



Dr.WEB

Enterprise Security Suite

Guida all'installazione

Жасағаныңды

دافع عن إبداعاتك

Защити созданное

Defend what you create

Protégez votre univers

Verteidige, was du erschaffen hast

Захисти створене

保护您创建的一切

Защити созданное

Proteggi ciò che crei

Жасағаныңды қорға

Защити созданное

Proteggi ciò che crei

Verteidige, was du erschaffen hast

Захисти створене

Defend what you create

脅威からの保護を提供します

Protégez votre univers

Proteggi ciò che crei

Захисти створене

دافع عن إبداعاتك

脅威からの保護を提供します

Defend what you create

Жасағаныңды қорға

دافع عن إبداعاتك

دافع عن إبداعاتك

Protégez votre univers

保护您创建的一切

Защити созданное

脅威からの保護を提供します

Захисти створене

Verteidige, was du erschaffen hast

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

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

Marchi

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

Disclaimer

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

Dr.Web Enterprise Security Suite

Versione 10.01.0

Guida all'installazione

11/09/2017

Doctor Web, Sede centrale in Russia

125040

Russia, Mosca

3° via Yamskogo polya, 2, 12A

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

Telefono +7 (495) 789-45-87

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

Doctor Web

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

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

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

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

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



Sommario

Capitolo 1: Dr.Web Enterprise Security Suite	6
1.1. Introduzione	6
1.1.1. Scopo del documento	6
1.1.2. Segni convenzionali e abbreviazioni	7
1.2. Sul prodotto	9
1.3. Requisiti di sistema	18
1.4. Contenuto del pacchetto	23
Capitolo 2: Concessione delle licenze	26
Capitolo 3: Introduzione all'uso	28
3.1. Creazione della rete antivirus	28
3.2. Configurazione delle connessioni di rete	31
3.2.1. Connessioni dirette	32
3.2.2. Servizio di rilevamento di Server Dr.Web	33
3.2.3. Utilizzo del protocollo SRV	34
Capitolo 4: Installazione dei componenti di Dr.Web Enterprise Security Suite	35
4.1. Installazione di Server Dr.Web	35
4.1.1. Installazione di Server Dr.Web per SO Windows®	36
4.1.2. Installazione di Server Dr.Web per SO della famiglia UNIX®	42
4.1.3. Installazione del pacchetto supplementare di Server Dr.Web	43
4.1.4. Installazione dell'estensione del Pannello di controllo della sicurezza Dr.Web	44
4.2. Installazione di Agent Dr.Web	46
4.2.1. File di installazione	48
4.2.2. Installazione locale di Agent Dr.Web	49
4.2.3. Rimozione di Agent Dr.Web per SO Windows®	59
4.3. Installazione di NAP Validator	72
4.4. Installazione del Server proxy	73
Capitolo 5: Rimozione dei componenti di Dr.Web Enterprise Security Suite	77
5.1. Rimozione di Server Dr.Web	77
5.1.1. Rimozione di Server Dr.Web per SO Windows®	77
5.1.2. Rimozione di Server Dr.Web per SO della famiglia UNIX®	77
5.2. Rimozione di Agent Dr.Web	79



5.2.1. Rimozione di Agent Dr.Web per SO Windows®	80
5.2.2. Rimozione di Agent Dr.Web con utilizzo del servizio Active Directory	82
5.3. Eliminazione del Server proxy	83
Capitolo 6: Aggiornamento dei componenti di Dr.Web Enterprise Security Suite	84
6.1. Aggiornamento di Server Dr.Web per SO Windows®	84
6.2. Aggiornamento di Server Dr.Web per SO della famiglia UNIX®	88
6.3. Aggiornamento dell'estensione del Pannello di controllo della sicurezza Dr.Web	94
6.4. Aggiornamento di Agent Dr.Web	94
6.4.1. Aggiornamento di Agent Dr.Web per le postazioni SO Windows®	94
6.4.2. Aggiornamento degli Agent Dr.Web per le postazioni SO Linux, Android e OS X	96
6.5. Aggiornamento del Server proxy	97
Indice analitico	98



Capitolo 1: Dr.Web Enterprise Security Suite

1.1. Introduzione

1.1.1. Scopo del documento

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

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

1. **Guida all'installazione** (file **drweb-esuite-10-install-manual-it.pdf**)

La guida all'installazione sarà utile per il responsabile della società che prende la decisione di acquistare e di installare il 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** (file **drweb-esuite-10-admin-manual-it.pdf**)

3. **Allegati** (file **drweb-esuite-10-appendices-it.pdf**)



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

Nella documentazione dell'amministratore non vengono descritti i pacchetti antivirus Dr.Web per computer protetti. Le informazioni pertinenti sono consultabili nel **Manuale dell'utente** della soluzione antivirus Dr.Web per il sistema operativo corrispondente.

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





1.1.2. Segni convenzionali e abbreviazioni

Segni convenzionali

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

Tabella 1-1. Segni convenzionali

Segno	Commento
	Nota importante o istruzione.
	Avviso di possibili situazioni di errore, nonché di punti importanti cui prestare particolare attenzione.
<i>Rete antivirus</i>	Un nuovo termine o un termine accentato nelle descrizioni.
<indirizzo_IP>	Campi in cui nomi di funzione vanno sostituiti con valori effettivi.
Salva	Nomi dei pulsanti di schermo, delle finestre, delle voci di menu e di altri elementi dell'interfaccia del programma.
CTRL	Nomi dei tasti della tastiera.
C:\Windows\	Nomi di file e directory, frammenti di codice.
<u>Allegato A</u>	Riferimenti incrociati ai capitoli del documento o collegamenti ipertestuali a risorse esterne.

