supporto della cifratura del traffico.

## Impostazioni di connessione

Per connettere il Server proxy Dr.Web al Server Dr.Web, è richiesto:

- **Certificato di Server Dr.Web** `drwcsd-certificate.pem`.

È necessaria la presenza dei certificati di tutti i Server Dr.Web a cui si connette il Server proxy Dr.Web e su cui viene reindirizzato il traffico client.

- Il certificato del Server Dr.Web è richiesto per la connessione al Server Dr.Web al fine di gestione delle impostazioni remota, nonché per il supporto della cifratura del traffico tra il Server Dr.Web e il Server proxy Dr.Web.
- Il certificato del Server proxy Dr.Web, che viene firmato con il certificato e la chiave privata del Server Dr.Web (la procedura viene effettuata automaticamente sul Server Dr.Web dopo la connessione e non richiede l'intervento dell'amministratore), è richiesto per la connessione degli Agent Dr.Web e per il supporto della cifratura del traffico tra gli Agent Dr.Web e il Server proxy Dr.Web.



Tutti i certificati dei Server Dr.Web sono memorizzati sul Server proxy Dr.Web nel file di configurazione `drwcsd-proxy-trusted.list` nel seguente formato (i record dei certificati sono separati da una o più righe vuote):

```
[<certificato_1>

[<certificato_2>

[<certificato_3>

...
```

- **Indirizzo di Server Dr.Web**

Il Server proxy Dr.Web si connette a tutti i Server Dr.Web che sono indicati nel suo file di configurazione per il reindirizzamento del traffico client. Tuttavia, la ricezione delle impostazioni è consentita solo da un determinato set di Server Dr.Web che sono contrassegnati come server di gestione. Se più Server Dr.Web sono contrassegnati come server di gestione, la connessione viene effettuata a tutti i Server Dr.Web uno dopo l'altro fino alla prima ricezione di una configurazione valida (non vuota).

- **L'identificatore e la password per l'accesso al Server Dr.Web.**

Le credenziali sono disponibili dopo la creazione di un account di Server proxy Dr.Web attraverso il Pannello di controllo (v. [Creazione dell'account del Server proxy Dr.Web](#)).



L'identificatore e la password di Server proxy Dr.Web vengono utilizzati in un unico esemplare. Su tutti i Server Dr.Web a cui si connette il Server proxy Dr.Web devono essere creati account di Server proxy Dr.Web con dati di autenticazione uguali.

I dati di autenticazione sono memorizzati sul Server proxy Dr.Web nel file di configurazione `drwcsd-proxy.auth` nel seguente formato:

```
[ <ID_del_Server_proxy> ]

[ <Password_del_Server_proxy> ]
```

## Connessione del Server proxy Dr.Web al Server Dr.Web



Per connettere il Server proxy Dr.Web, è necessario attivare il protocollo corrispondente sul lato Server Dr.Web. Per fare questo, nel Pannello di controllo nella sezione **Amministrazione** → **Configurazione del Server Dr.Web** → **Moduli** spuntare il flag **Protocollo di Server proxy Dr.Web**, salvare le impostazioni e riavviare il Server Dr.Web.



### Connessione automatica durante l'installazione in SO Windows:

- Se il Server proxy Dr.Web veniva installato [durante l'installazione di Agent Dr.Web](#) o [su una postazione con Agent Dr.Web](#) installato, la connessione al Server Dr.Web viene effettuata in modo automatico.
- Se il Server proxy Dr.Web veniva installato attraverso [l'installer grafico per SO Windows](#), la connessione al Server Dr.Web viene effettuata automaticamente in base ai parametri di connessione indicati dall'amministratore nelle impostazioni dell'installer.

Dopo l'installazione del Server proxy Dr.Web, i file per la connessione al Server Dr.Web di default si trovano nella directory: `C:\ProgramData\Doctor Web\drwcs\etc`.

### Connessione manuale durante l'installazione in SO della famiglia UNIX:

1. Installare il Server proxy Dr.Web per SO della famiglia UNIX secondo la procedura descritta nella sezione [Installazione del Server proxy Dr.Web tramite l'installer](#).
2. Creare un account di Server proxy Dr.Web tramite il Pannello di controllo, come descritto nella sezione [Creazione dell'account del Server proxy Dr.Web](#).
3. Copiare il certificato di Server Dr.Web sul computer su cui è installato il Server proxy Dr.Web.
4. Nel file di configurazione `drwcsd-proxy-trusted.list` indicare il certificato copiato sul computer nel passaggio 3: copiare il contenuto del file di certificato ed incollarlo nel file di configurazione secondo il formato descritto [sopra](#).
5. Nel file di configurazione `drwcsd-proxy.auth` definire le impostazioni di connessione al Server Dr.Web per l'account creato nel passaggio 2 secondo il formato descritto [sopra](#).

I file `drwcsd-proxy-trusted.list` e `drwcsd-proxy.auth` devono essere locati nelle seguenti directory:

- in caso di SO Linux: `/var/opt/drwcs/etc`
- in caso di SO FreeBSD: `/var/drwcs/etc`

È necessario impostare i seguenti permessi per i file:

```
drwcsd-proxy-trusted.list 0644 drwcs:drwcs  
drwcsd-proxy.auth 0600 drwcs:drwcs
```

### Connessione rapida tramite la riga di comando

Questa variante è particolarmente utile per SO della famiglia UNIX in quanto elimina la necessità di modificare manualmente i file di configurazione. Un comando unico può essere utilizzato per la connessione a un altro server, il reset delle impostazioni o in caso di problemi con la connessione esistente al server.

Utilizzare i seguenti comandi:

- SO Windows:



```
drwcsd-proxy deploy <server-address> <server-certificate> <proxy-login>
<proxy-password>
```

- SO Linux:

```
/etc/init.d/dwcp_proxy deploy <server-address> <server-certificate> <proxy-
login> <proxy-password>
```

- SO FreeBSD:

```
/usr/local/etc/rc.d/dwcp_proxy deploy <server-address> <server-certificate>
<proxy-login> <proxy-password>
```

In caso di connessione riuscita:

- Il nome utente e la password vengono scritti nel file di configurazione di Server proxy Dr.Web `drwcsd-proxy.auth`.
- Il certificato di Server Dr.Web viene scritto nel file di configurazione `drwcsd-proxy-trusted.list`.
- È stata generata una nuova chiave privata `drwcsd-proxy.pri`.
- Un nuovo certificato è stato generato, firmato sul server e aggiunto alla lista dei certificati del server proxy firmati (`drwcsd-proxy-signed.list`).
- Il file di configurazione è stato scaricato dal server e scritto nel file di configurazione `drwcsd-proxy.conf`.

## 5.6. Codici di errore restituiti nel processo di installazione

Se si verificano errori nel processo di installazione, verranno restituiti i seguenti codici di errore:

Codice di errore	Descrizione
0	Installazione completata con successo
1	Formato del comando non valido
2	Errore sconosciuto
3	Permessi insufficienti per completare l'operazione (permessi di scrittura nel registro, di creazione di file o di un'altra operazione necessaria per l'installazione)
4	Agent Dr.Web è già installato
5	L'installazione è già in esecuzione
7	L'installazione è stata annullata



Codice di errore	Descrizione
9	Superato il tempo di attesa di una risposta dal server
11	Permessi insufficienti per rimuovere l'applicazione
12	Versione del sistema operativo obsoleta
13	Rilevata applicazione incompatibile
14	L'installazione non è possibile, è necessario riavviare il sistema (il sistema è in attesa di riavvio prima del successivo tentativo di installazione)
15	Architettura del sistema operativo non supportata. Sono supportate solo x86 e x86_64
16	Il sistema operativo in uso non supporta l'algoritmo sha-2
50	La rimozione della versione standalone in background non è possibile

Per identificare la causa di un errore, è preferibile controllare i record del log. I codici di errore forniti sono generali, lo stesso errore può verificarsi per motivi diversi.



## Capitolo 6: Rimozione dei componenti di Dr.Web Enterprise Security Suite

### 6.1. Rimozione di Server Dr.Web

#### 6.1.1. Rimozione di Server Dr.Web per SO Windows

Per rimuovere il software Server Dr.Web o l'estensione del Pannello di controllo della sicurezza Dr.Web, avviare il pacchetto di installazione corrispondente alla versione del prodotto che è installata. L'installer determina automaticamente il prodotto software e offre di rimuoverlo. Per rimuovere il software, premere il pulsante **Rimuovi**.