Abbreviazioni

Nel testo del Manuale vengono utilizzate le seguenti abbreviazioni senza spiegazione:

- ACL – lista di controllo degli accessi (Access Control List),
- CDN – rete di distribuzione di contenuti (Content Delivery Network),
- CPU – processore centrale (Central Processing Unit),
- DFS – file system distribuito (Distributed File System),
- DNS – sistema dei nomi a dominio (Domain Name System),
- GUI – interfaccia utente grafica (Graphical User Interface), versione del programma con la GUI – una versione che utilizza gli strumenti della GUI,
- NAP – Network Access Protection,
- MTU – dimensione massima di un pacchetto dati (Maximum Transmission Unit),
- TTL – tempo di vita pacchetto (Time To Live),



- UDS – socket di dominio UNIX (UNIX Domain Socket),
- DB, DBMS – database, database management system,
- SAM Dr.Web – Sistema di aggiornamento mondiale di Dr.Web,
- LAN – rete locale,
- SO – sistema operativo,
- Software – programmi per computer.



Server di protezione centralizzata

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

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

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

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

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

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

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

Database unico

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

È possibile utilizzare i seguenti tipi di database:

Database incorporato. Vengono fornite due varianti del database incorporato direttamente nel Server di protezione centralizzata:

- SQLite2 (InitDB),
- SQLite3.

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

- Oracle,
- PostgreSQL,
- Driver ODBC per la connessione di altri database quali Microsoft SQL Server/Microsoft SQL Server Express.

È possibile utilizzare qualsiasi database che corrisponda alle esigenze dell'azienda. La scelta deve essere basata sulle esigenze che devono essere soddisfatti dal data warehouse, come per esempio: la possibilità di essere utilizzato in una rete antivirus di dimensioni adeguate, le caratteristiche di manutenzione del software del database, le possibilità 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 viene installato automaticamente insieme al Server e fornisce un'interfaccia web utilizzata per gestire su remoto il Server e la rete antivirus modificando le impostazioni del Server, nonché le impostazioni dei computer protetti, conservate sul Server e sui computer protetti.

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

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

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

Il Pannello di controllo di protezione centralizzata fornisce le seguenti possibilità:

- Facilità di installazione di Antivirus su postazioni protette, in particolare è possibile: installare su remoto sulle postazioni SO Windows con un esame preliminare della rete per cercare computer; creare pacchetti con identificatori univoci e con i parametri di connessione al Server per semplificare il processo di installazione di Antivirus da parte dell'amministratore o per consentire agli utenti di installare Antivirus su postazioni in modo autonomo (per maggiori informazioni consultare la sezione [Installazione di Agent Dr.Web](#)).
- Gestione semplificata delle postazioni della rete antivirus tramite il metodo di gruppi.
- Possibilità di gestire 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 di 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 su remoto sia secondo un calendario prestabilito che su una diretta richiesta dell'amministratore dal Pannello di controllo; configurare in modo centralizzato le impostazioni di scansione antivirus che vengono trasmesse su postazioni per eseguire in seguito una scansione locale con queste impostazioni.
- Ottenimento delle informazioni statistiche sullo stato delle postazioni protette, delle statistiche di virus, delle informazioni sullo stato del software antivirus installato, sullo stato dei componenti antivirus in esecuzione, nonché dell'elenco degli hardware e dei software della postazione protetta.
- Flessibile sistema di amministrazione del Server 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, per esempio Active Directory, LDAP, RADIUS, PAM.
- Gestione delle licenze di protezione antivirus di postazioni con un complesso sistema di assegnazione delle licenze a postazioni e gruppi di postazioni, nonché trasferimento del-



le licenze tra diversi Server in caso di una configurazione della rete antivirus con diversi server.

- Una vasta gamma di impostazioni per configurare il Server e i suoi componenti separati, in particolare, è possibile: impostare un calendario di manutenzione del Server; connettere procedure personalizzate; configurare in modo flessibile l'aggiornamento di tutti i componenti della rete antivirus da SAM e la successiva distribuzione degli aggiornamenti sulle postazioni; configurare i sistemi che avvisano l'amministratore degli eventi accaduti nella rete antivirus tramite diversi metodi di consegna di messaggi; configurare le relazioni tra i server in caso di una 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 Dr.Web il Web server che viene installato automaticamente insieme al Server. L'obiettivo principale del Web server è assicurare il lavoro con le pagine del Pannello di controllo e con le connessioni di rete client.

Pannello di controllo mobile di protezione centralizzata

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

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

1. 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.
2. Gestione delle postazioni su cui un aggiornamento del software antivirus non è riuscito:
 - visualizzazione delle postazioni fallite;
 - aggiornamento dei componenti sulle postazioni fallite.
3. 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.
4. Gestione delle nuove postazioni in attesa di essere collegate al Server Dr.Web:
 - conferma dell'accesso;
 - rigetto delle postazioni.
5. 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 da Quarantena sulla postazione selezionata o su tutte le postazioni di un gruppo.
6. Gestione delle postazioni e dei gruppi:
 - visualizzazione delle impostazioni;
 - visualizzazione e gestione della lista dei componenti del pacchetto antivirus;
 - rimozione;
 - invio dei messaggi con qualsiasi contenuto sulle postazioni;
 - riavvio delle postazioni SO Windows;
 - aggiunta alla lista dei preferiti per un rapido accesso.
 7. Ricerca delle postazioni e dei gruppi nella rete antivirus secondo vari parametri: nome, indirizzo, ID.
 8. 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 dell'eliminazione automatica delle notifiche.

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

Protezione delle postazioni della rete

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

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

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

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

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



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

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 scansione alla ricerca dei 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 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.

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, proteggendoli contro le modifiche accidentali o contro l'infezione dai 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 di applicazioni.

Quarantena

Isolamento di oggetti dannosi e sospetti in una directory speciale.

Auto-protezione

Protezione dei file e delle directory Dr.Web Enterprise Security Suite contro la rimozione o la modifica non autorizzata o accidentale da parte dell'utente e contro la rimozione o la



modifica da parte del malware. Quando l'auto-protezione è attivata, l'accesso ai file e alle directory Dr.Web Enterprise Security Suite è consentito solamente 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.

Postazioni SO famiglia UNIX®

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 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.

Postazioni OS X®

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 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.