Il software Server Dr.Web può anche essere rimosso tramite i mezzi standard SO Windows tramite l'elemento **Pannello di controllo** → **Installazione ed eliminazione programmi**.



Alla rimozione di Server Dr.Web il backup dei file di configurazione, delle chiavi di crittografia e del database viene eseguito solo se è attivata l'impostazione **Salva backup dei dati critici di Server Dr.Web**.

#### 6.1.2. Rimozione di Server Dr.Web per SO della famiglia UNIX



Tutte le azioni di rimozione si devono eseguire dall'account utente root (**root**).

##### Per rimuovere Server Dr.Web versione 10 e successive

SO di Server Dr.Web	Azione
FreeBSD	Eseguire lo script: <code>/usr/local/etc/drweb.com/software/drweb-esuite.remove</code>
Linux	Eseguire lo script: <code>/etc/opt/drweb.com/software/drweb-esuite.remove</code>



Quando il Server Dr.Web viene rimosso nei SO **FreeBSD** e **Linux**, i processi server verranno terminati automaticamente, il database, i file della chiave e di configurazione verranno copiati nella directory predefinita — `/var/tmp/drwcs` (l'elenco dei file per il



backup è riportato nella sezione [Aggiornamento di Server Dr.Web per SO della famiglia UNIX](#)).

Per annullare la copiatura di backup, è necessario dichiarare la variabile di ambiente `SKIP_BACKUP`. Il valore della variabile può essere qualsiasi. Per esempio:  
`SKIP_BACKUP="x"`

Inoltre, è possibile aggiungere la definizione di questa variabile al file `common.conf`.

## 6.2. Rimozione di Agent Dr.Web

Si può rimuovere l'Agent Dr.Web dalle postazioni protette nei seguenti modi:

- In caso delle postazioni SO Windows:
  - [Attraverso la rete tramite il Pannello di controllo](#).
  - [Localmente sulla postazione](#).
  - [Attraverso il servizio Active Directory](#), se l'Agent Dr.Web è stato installato attraverso questo servizio.
- In caso delle postazioni con SO Android, SO Linux, macOS — localmente sulla postazione.



La rimozione di Agent Dr.Web sulle postazioni SO Android, SO Linux, macOS è descritta nel **Manuale dell'utente** per il sistema operativo corrispondente.

### 6.2.1. Rimozione di Agent Dr.Web per SO Windows

#### Rimozione dell'Agent Dr.Web e del pacchetto antivirus in remoto



L'installazione e la rimozione del software Agent Dr.Web su remoto sono possibili solo in una rete locale e richiedono i privilegi di amministratore in questa rete.



Se Agent Dr.Web e il pacchetto antivirus vengono rimossi tramite il Pannello di controllo, la Quarantena dalla postazione non verrà rimossa.

#### Per rimuovere il software della postazione antivirus su remoto (solo in caso di SO della famiglia Windows)

1. Selezionare la voce **Rete antivirus** nel menu principale del Pannello di controllo.
2. Nella finestra che si è aperta, nella directory della rete antivirus selezionare il gruppo richiesto o postazioni antivirus separate.



3. Nella barra degli strumenti della directory di rete antivirus premere  **Generali** →  **Disinstalla Agent Dr.Web.**
4. Nella finestra che si è aperta **Disinstallazione di Agent Dr.Web**, se necessario, è possibile configurare i parametri di riavvio automatico delle postazioni selezionate dopo la rimozione di Agent Dr.Web:
  - La variante **Subito dopo la disinstallazione** prescrive alla postazione di riavviarsi 5 minuti dopo la rimozione di Agent Dr.Web.
  - La variante **All'ora impostata** consente di concretizzare l'ora di riavvio della postazione con passo di 1 ora.
  - La variante **Nel periodo impostato** dà la possibilità di indicare l'intervallo di tempo in cui verrà eseguito il riavvio.

Con qualsiasi variante di riavvio selezionata l'utente della postazione riceverà da Agent Dr.Web un avviso tempestivo sotto forma di finestra a comparsa.

Variante di riavvio	Avviso dell'utente
Non selezionata	La postazione non viene riavviata dopo la rimozione di Agent Dr.Web. Nessun avviso.
Subito dopo la disinstallazione	L'avviso compare 5 minuti prima del riavvio con l'indicazione dell'ora esatta in cui la postazione verrà riavviata.
All'ora impostata	<ul style="list-style-type: none"><li>• <b>Primo avviso</b> L'avviso compare subito dopo la rimozione di Agent Dr.Web e riporta l'ora esatta per cui è stato pianificato il riavvio.</li><li>• <b>Secondo avviso</b> L'avviso compare 5 minuti prima del riavvio con l'indicazione dell'ora esatta in cui la postazione verrà riavviata.</li><li>• <b>Se non c'è connessione con la postazione all'ora impostata</b> 15 minuti dopo il ripristino della connessione compare un avviso sul riavvio della postazione tra i prossimi 5 minuti con l'indicazione dell'ora esatta.</li></ul>
Nel periodo impostato	<ul style="list-style-type: none"><li>• <b>Primo avviso</b> L'avviso compare subito dopo la rimozione di Agent Dr.Web e riporta l'ora esatta nei limiti del periodo impostato in cui verrà eseguito il riavvio.</li><li>• <b>Secondo avviso</b> L'avviso compare 5 minuti prima del riavvio con l'indicazione dell'ora esatta in cui la postazione verrà riavviata.</li></ul>



Variante di riavvio	Avviso dell'utente
	<ul style="list-style-type: none"><li>• <b>Se non c'è connessione con la postazione nel periodo impostato</b></li></ul> <p>15 minuti dopo il ripristino della connessione compare un avviso sull'imminente riavvio il giorno successivo con l'indicazione dell'ora esatta nei limiti del periodo impostato.</p>

5. Il software Agent Dr.Web e il pacchetto antivirus verranno rimossi dalle postazioni selezionate.



Se il comando di avviare il processo di rimozione viene impartito in un momento in cui non c'è connessione tra il Server Dr.Web e la postazione antivirus, il software Agent Dr.Web sulla postazione selezionata verrà rimosso non appena tale connessione sarà ripristinata.

## Rimozione dell'Agent Dr.Web e del pacchetto antivirus in locale



Per la possibilità di rimozione in locale di Agent Dr.Web e del pacchetto antivirus questa opzione deve essere consentita sul Server Dr.Web nella sezione **Permessi** (v. **Manuale dell'amministratore**, p. [Permessi dell'utente della postazione](#)).

La rimozione del software antivirus della postazione (Agent Dr.Web e pacchetto antivirus) può essere effettuata in due modi:

1. [Tramite i mezzi standard di SO Windows.](#)
2. [Tramite l'installer di Agent Dr.Web.](#)



Se Agent Dr.Web e il pacchetto antivirus vengono rimossi tramite i mezzi standard di SO Windows o tramite l'installer di Agent Dr.Web, all'utente verrà restituita una richiesta di rimozione della Quarantena.

## Rimozione tramite i mezzi standard di SO Windows



Questo metodo di rimozione è disponibile solo se nel processo di installazione di Agent Dr.Web tramite l'installer grafico è stato spuntato il flag **Registra l'Agent Dr.Web nella lista dei programmi installati**.

Se Agent Dr.Web è stato installato in modalità background dell'installer, la rimozione del software antivirus tramite i mezzi standard sarà disponibile solo se nell'installazione è stata utilizzata l'opzione `/regagent yes`.

Per rimuovere Agent Dr.Web e il pacchetto antivirus tramite i mezzi standard di SO Windows, utilizzare l'elemento **Pannello di controllo** → **Installazione e eliminazione programmi** (le istruzioni dettagliate sono riportate nel **Manuale dell'utente** per Agent Dr.Web per Windows).