Filtraggio di chiamate e di messaggi

Il filtraggio di messaggi SMS e di chiamate consente di bloccare messaggi e chiamate indesiderati, per esempio messaggi di pubblicità, nonché chiamate e 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 di 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.

Server SO Novell® NetWare®

Scansione antivirus

Scansione del computer on demand e secondo il calendario.



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.

Assicurazione della comunicazione tra i componenti della rete anti-virus

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

Server proxy Dr.Web

Il Server proxy può essere incluso opzionalmente nella struttura di rete antivirus. L'obiettivo principale del Server proxy è assicurare la comunicazione del Server e delle postazioni protette nel caso non sia possibile organizzare l'accesso diretto, per esempio se il Server e le postazioni protette si trovano nelle reti diverse tra cui non c'è l'instradamento dei pacchetti. Tramite la funzione di memorizzazione in cache è anche possibile ridurre il traffico di rete e il tempo di ottenimento degli aggiornamenti da parte delle postazioni protette.

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.

Cifatura del traffico

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

Possibilità aggiuntive

NAP Validator

NAP Validator viene fornito come un componente aggiuntivo e permette di utilizzare la tecnologia Microsoft Network Access Protection (NAP) per controllare l'operatività del software delle postazioni protette. 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, fornito come utility aggiuntiva, permette di scaricare i prodotti Dr.Web Enterprise Security Suite dal Sistema di aggiornamento mondiale. Si può utilizzarlo per scaricare aggiornamenti dei prodotti Dr.Web Enterprise Security Suite per mettere gli aggiornamenti su un Server non connesso a Internet.

1.3. Requisiti di sistema

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

- che il Server Dr.Web sia installato su un computer connesso a Internet per la ricezione automatica degli aggiornamenti dai server SAM (Sistema di aggiornamento mondiale) Dr.Web;



È ammissibile la possibilità di distribuire gli aggiornamenti in un altro modo sui Server non connessi a Internet. In particolare, in una rete antivirus con diversi server è possibile che soltanto un Server riceva gli aggiornamenti dal SAM per la successiva distribuzione degli stessi sugli altri Server, oppure si può usare l'utility supplementare Loader di repository Dr.Web che scarica gli aggiornamenti dal SAM attraverso Internet e in seguito gli aggiornamenti vengono distribuiti sui Server.


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

Numeri di porte	Protocolli	Direzione delle connessioni	Scopo
2193	TCP	<ul style="list-style-type: none">• in ingresso, in uscita per il Server e il Server proxy• in uscita per Agent	Per la comunicazione dei componenti antivirus con il Server e per le connessioni tra i server.
	UDP	in ingresso, in uscita	Tra gli altri scopi, viene utilizzata dal Server proxy per stabilire una connessione con i client. Per il funzionamento dello Scanner di rete.
139, 445	TCP	<ul style="list-style-type: none">• in ingresso per il Server• in ingresso, in uscita per l'Agent• in uscita per il computer su cui viene aperto il Pannello di controllo	Per il funzionamento dell'Installer di rete.
	UDP	in ingresso, in uscita	
9080	HTTP	<ul style="list-style-type: none">• in ingresso per il Server• in uscita per il computer su cui viene aperto il Pannello di controllo	Per il funzionamento del Pannello di controllo della sicurezza Dr.Web.
9081	HTTPS		
10101	TCP		Per il funzionamento dell'utility di diagnostica remota del Server.
80	HTTP	in uscita	Per ricevere aggiornamenti da SAM.
443	HTTPS		



Notare: nelle versioni Server 4 veniva utilizzata la porta 2371 per la connessione dei componenti antivirus con il Server. Nella versione 10 questa porta non è più supportata.

Per il funzionamento del Server Dr.Web occorre:

Componente	Requisiti
Processore e sistema operativo	<p>Sono supportati i seguenti sistemi operativi installati sui computer con le CPU corrispondenti:</p> <ul style="list-style-type: none">• CPU con il supporto del set di istruzioni SSE2 e con la frequenza di clock di 1,3 GHz e superiori:<ul style="list-style-type: none">▫ SO Windows;▫ SO Linux;▫ SO FreeBSD;▫ SO Solaris x86.• CPU V9 UltraSPARC III e superiori:<ul style="list-style-type: none">▫ SO Solaris Sparc. <p>La lista completa degli SO supportati è riportata nel documento Allegati, in Allegato A.</p>
Memoria operativa	<ul style="list-style-type: none">• Requisiti minimi: 1 GB.• Requisiti consigliati: 2 GB e superiori.
Spazio su disco rigido	<p>almeno 12 GB: fino ai 8 GB per il database incorporato (directory di installazione), fino ai 4 GB nella directory temporanea di sistema (per i file operativi).</p> <p>A seconda delle impostazioni del Server, potrebbe essere necessario spazio aggiuntivo per la conservazione di file temporanei, per esempio di pacchetti di installazione di Agent personali (circa 8,5 MB ognuno) nella sottodirectory <code>var\installers-cache</code> della directory di installazione di Server Dr.Web.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> Per l'installazione del Server è necessario che sul disco di sistema in caso di SO Windows o in <code>/var/tmp</code> in caso di SO della famiglia UNIX (oppure in un'altra directory di file temporanei se è stata ridefinita), a prescindere dal luogo di installazione del Server stesso, ci siano almeno 1,2 GB per il pacchetto principale e 2,5 GB di memoria libera per il pacchetto supplementare per l'avvio dell'installer e per l'estrazione di file temporanei.</div>
Altro	<p>Per l'installazione di Server Dr.Web sotto SO della famiglia UNIX è necessaria la disponibilità delle librerie: <code>lsb</code> versione 3 e superiori, <code>glibc</code> versione 2.7 e superiori.</p> <p>Per l'utilizzo del DB PostgreSQL è necessaria la disponibilità della libreria <code>libpq</code>.</p> <p>Per l'utilizzo del DB Oracle è necessaria la disponibilità della libreria <code>libaio</code>.</p> <p>In aggiunta sotto SO FreeBSD è necessaria la disponibilità della libreria <code>compat-8x</code>.</p>