## Rimozione tramite l'installer

### • Modulo client win-es-agent-setup.exe

Per rimuovere il software Agent Dr.Web e il pacchetto antivirus tramite il modulo client che viene creato durante l'installazione di Agent Dr.Web, avviare il file di installazione `win-es-agent-setup.exe` con il parametro `/instMode remove`. In aggiunta utilizzare il parametro `/silent no` se è necessario controllare l'avanzamento della rimozione.

Il file di installazione `win-es-agent-setup.exe` di default si trova nella seguente directory:

- in caso di SO Windows XP e SO Windows Server 2003:  
`%ALLUSERSPROFILE%\Application Data\Doctor Web\Setup\`
- in caso di SO Windows Vista o versioni successive e SO Windows Server 2008 o versioni successive:  
`%ALLUSERSPROFILE%\Doctor Web\Setup\`

Per esempio, in caso di Windows 7, dove a `%ALLUSERPROFILE%` corrisponde `C:\ProgramData`:

```
C:\ProgramData\Doctor Web\Setup\win-es-agent-setup.exe /instMode  
remove /silent no
```

### • Pacchetto di installazione individuale `drweb_es_<SO>_<postazione>.exe`.

Per rimuovere il software Agent Dr.Web e il pacchetto antivirus tramite il pacchetto di installazione, avviare il file di installazione `drweb_es_<SO>_<postazione>.exe` della versione del prodotto che è installata.

### • Installer completo `drweb-<versione_agent>-<build>-esuite-agent-full-windows.exe`

Per rimuovere il software Agent Dr.Web e il pacchetto antivirus tramite l'installer completo, avviare il file di installazione `drweb-<versione_agent>-<build>-esuite-agent-full-windows.exe` della versione del prodotto che è installata.

### • Installer di rete `drwinst.exe`

Per rimuovere il software Agent Dr.Web e il pacchetto antivirus tramite l'installer di rete sulla postazione localmente, è necessario nella directory di installazione di Agent Dr.Web (di default è `C:\Program Files\DrWeb`) avviare l'installer `drwinst.exe` con il parametro `/instMode remove`. In aggiunta utilizzare il parametro `/silent no` se è necessario controllare l'avanzamento della rimozione.

Per esempio:

```
drwinst /instMode remove /silent no
```



All'avvio del pacchetto di installazione `drweb_es_<SO>_<postazione>.exe`, dell'installer completo `drweb-<versione_agent>-<build>-esuite-agent-full-windows.exe` e



dell'installer di rete `drwinst.exe`, viene avviato il modulo client `win-es-agent-setup.exe` che esegue direttamente la rimozione.

Il modulo client `win-es-agent-setup.exe` avviato senza parametri determina il prodotto installato e si avvia in modalità di modifica/rimozione. Per avviarlo subito in modalità di rimozione, utilizzare l'opzione `/instMode remove`.

## 6.2.2. Rimozione di Agent Dr.Web con utilizzo del servizio Active Directory



Per la possibilità di rimozione di Agent Dr.Web questa opzione deve essere consentita sul Server Dr.Web nella sezione **Permessi** (v. **Manuale dell'amministratore**, p. [Permessi dell'utente della postazione](#)).

1. Nel Pannello di controllo del SO Windows, nel menu **Amministrazione** selezionare l'elemento **Active Directory - utenti e computer**.
2. Nel dominio selezionare l'Unità organizzativa **ESS** creata. Dal menu contestuale selezionare la voce **Proprietà**. Si apre la finestra **Proprietà ESS**.
3. Passare alla scheda **Criteri di gruppo**. Selezionare l'elemento dell'elenco con il nome **Criteri ESS**. Fare doppio clic su di esso. Si apre la finestra **Editor di oggetti della politica di gruppo**.
4. Nella lista gerarchica selezionare **Configurazione computer** → **Impostazioni del software** → **Installazione software** → **Pacchetto**. In seguito, dal menu contestuale del pacchetto Agent Dr.Web selezionare **Tutte le attività** → **Elimina** → **OK**.
5. Nella scheda **Criteri di gruppo** fare clic su **OK**.
6. L'Agent Dr.Web verrà rimosso dai computer al momento della successiva registrazione nel dominio.

## 6.3. Rimozione di Server di scansione Dr.Web



L'operazione di rimozione deve essere eseguita dall'account di superutente (**root**).

Prima di rimuovere Server di scansione, assicurarsi che non ci siano postazioni nella rete antivirus configurate per l'interazione con esso. In caso contrario, queste postazioni rimarranno senza protezione.

### Per rimuovere Server di scansione Dr.Web

1. Sulla macchina virtuale nominata Server di scansione passare alla directory `/opt/drweb.com/bin`.



2. Eseguire lo script `uninst.sh`.
3. Sullo schermo comparirà il testo dell'invito alla rimozione. Per iniziare la procedura di rimozione, rispondere *Yes* o *Y* alla domanda "Do you want to continue?". Per rifiutare la rimozione di Server di scansione Dr.Web, inserire *No* o *N*. In questo caso il funzionamento del programma di rimozione terminerà.
4. Dopo la conferma verrà avviata la procedura di rimozione di tutti i pacchetti di Server di scansione Dr.Web. Sullo schermo verranno visualizzati i record che vengono registrati nel log e riflettono lo stato di avanzamento del processo di rimozione.
5. Al termine del processo il funzionamento del programma di rimozione terminerà automaticamente.

## 6.4. Rimozione del Server proxy Dr.Web

**Il Server proxy può essere rimosso in uno dei seguenti modi:**

1. [Localmente](#).

La rimozione in locale viene effettuata dall'amministratore direttamente sul computer su cui è installato il Server proxy.

2. [In remoto](#).

La rimozione del Server proxy in remoto viene effettuata nel Pannello di controllo tramite LAN ed è disponibile nel caso in cui il Server proxy è connesso al Server Dr.Web.

### 6.4.1. Rimozione del Server proxy Dr.Web in locale



Server proxy Dr.Web può essere rimosso in locale dal computer solo se è stato installato anche in locale, tramite l'installer. In caso contrario, seguire le istruzioni dalla sezione [Rimozione del Server proxy Dr.Web in remoto](#).

### In caso di SO Windows



Alla rimozione del Server proxy i suoi file di configurazione non vengono rimossi e rimangono nella directory `%ALLUSERSPROFILE%\Doctor Web\`.

Server proxy Dr.Web installato su SO Windows può essere rimosso con i mezzi standard del sistema operativo o tramite l'installer.

### Eliminazione tramite i mezzi standard

Utilizzare l'elemento **Pannello di controllo** → **Installazione ed eliminazione programmi** (**Programmi e funzionalità** in caso di SO Windows 2008 o versioni successive).



## Eliminazione tramite l'installer

### • Modulo client proxy-setup.exe

Per la rimozione tramite il modulo client che viene creato durante l'installazione di Server proxy, eseguire il file di installazione `proxy-setup.exe` con il parametro `/instMode remove`. In aggiunta utilizzare il parametro `/silent no` se è necessario controllare l'avanzamento della rimozione.

Il file di installazione `proxy-setup.exe` di default si trova nella seguente directory:

- in caso di SO Windows XP e SO Windows Server 2003:  
%ALLUSERSPROFILE%\Application Data\Doctor Web\Setup\drweb-win-proxy\  
proxy\
- in caso di SO Windows Vista o versioni successive e SO Windows Server 2008 o versioni successive:  
%ALLUSERSPROFILE%\Doctor Web\Setup\drweb-win-proxy\  
proxy\

Esempio del comando per l'avvio del modulo su Windows 10, dove %ALLUSERPROFILE% corrisponde a C:\ProgramData:

```
C:\ProgramData\Doctor Web\Setup\drweb-win-proxy\proxy-setup.exe /instMode  
remove /silent no
```

### • Installer drweb-proxy-<versione\_pacchetto>-<build>-windows-nt-<numero\_di\_bit>.exe

Per rimuovere il Server proxy tramite l'installer, scaricare dalla [pagina di installazione](#) ed eseguire il file di installazione `drweb-proxy-<versione_pacchetto>-<build>-windows-nt-<numero_di_bit>.exe`. Seguire le istruzioni.

## In caso di SO della famiglia UNIX



Alla rimozione del Server proxy, nella directory `/var/tmp/drwcd-proxy` viene automaticamente salvata una copia di backup dei file di configurazione.