**Per il funzionamento del Server proxy Dr.Web occorre:**

Componente	Requisito
Processore	Intel® Pentium® III frequenza di 667 MHz e superiori.
Memoria operativa	almeno 1 GB.
Spazio su disco rigido	almeno 1 GB.
Sistema operativo	<ul style="list-style-type: none">• Windows;• Linux;• FreeBSD;• Solaris. <p>La lista completa degli SO supportati è riportata nel documento Allegati, in Allegato A.</p>
Altro	<p>Per l'installazione del Server proxy sotto SO della famiglia UNIX è necessaria la disponibilità delle librerie: <code>libc</code> versione 3 e superiori.</p> <p>In aggiunta sotto SO FreeBSD è necessaria la disponibilità della libreria <code>compat-8x</code>.</p>

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

a) Browser web:

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

Se si usa il web browser Windows Internet Explorer, si deve tener conto delle seguenti particolarità:

- Non è garantita la completa operatività del Pannello di controllo sotto il web browser Windows Internet Explorer con la modalità attivata **Enhanced Security Configuration for Windows Internet Explorer**.



- Se il Server viene installato su un computer il cui nome include il carattere "_" (trattino basso), non sarà possibile gestire il Server attraverso il Pannello di controllo nel browser. In questo caso deve essere utilizzato un altro web browser.
 - Per il corretto funzionamento del Pannello di controllo, l'indirizzo IP e/o il nome DNS del computer su cui è installato il Server Dr.Web devono essere aggiunti ai siti attendibili del web browser in cui viene aperto il Pannello di controllo.
 - Per aprire il Pannello di controllo in modo corretto tramite il menu **Start** in SO Windows 8 e Windows Server 2012 con l'interfaccia delle piastrelle dinamiche, 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**.
- b) Per utilizzare le piene funzionalità del Pannello di controllo, è necessario installare l'estensione del Pannello di controllo della sicurezza Dr.Web. L'estensione viene fornita insieme al pacchetto Server e viene installata a richiesta del browser nel processo di utilizzo degli elementi del Pannello di controllo che necessitano del caricamento dell'estensione (per Scanner di rete, per l'installazione remota di componenti antivirus).

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

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



Per il funzionamento dell'Estensione del Pannello di controllo della sicurezza Dr.Web sulla pagina dello Scanner di rete in SO Windows, così come in SO della famiglia GNU/Linux, sono necessari i permessi di amministratore (root).

In caso di utilizzo dei browser Mozilla Firefox e Google Chrome, l'estensione del Pannello di controllo della sicurezza Dr.Web è disponibile soltanto per le versioni sotto SO Windows e SO della famiglia Linux.

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

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

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

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

Per il funzionamento di NAP occorre:**Per il server:**

- SO Windows Server 2008.

Per gli agent:

- SO Windows XP SP3, SO Windows Vista, SO Windows Server 2008.

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

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

- SO Windows:

Componente	Requisito
Processore	CPU con la frequenza di clock di 1 GHz e superiori.
Memoria operativa libera	Almeno 512 MB.
Spazio libero su disco rigido	Almeno 1 GB per i file eseguibili + spazio aggiuntivo per i log di funzionamento e per i file temporanei.
Altro	<ol style="list-style-type: none">1. Per il corretto funzionamento della guida sensibile al contesto di Agent Dr.Web per Windows è necessaria la disponibilità di Windows® Internet Explorer® 6.0 e superiori.2. Per il plugin Dr.Web per Microsoft Outlook deve essere installato il client Microsoft Outlook di Microsoft Office:<ul style="list-style-type: none">• Outlook 2000;• Outlook 2002;



Componente	Requisito
	<ul style="list-style-type: none">• Outlook 2003;• Outlook 2007;• Outlook 2010 SP2;• Outlook 2013;• Outlook 2016.

- SO della famiglia Linux:

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

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



Sulle postazioni della rete antivirus gestita tramite Dr.Web non deve essere utilizzato altro software antivirus (neanche altre versioni dei programmi antivirus Dr.Web).



La descrizione delle funzionalità di Agent è riportata nei manuali utente per il sistema operativo corrispondente.

1.4. Contenuto del pacchetto

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

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

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



Nome del file	Componente
drweb-esuite-proxy-10.01.0-<build>-<versione_SO>.run	Server proxy

2. In caso di Windows – come file eseguibili:

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

Il pacchetto di Server Dr.Web è composto da due pacchetti:

1. *Pacchetto principale* – il pacchetto base per l'installazione di Server Dr.Web. Il pacchetto include le parti analoghe a quelle incluse nel pacchetto delle versioni precedenti di Dr.Web Enterprise Security Suite.

Il pacchetto principale permette di installare il Server Dr.Web stesso che include i pacchetti di protezione antivirus soltanto per le postazioni Windows.

2. *Pacchetto supplementare (extra)* – include i pacchetti di tutti i prodotti per l'impresa forniti per l'installazione sulle postazioni protette gestite da tutti gli SO supportati.

Viene installato come un supplemento su un computer su cui è già installato il pacchetto principale di Server Dr.Web.



Il pacchetto supplementare deve essere dello stesso tipo del pacchetto principale.

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

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

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



Capitolo 2: Concessione delle licenze

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

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



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

File della chiave di licenza

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



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

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

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

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

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



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

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



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

L'utilizzo dei file della chiave di licenza nel processo di installazione del programma è descritto in 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 3: Introduzione all'uso

3.1. Creazione della rete antivirus

Brevi istruzioni per l'installazione di una rete antivirus:

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

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



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

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

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

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

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



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

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

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

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

4. Se la rete antivirus includerà le postazioni protette SO Android, SO Linux, OS X, installare il pacchetto supplementare di Server Dr.Web su tutti i computer su cui è installato il pacchetto principale di Server.



5. Se necessario, installare e configurare il Server proxy. La descrizione viene riportata in p. [Installazione del Server proxy](#).
6. Per configurare il Server e il software antivirus su postazioni, è necessario connettersi al Server attraverso il Pannello di controllo della sicurezza Dr.Web.