SO del Server proxy	Azione
FreeBSD	Eseguire lo script:  <code>/usr/local/etc/drweb.com/software/drweb-esuite-proxy.remove</code>
Linux	Eseguire lo script:  <code>/etc/opt/drweb.com/software/drweb-proxy.remove</code>



## 6.4.2. Rimozione del Server proxy Dr.Web in remoto

La rimozione del Server proxy in remoto è disponibile nel caso in cui il Server proxy è connesso al Server Dr.Web (v. [Connessione del Server proxy Dr.Web al Server Dr.Web](#)).



Se l'account Server proxy viene rimosso nel Pannello di controllo, il Server proxy stesso viene rimosso dalla postazione.

### Per rimuovere il Server proxy

1. Selezionare la voce **Rete antivirus** nel menu principale del Pannello di controllo.
2. Nella finestra che si è aperta, nella lista gerarchica fare clic sul nome di uno o più Server proxy che si vuole rimuovere.
3. Nella barra degli strumenti premere **Generali** → **Rimuovi gli oggetti selezionati**.
4. Si apre la finestra di conferma della rimozione dell'oggetto. Fare clic su **OK**.

### Per rimuovere il Server proxy che è installato sulla postazione associata

1. Selezionare la voce **Rete antivirus** nel menu principale del Pannello di controllo.
2. Aprire la sezione delle proprietà della postazione su cui è installato il Server proxy in uno dei seguenti modi:
  - a) Premere il nome della postazione nella lista gerarchica della rete antivirus. Nella parte destra della finestra del Pannello di controllo si apre automaticamente una sezione con le proprietà della postazione.
  - b) Selezionare la voce **Proprietà** del menu di gestione. Si apre la finestra con le proprietà della postazione.
3. Nella finestra delle proprietà della postazione passare alla sezione **Server proxy**.
4. Premere **Rimuovi Server proxy**.
5. Fare clic su **Salva**. Il Server proxy verrà disinstallato dalla postazione. L'account del Server proxy verrà rimosso dal Server Dr.Web.



## Capitolo 7: Aggiornamento dei componenti di Dr.Web Enterprise Security Suite



L'aggiornamento di Server Dr.Web dalle versioni 12 alla versione 13 è disponibile tramite il Pannello di controllo. La procedura è descritta in **Manuale dell'amministratore**, sezione [Aggiornamento di Server Dr.Web e ripristino da copia di backup](#).

Prima di cominciare ad aggiornare Dr.Web Enterprise Security Suite e singoli componenti, notare le seguenti importanti caratteristiche:

- Prima dell'inizio dell'aggiornamento si consiglia vivamente di controllare la correttezza delle impostazioni del protocollo TCP/IP per la possibilità di accesso a internet. In particolare, il servizio DNS deve essere attivato e contenere le impostazioni corrette.
- Prima di aggiornare Server Dr.Web, si consiglia di aggiornare tutti i componenti della rete antivirus Dr.Web Enterprise Security Suite, inclusi Agent Dr.Web, all'ultima versione disponibile su SAM.
- Nel caso di configurazione di rete antivirus con diversi server, è necessario tenere presente che tra i Server Dr.Web versione 13 e i Server Dr.Web versioni 6 la trasmissione di aggiornamenti tra server non viene effettuata, e la comunicazione tra i server viene utilizzata solo per la trasmissione delle statistiche. Per assicurare la trasmissione degli aggiornamenti tra i server, è necessario aggiornare tutti i Server Dr.Web. Se è necessario lasciare nella rete antivirus i Server Dr.Web di versioni precedenti per la connessione degli Agent Dr.Web installati su sistemi operativi non supportati dalla versione 13 (v. [Aggiornamento di Agent Dr.Web](#)), i Server Dr.Web versioni 6 e i Server Dr.Web versione 13 devono ricevere aggiornamenti in modo indipendente.
- L'aggiornamento del cluster di Server Dr.Web dalla versione 11 alla versione 13 deve essere eseguito separatamente, cioè i nodi devono essere disconnessi dal cluster uno per uno, associati al database interno e aggiornati, dopodiché devono essere nuovamente collegati uno per uno al cluster comune.
- Per una rete antivirus in cui viene utilizzato il Server proxy Dr.Web, in caso di aggiornamento dei componenti alla versione 13, è necessario aggiornare anche il Server proxy alla versione 13. Altrimenti la connessione degli Agent Dr.Web forniti con la versione 13 al Server Dr.Web versione 13 non sarà possibile. Si consiglia di effettuare l'aggiornamento nel seguente ordine: Server Dr.Web → Server proxy Dr.Web → Agent Dr.Web.
- Durante l'aggiornamento di Server Dr.Web le impostazioni del repository non vengono trasferite nella nuova versione (vengono resettate ai valori di default), tuttavia, viene eseguito un back delle impostazioni. Se necessario, configurare le impostazioni del repository manualmente dopo l'aggiornamento di Server Dr.Web.
- Se il Server Dr.Web è aggiornato alla 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.

## 7.1. Aggiornamento di Server Dr.Web per SO Windows

Sono disponibili le seguenti varianti di aggiornamento:

- L'aggiornamento di Server Dr.Web versione 11 o versioni successive viene eseguito automaticamente tramite l'installer.
- L'aggiornamento di Server Dr.Web versione 12 o versioni successive è disponibile tramite il Pannello di controllo. La procedura è descritta in **Manuale dell'amministratore**, sezione [Aggiornamento di Server Dr.Web e ripristino da copia di backup](#).



Se è richiesto l'aggiornamento dalla versione 6 o 10, è necessario prima eseguire l'aggiornamento alla versione 11, e quindi alla versione 13.

Prima di iniziare l'aggiornamento di Server Dr.Web, prestare attenzione alla sezione [Aggiornamento di Agent Dr.Web](#).



Non tutti gli aggiornamenti di Server Dr.Web all'interno della versione 13 contengono il file di pacchetto. Alcuni di essi possono essere installati solo tramite il Pannello di controllo.

### Salvataggio dei file di configurazione

In caso di aggiornamento di Server Dr.Web alla versione 13 tramite l'installer, i file di configurazione vengono salvati nella directory che viene specificata nell'impostazione **Salva backup dei dati critici di Server Dr.Web** nel processo di aggiornamento (di default è `<disco_di_installazione>.\DrWeb Backup`).

Vengono salvati i seguenti file di configurazione:

File	Descrizione
agent.key (il nome può essere diverso)	chiave di licenza di Agent Dr.Web
auth-ads.conf	file di configurazione per l'autenticazione esterna degli amministratori attraverso Active Directory
auth-radius.conf	file di configurazione per l'autenticazione esterna degli amministratori attraverso RADIUS



File	Descrizione
<code>auth-ldap.conf</code>	file di configurazione per l'autenticazione esterna degli amministratori attraverso LDAP
<code>auth-ldap-rfc4515.conf</code>	file di configurazione dell'autenticazione esterna degli amministratori attraverso LDAP in base a uno schema semplificato
<code>auth-ldap-rfc4515-check-group.conf</code>	modello di file di configurazione dell'autenticazione esterna degli amministratori attraverso LDAP in base a uno schema semplificato con la verifica dell'appartenenza al gruppo di Active Directory
<code>auth-ldap-rfc4515-check-group-novar.conf</code>	modello di file di configurazione dell'autenticazione esterna degli amministratori attraverso LDAP in base a uno schema semplificato con la verifica dell'appartenenza al gruppo di Active Directory con l'uso delle variabili
<code>auth-ldap-rfc4515-simple-login.conf</code>	modello di file di configurazione dell'autenticazione esterna degli amministratori attraverso LDAP in base a uno schema semplificato
<code>auth-pam.conf</code>	file di configurazione per l'autenticazione esterna degli amministratori attraverso PAM
<code>enterprise.key</code> (il nome può essere diverso)	chiave di licenza di Server Dr.Web. Viene salvata se era presente dopo l'aggiornamento da versioni precedenti. In caso di installazione di un nuovo Server Dr.Web 13 è assente
<code>drwcsd-certificate.pem</code>	certificato di Server Dr.Web
<code>download.conf</code>	impostazioni di rete per la generazione dei pacchetti di installazione di Agent Dr.Web
<code>drwcsd.conf</code> (il nome può essere diverso)	file di configurazione del Server Dr.Web.
<code>drwcsd.conf.distr</code>	modello di file di configurazione di Server Dr.Web con i parametri di default
<code>drwcsd.pri</code>	chiave di cifratura privata
<code>dbexport.gz</code>	esportazione del database
<code>drwcsd.pub</code> (il nome può essere diverso)	chiave di cifratura pubblica
<code>frontdoor.conf</code>	file di configurazione per l'utility di diagnostica remota del Server Dr.Web
<code>openssl.cnf</code>	certificato di Server Dr.Web per HTTPS
<code>webmin.conf</code>	file di configurazione del Pannello di controllo



File	Descrizione
yalocator.apikey	Chiave API per l'Estensione Yandex Locator

Se necessario, salvare altri file importanti in un percorso diverso dalla directory di installazione di Server Dr.Web, per esempio, modelli di report che si trovano nella directory `\var\templates`.

## Salvataggio del database



Prima dell'aggiornamento, assicurarsi che nel DBMS Microsoft SQL sia indicato l'ordinamento con distinzione tra maiuscole e minuscole (suffisso `_CS`) e con considerazione di segni diacritici (suffisso `_AS`). In caso contrario, l'aggiornamento automatico non sarà possibile.

Prima dell'aggiornamento, assicurarsi inoltre che il DBMS utilizzato sia supportato dal Server Dr.Web versione 13. In caso contrario, l'aggiornamento automatico non sarà possibile. La lista dei DBMS supportati è riportata in documento **Allegati**, in [Allegato A. Impostazioni per l'utilizzo dei DBMS. Parametri dei driver dei DBMS](#).

Prima di aggiornare il software Dr.Web Enterprise Security Suite, si consiglia di eseguire il backup del database.

### Per salvare il database

1. Arrestare Server Dr.Web.
2. Esportare il database nel file:
  - in caso di Server Dr.Web fino alla versione 13

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -verbosity=all exportdb <directory_di_backup>\esbase.es
```

- in caso di Server Dr.Web a partire dalla versione 13

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -verbosity=all modexecdb database-export <directory_di_backup>\esbase.es
```

In caso di Server Dr.Web che utilizzano un database esterno, si consiglia di utilizzare gli strumenti standard forniti insieme al database.



Assicurarsi che l'esportazione del database di Dr.Web Enterprise Security Suite sia completata con successo. Se non sarà disponibile una copia di backup del database, non

sarà possibile ripristinare il Server Dr.Web in caso di circostanze impreviste.

## Aggiornamento di Server Dr.Web

Per aggiornare il Server Dr.Web, eseguire il file del pacchetto.



Di default, come lingua dell'installer viene selezionata la lingua del sistema operativo. Se necessario, si può cambiare la lingua di installazione in qualsiasi passo, selezionando la voce corrispondente nell'angolo superiore destro della finestra di installer.

Se viene utilizzato un database esterno di Server Dr.Web, nel processo di aggiornamento selezionare inoltre l'opzione **Utilizza il database esistente**.



Se si intende utilizzare come database esterno il database Oracle attraverso la connessione ODBC, nel corso dell'installazione (l'aggiornamento) di Server Dr.Web nelle impostazioni dell'installer annullare l'installazione del client incorporato per il DBMS Oracle (nella sezione **Supporto dei database** → **Driver del database Oracle**).

Altrimenti, l'utilizzo del database Oracle attraverso ODBC non sarà possibile per conflitto di librerie.

1. In caso di aggiornamento dalla versione 11, 12 e all'interno della versione 13, si aprirà una finestra che informa sulla presenza di un software Server Dr.Web di versione precedente installato e fornisce una breve descrizione del processo di aggiornamento alla nuova versione. Per iniziare a configurare la procedura di aggiornamento, premere il pulsante **Aggiorna**.
2. Si aprirà una finestra per la configurazione di un backup dei dati critici prima della rimozione del Server Dr.Web versione precedente. È consigliabile impostare il flag **Salva backup dei dati critici di Server Dr.Web**. Se necessario, è possibile modificare la directory per il backup impostata di default (<disco\_di\_installazione>:\DrWeb Backup). Per iniziare il processo di rimozione della versione precedente di Server Dr.Web, premere **Rimuovi**.
3. Al termine della rimozione della versione precedente di Server Dr.Web inizia l'installazione della nuova versione. Si apre una finestra con informazioni sul prodotto e con un link al testo del contratto di licenza. Dopo aver letto le condizioni del contratto di licenza, per continuare l'aggiornamento, spuntare il flag **Accetto le condizioni del Contratto di licenza** e premere il pulsante **Avanti**.
4. Nei passaggi successivi viene eseguita la configurazione di Server Dr.Web con l'utilizzo del [database esistente](#) (in modo simile al processo di [Installazione di Server Dr.Web](#) in base ai [file di configurazione](#) dalla versione precedente). L'installer determina automaticamente la directory di installazione di Server Dr.Web, la posizione dei file di configurazione e del



database incorporato dall'installazione precedente. Se necessario, è possibile modificare i percorsi dei file che sono stati trovati automaticamente dall'installer.

5. Per iniziare il processo di installazione di Server Dr.Web versione 13, premere il pulsante **Installa**.



Dopo il completamento degli aggiornamenti dei Server Dr.Web della rete antivirus, è necessario:

1. Configurare nuovamente le impostazioni di cifratura e compressione dei Server Dr.Web associati (v. **Manuale dell'amministratore**, sezione [Configurazione delle relazioni tra i Server Dr.Web](#)).
2. Cancellare la cache del browser utilizzato per la connessione al Pannello di controllo.

## 7.2. Aggiornamento di Server Dr.Web per SO della famiglia UNIX

Server Dr.Web può essere aggiornato alla versione 13 in più modi:

- L'aggiornamento di Server Dr.Web versione 11 o versioni successive per i tipi di pacchetti uguali viene eseguito automaticamente tramite l'installer per tutti i sistemi operativi della famiglia UNIX. Se desiderato, è anche possibile effettuare l'aggiornamento manualmente.
- L'aggiornamento di Server Dr.Web versione 12 o versioni successive è inoltre disponibile tramite il Pannello di controllo. La procedura è descritta in **Manuale dell'amministratore**, sezione [Aggiornamento di Server Dr.Web e ripristino da copia di backup](#).



Prima di iniziare l'aggiornamento di Server Dr.Web, prestare attenzione alla sezione [Aggiornamento di Agent Dr.Web](#).



L'aggiornamento di Server Dr.Web all'interno della versione 13 può inoltre essere eseguito tramite il Pannello di controllo. La procedura è descritta in **Manuale dell'amministratore**, sezione [Aggiornamento di Server Dr.Web e ripristino da copia di backup](#).

---

Non tutti gli aggiornamenti di Server Dr.Web all'interno della versione 13 contengono il file di pacchetto. Alcuni di essi possono essere installati solo tramite il Pannello di controllo.



## Salvataggio dei file di configurazione

Alla rimozione e all'aggiornamento automatico del Server Dr.Web alla versione 13 i file di configurazione vengono salvati nella directory impostata per il backup di default: `/var/tmp/drwcs/`.