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

Il Pannello di controllo è disponibile sull'indirizzo:

`http://<Indirizzo_Server>:9080`

o

`https://<Indirizzo_Server>:9081`

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

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

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

La password:

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



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

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

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



Manuale dell'amministratore, p. [Aggiornamento di Server Dr.Web e ripristino da copia di backup](#).

- d. Se necessario, configurare [Connessioni di rete](#) per modificare le impostazioni di rete di default utilizzate per l'interazione di tutti i componenti della rete antivirus.
 - e. Se necessario, configurare la lista degli amministratori di Server. Inoltre, è disponibile l'autenticazione di amministratori esterna. Per maggiori informazioni v. **Manuale dell'amministratore**, [Capitolo 5: Amministratori della rete antivirus](#).
 - f. Prima di iniziare ad utilizzare il software antivirus, è consigliabile modificare l'impostazione della directory per il backup dei dati critici del Server (v. **Manuale dell'amministratore**, p. [Configurazione del calendario di Server Dr.Web](#)). È preferibile collocare questa directory su un altro disco locale per ridurre la probabilità di una perdita simultanea dei file del software Server e della copia di backup.
8. Configurare il software antivirus per le postazioni (la configurazione dei gruppi e delle postazioni viene descritta dettagliatamente in **Manuale dell'amministratore**, in [Capitolo 6](#) e [Capitolo 7](#)):
- a. Se necessario, creare gruppi di postazioni personalizzati.
 - b. Configurare il gruppo **Everyone** e i gruppi personalizzati creati. In particolare, configurare la sezione dei componenti da installare.
9. Installare il software Agent Dr.Web sulle postazioni.

Nella sezione [File di installazione](#) controllare l'elenco dei file disponibili per l'installazione di Agent. Selezionare la variante di installazione adatta, basandosi sul sistema operativo della postazione, sulla possibilità di installazione su remoto, sulla variante di configurazione delle impostazioni di Server nel corso dell'installazione di Agent ecc. Per esempio:

- Se gli utenti installano l'antivirus in autonomo, utilizzare pacchetti di installazione personali che vengono creati attraverso il Pannello di controllo separatamente per ciascuna postazione. Questo tipo di pacchetti può inoltre essere inviato agli utenti via email direttamente dal Pannello di controllo. Dopo l'installazione le postazioni si connettono al Server in modo automatico.
- Per un'installazione remota attraverso la rete allo stesso tempo su una o più postazioni (soltanto per le postazioni SO Windows) utilizzare l'installer di rete. L'antivirus viene installato attraverso il Pannello di controllo con l'impiego di una determinata estensione del browser.
- Inoltre, è possibile installare l'antivirus in remoto attraverso la rete su una o più postazioni, utilizzando il servizio Active Directory. A tale scopo si usa l'installer di Agent Dr.Web per le reti con Active Directory che viene fornito insieme al pacchetto Dr.Web Enterprise Security Suite, ma separatamente dall'installer di Server.
- Se nel processo dell'installazione è necessario ridurre il carico sul canale di comunicazione tra Server e postazioni, è possibile utilizzare l'installer completo che installa contemporaneamente Agent e i componenti di protezione.
- L'installazione su postazioni Android, Linux, OS X può essere eseguita localmente secondo le regole generali. Inoltre, un prodotto standalone già installato può connettersi al Server sulla base della configurazione corrispondente.



10. Non appena installati sui computer, gli Agent si connettono automaticamente al Server. Le postazioni antivirus vengono autenticate sul Server a seconda dei criteri scelti (v. **Manuale dell'amministratore**, p. [Criteri di approvazione delle postazioni](#)):
- In caso di installazione dai pacchetti di installazione e inoltre in caso di configurazione di conferma automatica sul Server, le postazioni vengono registrate automaticamente al momento della prima connessione al Server e non è richiesta alcuna ulteriore conferma.
 - In caso di installazione dagli installer e di configurazione di conferma di accesso manuale, l'amministratore deve confermare manualmente le nuove postazioni in modo da registrarle sul Server. In questo caso, le nuove postazioni non vengono connesse automaticamente, ma vengono messe dal Server nel gruppo dei nuovi arrivi.
11. Dopo che la postazione si è connessa al Server e ha ottenuto le impostazioni, su di essa viene installato il relativo set di componenti del pacchetto antivirus, definito nelle impostazioni del gruppo primario della postazione.



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

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

3.2. Configurazione delle connessioni di rete

Informazioni generali

Al Server Dr.Web si connettono i seguenti client:

- Agent Dr.Web,
- Installer di Agent Dr.Web,
- altri Server Dr.Web.

Una connessione viene sempre stabilita da parte del client.

Sono disponibili i seguenti modi di connessione dei client al Server:

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 Server](#).

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

Questo approccio è da utilizzare 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.

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



Questo approccio permette di cercare il Server per nome del computer e/o del servizio Server 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 Server 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 l'installer aggiunge automaticamente le porte e le interfacce di Server 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.

3.2.1. Connessioni dirette

Configurazione del Server Dr.Web

Nelle impostazioni di Server deve essere indicato l'indirizzo (v. documento **Allegati**, p. [Allegato E. Specifica di indirizzo di rete](#)) su cui il Server deve essere "in ascolto" per la ricezione delle connessioni TCP in arrivo.

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

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

- **Indirizzo:** valore vuoto – utilizza *tutte le interfacce di rete* per questo computer su cui è installato Server.
- **Porta:** 2193 – utilizza la porta 2193 assegnata a Dr.Web Enterprise Security Suite in IANA.



Notare: nelle versioni Server 4 veniva utilizzata la porta 2371. Nella versione 10 questa porta non è più supportata.

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



Configurazione dell'Agent Dr.Web

Durante l'installazione dell'Agent, l'indirizzo del Server (indirizzo IP o nome DNS del computer su cui è avviato il Server Dr.Web) può essere esplicitamente indicato nei parametri di installazione:

```
drwinst <Indirizzo_Server>
```

Durante l'installazione dell'Agent, è consigliabile utilizzare il nome del Server registrato nel servizio DNS. Questo semplifica il processo di configurazione della rete antivirus nel caso si dovrà reinstallare il Server Dr.Web su un altro computer.

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

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

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

3.2.2. Servizio di rilevamento di Server Dr.Web

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

Per questo fine, il Server deve rimanere "in ascolto" di tali richieste sulla rete.

Sono possibili diverse varianti di configurazione di questo modo. L'importante è che il metodo di ricerca del Server, impostato per i client, corrisponda alle impostazioni della parte relativa del Server.

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

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

Di default per "l'ascolto" da parte del Server viene impostato (come per le connessioni dirette):
`udp/231.0.0.1:2193`.



Notare: nei Server versione 4 veniva utilizzata la porta 2371. Nella versione 10 questa porta non è più supportata.



Questo parametro viene configurato nelle impostazioni del Pannello di controllo **Amministrazione** → **Configurazione del Server Dr.Web** → scheda **Rete** → scheda **Trasporto** → campo **Gruppo multicast**.

3.2.3. Utilizzo del protocollo SRV

I client SO Windows supportano il protocollo di rete del client SRV (la descrizione del formato è riportata nel documento **Allegati**, p. [Allegato E. Specifica di indirizzo di rete](#)).

Un client può connettersi al Server tramite i record SRV nel seguente modo:

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



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

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

Per esempio, l'esecuzione dell'installer di Agent:

- 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 Server.



Se per la connessione, il Server non è indicato in modo esplicito, come il nome del servizio predefinito viene utilizzato `drwcs`.



Capitolo 4: Installazione dei componenti di Dr.Web Enterprise Security Suite

4.1. 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'installazione del pacchetto completo di Server Dr.Web consiste in due fasi:

1. Installazione del *pacchetto principale*. Il pacchetto principale permette di installare il Server Dr.Web stesso che include i pacchetti di protezione antivirus soltanto per le postazioni Windows.
2. Installazione *del pacchetto supplementare (extra)*. Il pacchetto supplementare include i pacchetti di tutti i prodotti per l'impresa forniti che possono essere installati sulle postazioni protette con tutti i SO supportati. Viene installato come un supplemento su un computer su cui è già installato il pacchetto principale di Server Dr.Web.

L'avanzamento del processo di installazione di Server Dr.Web dipende dalla versione del Server (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 di rete antivirus nel processo del funzionamento del Server.

Se il software Server è già installato, consultare le rispettive 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, è stato rimosso un Server installato in precedenza, durante l'installazione verranno cancellati i contenuti del repository e verrà installata una sua versione nuova. Se per qualche motivo è stato mantenuto il repository della versione precedente, è necessario cancellarne manualmente tutti i contenuti prima di installare la nuova versione del Server ed è necessario aggiornare il repository completamente dopo l'installazione del Server.

La lingua del nome della directory in cui viene installato il Server deve corrispondere alla lingua indicata nelle impostazioni di lingua del SO Windows per i programmi che non utilizzano Unicode. Altrimenti, l'installazione del Server non verrà avviata.

Eccezione – 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 per configurare il Server.



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.

4.1.1. 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. I permessi di accesso devono essere configurati così affinché 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 manuale dei componenti Dr.Web Enterprise Security Suite](#)).

Se si utilizza un database esterno, si deve creare prima un database e configurare il driver corrispondente (v. il documento **Allegati**, p. [Allegato B. Impostazioni necessarie per l'utilizzo di DBMS. Parametri dei driver di DBMS](#)).

L'installer del Server supporta la modalità di modifica di prodotto. Per aggiungere o rimuovere singoli componenti, per esempio driver per la gestione dei database, basta avviare l'installer del Server e selezionare l'opzione **Modifica**.

In [Immagine 4-1](#) 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](#).