Alla rimozione di Server Dr.Web vengono salvati i seguenti file di configurazione:

File	Descrizione
<code>agent.key</code> (il nome può essere diverso)	chiave di licenza di Agent Dr.Web
<code>auth-ldap.conf</code>	file di configurazione per l'autenticazione esterna degli amministratori attraverso LDAP
<code>auth-ldap-rfc4515.conf</code>	file di configurazione dell'autenticazione esterna degli amministratori attraverso LDAP in base a uno schema semplificato
<code>auth-pam.conf</code>	file di configurazione per l'autenticazione esterna degli amministratori attraverso PAM
<code>auth-radius.conf</code>	file di configurazione per l'autenticazione esterna degli amministratori attraverso RADIUS
<code>certificate.pem</code>	certificato per SSL
<code>common.conf</code>	file di configurazione (per alcuni SO della famiglia UNIX)
<code>dbexport.gz</code>	esportazione del database (viene creato nel processo di rimozione del Server Dr.Web dal comando <code>drwcs.sh xmlexportdb</code> )
<code>download.conf</code>	impostazioni di rete per la generazione dei pacchetti di installazione di Agent Dr.Web
<code>drwcsd-certificate.pem</code>	certificato di Server Dr.Web
<code>drwcsd.conf</code> (il nome può essere diverso)	file di configurazione del Server Dr.Web.
<code>drwcsd.pri</code>	chiave di cifratura privata
<code>drwcsd.pub</code> (il nome può essere diverso)	chiave di cifratura pubblica
<code>enterprise.key</code> (il nome può essere diverso)	chiave di licenza di Server Dr.Web. Viene salvata se era presente dopo l'aggiornamento da versioni precedenti. In caso di installazione di un nuovo Server Dr.Web 13 è assente



File	Descrizione
frontdoor.conf	file di configurazione per l'utility di diagnostica remota del Server Dr.Web
local.conf	impostazioni del log di Server Dr.Web
private-key.pem	chiave privata RSA
webmin.conf	file di configurazione del Pannello di controllo
yalocator.apikey	Chiave API per l'Estensione Yandex Locator

Nel caso di [aggiornamento automatico](#) nella directory per il backup vengono salvati i seguenti file:

File	Descrizione
auth-ldap.conf	file di configurazione per l'autenticazione esterna degli amministratori attraverso LDAP
auth-ldap-ldap-rfc4515.conf	file di configurazione dell'autenticazione esterna degli amministratori attraverso LDAP in base a uno schema semplificato
auth-pam.conf	file di configurazione per l'autenticazione esterna degli amministratori attraverso PAM
auth-radius.conf	file di configurazione per l'autenticazione esterna degli amministratori attraverso RADIUS
db.backup.gz	esportazione del database (viene creato nel processo di aggiornamento del Server Dr.Web dal comando <code>drwcs.sh exportdb</code> )

## Salvataggio del database

Prima di aggiornare il software Dr.Web Enterprise Security Suite, si consiglia di eseguire il backup del database.

### Per salvare il database

1. Arrestare Server Dr.Web.
2. Esportare il database nel file:
  - In caso di SO FreeBSD:

- in caso di Server Dr.Web fino alla versione 13

```
# /usr/local/etc/rc.d/drwcsd exportdb /var/tmp/esbase.es
```



- in caso di Server Dr.Web a partire dalla versione 13

```
# /usr/local/etc/rc.d/drwcsd modexecdb database-export /var/tmp/esbase.es
```
- In caso di SO Linux:
  - in caso di Server Dr.Web fino alla versione 13

```
# /etc/init.d/drwcsd exportdb /var/tmp/esbase.es
```
  - in caso di Server Dr.Web a partire dalla versione 13

```
# /etc/init.d/drwcsd modexecdb database-export /var/tmp/esbase.es
```

In caso di Server Dr.Web che utilizzano un database esterno, si consiglia di utilizzare gli strumenti standard forniti insieme al database.



Assicurarsi che l'esportazione del database di Dr.Web Enterprise Security Suite sia completata con successo. Se non sarà disponibile una copia di backup del database, non sarà possibile ripristinare il Server Dr.Web in caso di circostanze impreviste.

## Aggiornamento automatico

L'aggiornamento di Server Dr.Web versione 11 o versioni successive per i tipi di pacchetti uguali viene eseguito automaticamente per tutti i sistemi operativi della famiglia UNIX.

In questo caso i [file di configurazione](#) verranno convertiti automaticamente e collocati nelle directory richieste. Inoltre, alcuni [file di configurazione](#) vengono salvati nella directory per il backup.

## Aggiornamento manuale

Se non è possibile effettuare l'aggiornamento di Server Dr.Web dalla versione 11 e successive sopra il pacchetto già installato, è necessario rimuovere il software Server Dr.Web delle versioni precedenti salvando una copia di backup e installare il software versione 13 sulla base della copia di backup salvata.

### Per aggiornare Server Dr.Web

1. Arrestare Server Dr.Web.
2. Se si vogliono utilizzare in seguito alcuni file (oltre ai [file](#) che verranno salvati in automatico nel processo di rimozione di Server Dr.Web nel passaggio **3**), creare manualmente i backup di questi file, per esempio, di modelli di report ecc.
3. Rimuovere il software Server Dr.Web (v. [Rimozione di Server Dr.Web per SO della famiglia UNIX](#)). Verrà automaticamente chiesto di salvare le copie di backup dei [file](#). Per fare ciò, basta inserire il percorso per il salvataggio o accettare il percorso proposto di default.
4. Installare il Server Dr.Web versione 13 secondo la procedura di installazione standard (v. [Installazione di Server Dr.Web per SO della famiglia UNIX](#)) sulla base della copia di backup



creata nel passaggio 3. Tutti i file di configurazione salvati e il database incorporato (nel caso di utilizzo del database incorporato) verranno convertiti automaticamente per l'uso dal Server Dr.Web versione 13. Senza la conversione automatica non è possibile utilizzare il database (nel caso di utilizzo del database incorporato) e alcuni file di configurazione del Server Dr.Web delle versioni precedenti.

Se alcuni file sono stati salvati manualmente, metterli nelle stesse directory in cui si trovavano nella versione precedente di Server Dr.Web.



Per tutti i file salvati dalla versione precedente di Server Dr.Web (v. passaggio 4) è necessario impostare come proprietario di file l'utente selezionato durante l'installazione della nuova versione di Server Dr.Web (di default è **drwcs**).

5. Avviare il Server Dr.Web.
6. Configurare l'aggiornamento del repository ed aggiornarlo completamente.



Dopo il completamento degli aggiornamenti dei Server Dr.Web della rete antivirus, è necessario configurare nuovamente le impostazioni di cifratura e compressione dei Server Dr.Web associati (v. **Manuale dell'amministratore**, sezione [Configurazione delle relazioni tra i Server Dr.Web](#)).

## 7.3. Aggiornamento di Agent Dr.Web

L'aggiornamento di Agent Dr.Web successivo all'aggiornamento del software Server Dr.Web è descritto per le seguenti varianti:

1. [Aggiornamento di Agent Dr.Web per le postazioni SO Windows](#),
2. [Aggiornamento di Agent Dr.Web per le postazioni SO Android](#),
3. [Aggiornamento di Agent Dr.Web per le postazioni SO Linux e macOS](#).

### 7.3.1. Aggiornamento di Agent Dr.Web per le postazioni SO Windows

#### Aggiornamento di Agent Dr.Web forniti con Dr.Web Enterprise Security Suite 10

L'aggiornamento degli Agent Dr.Web forniti con la versione Dr.Web Enterprise Security Suite 10 viene eseguito in modo automatico.

Dopo l'aggiornamento automatico viene visualizzato un avviso pop-up di necessità di riavvio; nel Pannello di controllo nello status della postazione viene segnata la necessità di riavvio dopo l'aggiornamento. Per completare l'aggiornamento, riavviare la postazione localmente o in remoto attraverso il Pannello di controllo.



Nel caso di connessione della postazione al Server Dr.Web attraverso il Server proxy Dr.Web versione 10 o precedenti, prima di aggiornare l'Agent Dr.Web, è necessario aggiornare il Server proxy alla versione 13 o rimuovere il Server proxy.



A causa di supporto terminato della 10 versione, un aggiornamento riuscito dalla 10 versione a quella 13 non è garantito. In questo caso, è necessario aggiornare prima a quella 11, e quindi alla 13 versione.

## Aggiornamento automatico di Agent Dr.Web forniti con Dr.Web Enterprise Security Suite 6

Per la possibilità di aggiornamento automatico devono essere soddisfatte le seguenti condizioni:

1. Gli Agent Dr.Web devono essere installati su computer con i sistemi operativi della famiglia Windows supportati per l'installazione di Agent Dr.Web per Dr.Web Enterprise Security Suite versione 13.0 (v. [Requisiti di sistema](#)).
2. Quando si esegue l'aggiornamento automatico, sono possibili le seguenti varianti delle azioni a seconda delle impostazioni di Server Dr.Web:
  - a) [L'aggiornamento automatico](#) viene eseguito se all'aggiornamento di Server Dr.Web sono state salvate le chiavi di crittografia e le impostazioni di rete del Server Dr.Web precedente.
  - b) [Durante l'aggiornamento automatico è necessaria una configurazione manuale](#) se all'aggiornamento di Server Dr.Web sono state impostate nuove chiavi di crittografia e impostazioni di rete di Server Dr.Web.



Nel corso dell'aggiornamento automatico, prestare attenzione alle seguenti caratteristiche:

1. Dopo la rimozione di Agent Dr.Web l'avviso di necessità di riavvio della postazione non viene visualizzato. L'amministratore deve lanciare manualmente il riavvio della postazione.
2. Nell'intervallo tra la rimozione della vecchia versione di Agent Dr.Web e l'installazione della nuova versione, le postazioni saranno senza protezione antivirus.
3. Dopo un aggiornamento di Agent Dr.Web senza riavvio della postazione, il funzionamento del software antivirus sarà limitato. In tale caso non è assicurata la completa protezione antivirus della postazione. È necessario che l'utente riavvii la postazione su richiesta di Agent Dr.Web.

### L'aggiornamento automatico di Agent Dr.Web viene eseguito secondo il seguente schema:

1. Quando viene lanciato l'aggiornamento, viene rimossa la vecchia versione di Agent Dr.Web.
2. La postazione viene riavviata manualmente.



3. Viene installata la nuova versione di Agent Dr.Web. A questo scopo, viene creato automaticamente un task nel calendario di Server Dr.Web.
4. Al termine dell'aggiornamento di Agent Dr.Web, la postazione si connette automaticamente al Server Dr.Web. Nella sezione **Stato** del Pannello di controllo per la postazione aggiornata verrà visualizzato un avviso di necessità di riavvio. È necessario riavviare la postazione.

**L'aggiornamento automatico di Agent Dr.Web con configurazione manuale viene eseguito secondo il seguente schema:**

1. Modificare manualmente le impostazioni di connessione al nuovo Server Dr.Web e sostituire la chiave di cifratura pubblica sulla postazione.
2. Dopo la modifica delle impostazioni sulla postazione e la connessione della postazione al Server Dr.Web viene avviato il processo di aggiornamento dell'Agent.
3. Quando viene lanciato l'aggiornamento, viene rimossa la vecchia versione di Agent Dr.Web.
4. La postazione viene riavviata manualmente.
5. Viene installata la nuova versione di Agent Dr.Web. A questo scopo, viene creato automaticamente un task nel calendario di Server Dr.Web.
6. Al termine dell'aggiornamento di Agent Dr.Web, la postazione si connette automaticamente al Server Dr.Web. Nella sezione **Stato** del Pannello di controllo per la postazione aggiornata verrà visualizzato un avviso di necessità di riavvio. È necessario riavviare la postazione.

## Aggiornamento manuale di Agent Dr.Web forniti con Dr.Web Enterprise Security Suite 6

Se l'installazione di nuova versione di Agent Dr.Web con aggiornamento automatico non è riuscita per qualche ragione, ulteriori tentativi di installazione non verranno effettuati. Il software antivirus non verrà installato sulla postazione, e nel Pannello di controllo tale postazione verrà visualizzata come disconnessa.

In questo caso, è necessario [installare Agent Dr.Web](#) manualmente. Dopo l'installazione del nuovo Agent Dr.Web sarà necessario unire la vecchia postazione e quella nuova nel Pannello di controllo nella lista gerarchica della rete antivirus.

## Se l'aggiornamento non è supportato

Se gli Agent Dr.Web sono installati su postazioni con sistemi operativi non supportati per l'installazione di Agent Dr.Web per Dr.Web Enterprise Security Suite versione 13.0, non verrà eseguita nessuna azione di aggiornamento.

Gli Agent Dr.Web installati su sistemi operativi non supportati non potranno ricevere aggiornamenti (compresi aggiornamenti dei database dei virus) dal nuovo Server Dr.Web. Se è richiesta la presenza di Agent Dr.Web sotto sistemi operativi non supportati, è necessario lasciare nella rete antivirus i Server Dr.Web di versioni precedenti a cui sono connessi questi



Agent Dr.Web. In tale caso, i Server Dr.Web versioni 6 e i Server Dr.Web versione 13.0 devono ricevere aggiornamenti in modo indipendente.



Le raccomandazioni per l'aggiornamento di Agent Dr.Web installati su postazioni che svolgono funzionalità LAN critiche sono riportate in documento **Allegati**, sezione [Aggiornamento degli Agent sui server LAN](#).

## 7.3.2. Aggiornamento di Agent Dr.Web per le postazioni SO Android



Dr.Web Enterprise Security Suite 13.0 supporta l'uso di Agent Dr.Web per Android a partire dalla versione 12.2.

### Agent Dr.Web per Android su dispositivi mobili può essere aggiornato

1. Automaticamente. A partire dalla versione 12.6.4 Agent Dr.Web per Android si aggiorna in autonomo quando da Server Dr.Web arrivano informazioni sulla disponibilità di una nuova versione. Per l'aggiornamento automatico assicurarsi che nelle impostazioni del repository di Server Dr.Web nel Pannello di controllo sia impostato l'aggiornamento del prodotto Dr.Web per Android (**Amministrazione** → **Configurazione generale del repository** → **Pacchetti di installazione Dr.Web** → **Prodotti aziendali Dr.Web**), e nelle impostazioni di Dr.Web per Android nel Pannello di controllo sia spuntato il flag corrispondente (**Rete antivirus** → gruppo di postazioni o singola postazione con SO Android → **Dr.Web per Android** → **Aggiornamenti** → **Verifica la disponibilità di una nuova versione**).
2. Manualmente, installando sul dispositivo mobile il pacchetto di installazione della nuova versione. Per fare ciò, assicurarsi che nelle impostazioni del repository di Server Dr.Web nel Pannello di controllo sia impostato l'aggiornamento del prodotto Dr.Web per Android (**Amministrazione** → **Configurazione generale del repository** → **Pacchetti di installazione Dr.Web** → **Prodotti aziendali Dr.Web**), dopodiché scaricare il pacchetto generato nel Pannello di controllo nelle proprietà della postazione o sulla pagina **Amministrazione** → **Prodotti aziendali**.



A partire dalla versione 12, Server Dr.Web ha la possibilità di aggiornare l'applicazione Dr.Web Security Space per Android a condizione che tale versione dell'applicazione sia stata installata da Server Dr.Web.



### 7.3.3. Aggiornamento di Agent Dr.Web per le postazioni SO Linux e macOS

Gli Agent Dr.Web installati su postazioni con sistemi operativi della famiglia Linux e macOS si conetteranno al Server Dr.Web versione 13.0 se sono soddisfatte le seguenti condizioni:

1. Gli Agent Dr.Web devono essere installati su computer con i sistemi operativi supportati per l'installazione di Agent Dr.Web per Dr.Web Enterprise Security Suite versione 13.0 (v. [Requisiti di sistema](#)).
2. Sulle postazioni devono essere impostate le chiavi di cifratura e le impostazioni di rete del Server Dr.Web aggiornato.

#### Dopo la connessione delle postazioni al Server Dr.Web aggiornato:

1. Sulle postazioni vengono aggiornati solo i database dei virus. L'aggiornamento automatico del software antivirus stesso non viene eseguito.
2. Se sulle postazioni è installata l'ultima versione del software, nessuna ulteriore azione è necessaria.
3. Se il software sulle postazioni non è aggiornato, scaricare il pacchetto di installazione della nuova versione di Agent Dr.Web nel Pannello di controllo nelle proprietà della postazione o sulla [pagina di installazione](#). Aggiornare il software delle postazioni manualmente, come descritto nei relativi **Manuali utente**.

## 7.4. Aggiornamento del Server proxy Dr.Web

### 7.4.1. Aggiornamento del Server proxy Dr.Web durante il funzionamento

L'aggiornamento del Server proxy può essere eseguito automaticamente durante il funzionamento.



Se il Server Dr.Web sotto SO della famiglia UNIX è stato precedentemente aggiornato dalla versione 11.0 o 11.0.1, l'aggiornamento automatico del Server proxy Dr.Web sarà impossibile. Per togliere questa restrizione, è necessario nella sezione **Amministrazione** → **Configurazione dettagliata del repository** → **Server proxy Dr.Web** → **Sincronizzazione** nel campo **Aggiorna soltanto i seguenti file** rimuovere manualmente il suffisso `^win.*`.