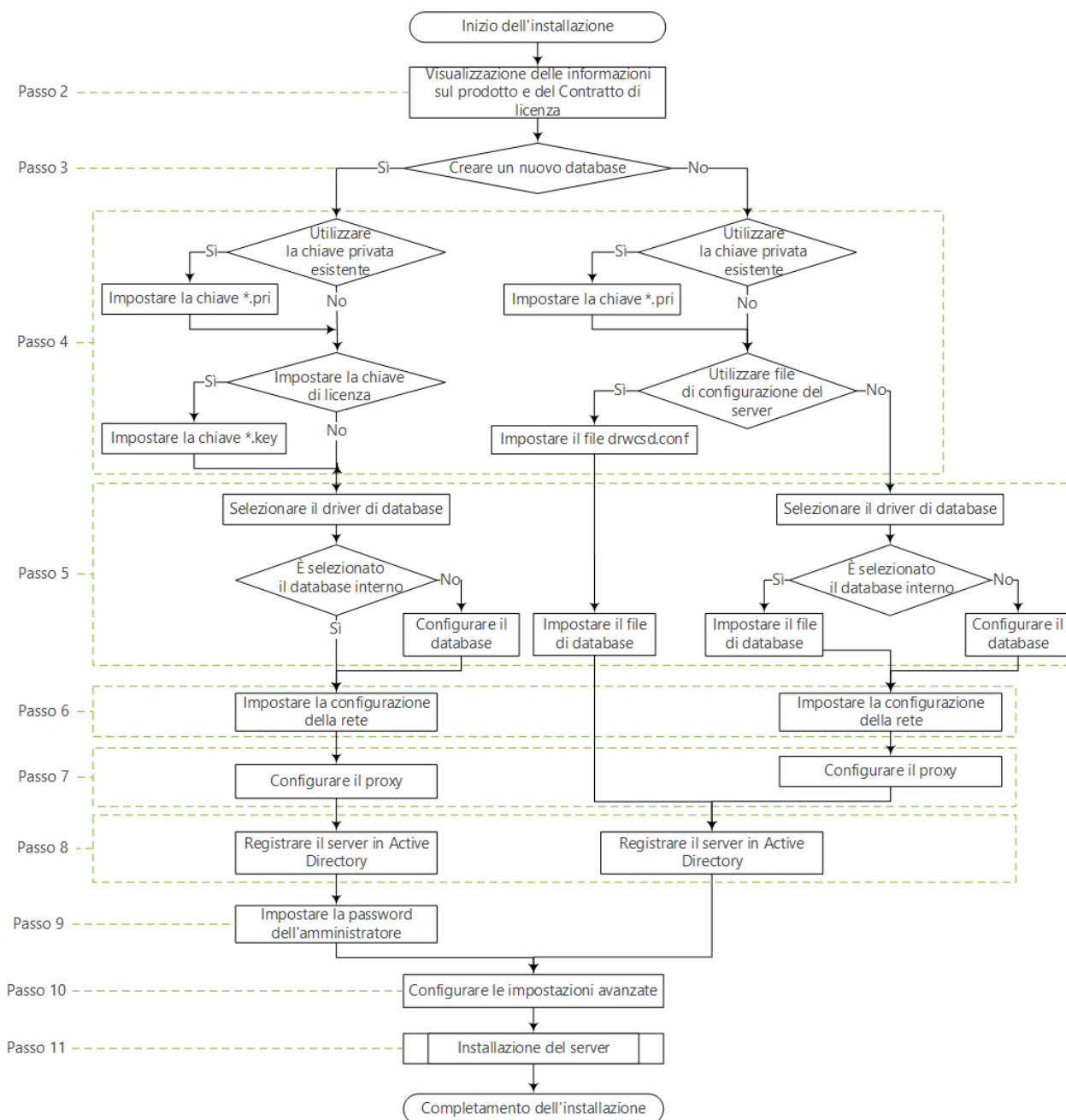


Immagine 4-1. Schema a blocchi del processo di installazione di Server Dr.Web (Premere un blocco dello schema per passare alla descrizione)

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

1. Avviare il file del pacchetto.



Di default, come la 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 le informazioni sul prodotto che viene installato e con il testo del contratto di licenza. Dopo aver letto i termini del Contratto di licenza, per continuare l'installazione, spuntare il flag **Accetto i termini del Contratto di licenza** e premere il pulsante **Installa**.



3. Nella finestra successiva selezionare quale database deve essere utilizzato per la rete antivirus:
- **Crea un nuovo database** – per creare una nuova rete antivirus.
 - **Usa il database esistente** – per mantenere il database del Server dell'installazione precedente. Il file del database può essere indicato in seguito (v. passaggio 5).

4. Nella finestra successiva configurare le impostazioni del database.

a) Se nel passo 3 si è selezionata l'opzione **Crea un nuovo database**, nella finestra **Impostazioni del nuovo database** configurare le seguenti impostazioni:

- Il flag **Imposta chiave di licenza** consente di impostare il file della chiave di licenza di Agent Dr.Web nel corso dell'installazione di Server.
 - Se il flag è deselezionato, il Server viene installato senza la chiave di licenza di Agent. In questo caso le chiavi di licenza devono essere aggiunte dopo l'installazione del Server, attraverso la [Gestione licenze](#).
 - Se il flag è selezionato, è necessario impostare nel campo corrispondente il percorso del file della chiave di licenza di Agent.
- Il flag **Utilizza la chiave di cifratura privata esistente** consente di utilizzare le chiavi di cifratura esistenti, per esempio quelle da un'installazione precedente di Server.
- In caso della prima installazione di Server togliere il flag **Utilizza la chiave di cifratura privata esistente**. Le nuove chiavi di cifratura verranno generate automaticamente nel processo di installazione.
- Se si installa il Server per una rete antivirus esistente, spuntare il flag **Utilizza la chiave di cifratura privata esistente** ed impostare nel campo corrispondente il percorso del file con la chiave privata. Verrà creato automaticamente un file con la chiave pubblica (i contenuti della chiave pubblica corrisponderanno ai contenuti della chiave pubblica precedente). Questo consentirà agli Agent già installati di connettersi al nuovo Server. Nel caso contrario, dopo l'installazione sarà necessario copiare la nuova chiave di cifratura pubblica su tutte le postazioni su cui in precedenza sono stati installati gli Agent Dr.Web.
Se un errore si verifica durante l'estrazione della chiave pubblica, impostare il percorso del file con la relativa chiave pubblica manualmente nel campo che si è aperto **Impostare la chiave di cifratura pubblica**.

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](#)).

b) Se nel passo 3 si è selezionata l'opzione **Usa il database esistente**, nella finestra **Impostazioni del database esistente** configurare le seguenti impostazioni:

- Il flag **Utilizza il file di configurazione esistente** consente di configurare le impostazioni del Server.
 - Se il flag è deselezionato, verrà creato un file di configurazione di Server con le impostazioni predefinite.
 - Se il flag è selezionato, è necessario impostare nel campo corrispondente il percorso del file di configurazione di Server.
- Il flag **Utilizza la chiave di cifratura privata esistente** consente di utilizzare le chiavi di cifratura esistenti, per esempio quelle da un'installazione precedente di Server.



- In caso della prima installazione di Server togliere il flag **Utilizza la chiave di cifratura privata esistente**. Le nuove chiavi di cifratura verranno generate automaticamente nel processo di installazione.
- Se si installa il Server per una rete antivirus esistente, spuntare il flag **Utilizza la chiave di cifratura privata esistente** ed impostare nel campo corrispondente il percorso del file con la chiave privata. Verrà creato automaticamente un file con la chiave pubblica (i contenuti della chiave pubblica corrisponderanno ai contenuti della chiave pubblica precedente). Questo consentirà agli Agent già installati di connettersi al nuovo Server. Nel caso contrario, dopo l'installazione sarà necessario copiare la nuova chiave di cifratura pubblica su tutte le postazioni su cui in precedenza sono stati installati gli Agent Dr.Web.
Se un errore si verifica durante l'estrazione della chiave pubblica, impostare il percorso del file con la relativa chiave pubblica manualmente nel campo che si è aperto **Impostare la chiave di cifratura pubblica**.