Nel caso di installazione iniziale del Server Dr.Web versione 11.0.2 le restrizioni sull'aggiornamento automatico del Server proxy non vengono imposte.



### Il calendario di aggiornamento dipende dalle impostazioni di memorizzazione in cache proattiva del Server proxy:

1. Se il Server proxy non è incluso nella lista per la memorizzazione in cache proattiva (anche nel caso in cui la memorizzazione nella cache non viene utilizzata), gli aggiornamenti del Server proxy verranno scaricati e installati secondo il calendario di aggiornamento automatico.
2. Se il Server proxy è incluso nella lista per la memorizzazione in cache proattiva, gli aggiornamenti del Server proxy verranno scaricati secondo il calendario di memorizzazione in cache proattiva. Nel caso di ricezione di una nuova revisione del Server proxy, l'aggiornamento a questa revisione avverrà secondo il calendario di aggiornamento automatico.

### L'aggiornamento automatico può essere configurato in uno dei seguenti modi:

- Attraverso le impostazioni di Server proxy nel Pannello di controllo del Server Dr.Web di gestione nella sezione **Aggiornamenti**. La descrizione dettagliata è riportata nel documento **Manuale dell'amministratore**, sezione [Configurazione del Server proxy in remoto](#).
- Attraverso il file di configurazione di Server proxy `drwcsd-proxy.conf`. La descrizione dettagliata è riportata in documento **Allegati**, [F4. File di configurazione di Server proxy Dr.Web](#).

## 7.4.2. Aggiornamento del Server proxy Dr.Web attraverso l'installer

### I file di configurazione del Server proxy

I file di configurazione del Server proxy versione 11 e successive:

File	Descrizione
<code>drwcsd-proxy.conf</code>	file di configurazione di Server proxy (v. documento <b>Allegati</b> , p. <a href="#">Aggiornamento di Agent Dr.Web per le postazioni SO Linux e macOS</a> )
<code>drwcsd-proxy.auth</code>	dati di identificazione (l'ID e la password) per l'accesso ai Server Dr.Web
<code>drwcsd-proxy-trusted.list</code>	lista dei certificati affidabili dei Server Dr.Web
<code>drwcsd-proxy-signed.list</code>	lista dei certificati firmati del Server proxy
<code>drwcsd-proxy.pri</code>	chiave di cifratura privata del Server proxy



## Aggiornamento del Server proxy sotto il sistema operativo Windows

L'aggiornamento viene effettuato automaticamente per mezzo dell'installer.

### Per aggiornare il Server proxy versione 11 e successive

1. Avviare il file del pacchetto del Server proxy.
2. Si apre una finestra che avvisa del software Server proxy versione precedente installato e offre di aggiornarlo alla versione nuova. Per iniziare a configurare la procedura di aggiornamento, premere il pulsante **Upgrade**.
3. Si apre una finestra con informazioni sulla rimozione del Server proxy versione precedente. Per iniziare il processo di rimozione, premere **Uninstall**.
4. Una volta completata la rimozione della versione precedente del Server proxy, inizierà l'installazione della versione nuova. Si apre una finestra con informazioni sul prodotto. Premere il pulsante **Next**.
5. Nei passaggi successivi il Server proxy viene configurato in modo simile al processo di [Installazione di Server proxy Dr.Web](#) in base ai [file di configurazione](#) dalla versione precedente. L'installer determina automaticamente la directory di installazione di Server proxy e la posizione dei file di configurazione dall'installazione precedente. Se necessario, è possibile modificare le impostazioni prese dai file, che sono state trovate automaticamente dall'installer.
6. Per iniziare il processo di installazione del Server proxy, premere il pulsante **Install**.

## Aggiornamento del Server proxy sotto i sistemi operativi della famiglia UNIX

### Per aggiornare il Server proxy versione 11.0 o precedenti



Quando viene aggiornato il Server proxy, vengono rimossi i [file di configurazione](#). Se necessario, salvare i file di configurazione manualmente prima di iniziare l'aggiornamento.

1. Per avviare il processo di aggiornamento, eseguire il file del pacchetto del Server proxy:  
`./<file_del_pacchetto>.tar.gz.run`
2. Dopo il completamento dell'aggiornamento, se necessario, portare manualmente nei nuovi file di configurazione le impostazioni dai [file di configurazione](#) salvati prima dell'inizio dell'aggiornamento.



### Per aggiornare il Server proxy versione 11.0.1

1. Per avviare il processo di aggiornamento, eseguire il file del pacchetto del Server proxy:  
`./<file_del_pacchetto>.tar.gz.run`
2. Durante la rimozione della versione precedente verranno automaticamente salvati i [file di configurazione](#) del Server proxy.
3. Durante il processo di aggiornamento verrà offerto di utilizzare i file di configurazione da un'installazione precedente del Server proxy salvati tramite il backup:
  - Per utilizzare una copia di backup memorizzata di default nella directory `/var/tmp/drwcsd-proxy`, premere INVIO.
  - Per utilizzare una copia di backup da un'altra directory, inserire manualmente il percorso della copia di backup.
  - È inoltre possibile installare il Server proxy con le impostazioni predefinite, senza utilizzare una copia di backup della configurazione da un'installazione precedente. Per fare ciò, premere 0.



## Indice analitico

### A

- account
  - postazione 72
  - Server proxy 102
- Active Directory
  - informazioni generali 53
  - installazione di Agent 94
  - rimozione di Agent 119
- Agent
  - aggiornamento 132
  - installazione 65, 77
  - installazione locale 70
  - installazione, Active Directory 94
  - installazione, remota 81
  - installazione, su remoto 82, 94
  - rimozione, Active Directory 119
  - rimozione, in caso di SO Windows 115
- aggiornamento
  - Agent 132
  - Server, per SO UNIX 128
  - Server, per SO Windows 124

### C

- certificato 49
- chiave privata 49
- chiave pubblica 49
- chiavi
  - demo 34
  - di cifratura 49
  - di licenza 33
- chiavi demo 34
- chiavi di licenza
  - ottenimento 33
- cifratura
  - informazioni generali 42
- codici di errore
  - installazione 112
- compressione del traffico 42
- concessione delle licenze 33
- creazione
  - account, postazione 72
  - account, Server proxy 102

### I

- icone

- scanner di rete 83
- installazione 65
  - Agent 65
  - codici di errore 112
  - NAP Validator 101
  - pacchetto antivirus 65
  - Server proxy 101
  - Server, per SO UNIX 63
  - Server, per SO Windows 57
- installazione di Agent 65
  - Active Directory 94
  - installer 77
  - localmente 70
  - pacchetto di installazione di gruppo 76
  - pacchetto di installazione individuale 72
  - remota 81
  - su remoto 82, 94
- installer
  - contenuti 67
  - installazione 77
  - rimozione 118
  - tipi 67

### N

- NAP Validator
  - installazione 101

### P

- pacchetto 31
- pacchetto antivirus
  - installazione 65
  - rimozione 115
- pacchetto di installazione
  - contenuti 67
  - di gruppo 67, 76
  - individuale 67, 72
  - tipi, confronto 70
- pacchetto di installazione di gruppo
  - informazioni generali 67
  - installazione 76
- pacchetto di installazione individuale
  - informazioni generali 67
  - installazione 72
- pagina di installazione 67
- postazione
  - account, creazione 72



## Indice analitico

protocollo SRV 42

### R

registrazione

prodotto Dr.Web 33

rete antivirus

creazione 35

rimozione

Agent 115

componenti 115

pacchetto antivirus 115

Server proxy 120

Server, per SO UNIX 114

Server, per SO Windows 114

rimozione di Agent

Active Directory 119

in caso di SO Windows 115

installer 118

### S

scanner di rete 82

Server Dr.Web

aggiornamento, per SO UNIX 128

aggiornamento, per SO Windows 124

installazione, per SO UNIX 63

installazione, per SO Windows 57

rimozione, in caso di SO UNIX 114

rimozione, in caso di SO Windows 114

Server proxy

account 102

connessione al Server Dr.Web 109

installazione 101

rimozione 120

servizio di rilevamento Server 41

### T

traffico

cifratura 42

compressione 42