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. Nella finestra **Driver di database**, vengono configurati i parametri del database in uso che dipendono dalla scelta del tipo di database nel passo **3** e dalla disponibilità del file di configurazione di Server, impostato nel passo **4**:
 - Se nel passo **3** si è selezionata l'opzione **Crea un nuovo database** o per l'opzione **Usa il database esistente** nel passo **4** non si è impostato il percorso del file di configurazione di Server, selezionare il driver da utilizzare. Con questo:
 - 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 negli allegati (v. documento **Allegati**, p. [Allegato B. Impostazioni necessarie per l'utilizzo di DBMS. Parametri dei driver di DBMS](#)).
 - Se nel passo **3** si è selezionata l'opzione **Usa il database esistente** e nel passo **4** si è impostato il percorso del file di configurazione di Server, impostare il percorso del file del database che verrà utilizzato secondo il file di configurazione di Server impostato.
6. Se nel passo **3** si è selezionata l'opzione **Crea un nuovo database** o per l'opzione **Usa il database esistente** nel passo **4** non si è impostato il percorso del file di configurazione di Server, si aprirà la finestra **Configurazione della rete**. In questa finestra viene impostato il protocollo di rete per il funzionamento del Server (è consentito impostare soltanto un protocollo di rete; è possibile configurare ulteriori protocolli in seguito).

Per assegnare le impostazioni di rete da un set predefinito, selezionare dalla lista a cascata una delle seguenti varianti:

- **Configurazione standard** prescrive l'utilizzo delle impostazioni predefinite sulla base del servizio di rilevamento di Server.
- **Configurazione limitata** prescrive la limitazione del funzionamento del Server alla sola interfaccia di rete interna – 127.0.0.1. Con queste impostazioni si può gestire il Server sol-



tanto dal Pannello di controllo aperto sullo stesso computer, nonché al Server può connettersi soltanto l'Agent avviato sullo stesso computer. In seguito, dopo la configurazione delle impostazioni del Server, le impostazioni di rete potranno essere modificate.

- **Configurazione personalizzata** significa la modificazione delle seguenti impostazioni predefinite:
 - Nei campi **Interfaccia** e **Porta** impostare i rispettivi valori per le connessioni al Server. Di default, è impostata l'interfaccia 0.0.0.0, il che significa che si può accedere al Server su tutte le interfacce.



Di default viene utilizzata la porta 2193.

Notare: nelle versioni Server 4 veniva utilizzata la porta 2371. Nella versione 10 questa porta non è più supportata.

Gli indirizzi vengono impostati nel formato di indirizzo di rete riportato nel documento **Allegati**, nella sezione [Allegato E. Specifica di indirizzo di rete](#).

- Spuntare il flag **Limita l'accesso al Server Dr.Web**, per limitare l'accesso locale al Server. L'accesso verrà negato agli Installer di Agent, agli Agent ed agli altri Server (se vi è già una rete antivirus costruita con l'ausilio di 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 **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.
7. Se nel passo **3** si è selezionata l'opzione **Crea un nuovo database** o per l'opzione **Usa il database esistente** nel passo **4** non si è impostato il percorso del file di configurazione di Server, si aprirà la finestra di **Server proxy** per configurare le impostazioni dell'utilizzo del server proxy per la connessione al Server:

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.
8. 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.
9. Se nel passo **3** si è selezionata l'opzione **Crea un nuovo database**, si aprirà la finestra **Password dell'amministratore**. Impostare la password dell'amministratore di rete antivirus, creato di default con il nome utente **admin** e con i completi permessi di gestione della rete antivirus.
10. Nella finestra successiva la Procedura guidata informa che è pronta ad installare il Server. Se necessario, si possono configurare parametri aggiuntivi di installazione. 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 cartella 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 (di default viene impostato il nome nascosto della risorsa condivisa).
 - Spuntare il flag **Avvia il Server Dr.Web dopo la fine dell'installazione** per avviare il Server automaticamente dopo l'installazione.
 - Spuntare il flag **Aggiorna repository dopo la fine dell'installazione** per aggiornare automaticamente il repository di Server subito dopo il completamento dell'installazione.
 - 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 **Cartella di installazione di Server Dr.Web** viene impostata la directory in cui viene installato il Server. Per modificare la directory predefinita, premere il pulsante **Sfoggia** e selezionare la directory desiderata.
 - Nel campo **Cartella per il backup di Server Dr.Web** viene impostata la directory in cui verranno salvati i backup dei dati critici del Server secondo il calendario dei task del Server. Per cambiare la directory predefinita, premere il pulsante **Sfoggia** e selezionare la directory desiderata.
 - Nella scheda **Componenti** si possono selezionare i componenti che si desidera installare.



Se si intende utilizzare ODBC per Oracle come il database esterno, annullare l'installazione del client incorporato per il DBMS Oracle (nella sezione **Supporto dei database** → **Driver del database Oracle**).

Nel caso contrario, l'utilizzo del database Oracle non sarà possibile per conflitto di librerie.

- Nella scheda **Log** si possono configurare le impostazioni della registrazione del log dell'installazione e del funzionamento del Server.

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.

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

12. 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 del Server.

Quando il Server viene installato, nel menu principale del SO Windows **Programmi** viene collocata la directory **Dr.Web Server** contenente i seguenti elementi di configurazione e di gestione base del Server:

- La directory **Gestione del server** contiene i comandi di avvio, di riavvio e di arresto del Server, nonché i comandi di configurazione del logging e gli altri comandi del Server descritti in dettaglio nel documento **Allegati**, p. [H4. Server Dr.Web](#).
- La voce **Interfaccia web** – per aprire il Pannello di controllo e per connettersi al Server installato sul questo computer (sull'indirizzo <http://localhost:9080>).
- La voce **Documentazione** – per aprire la documentazione dell'amministratore in formato HTML.

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

4.1.2. Installazione di Server Dr.Web per SO della famiglia UNIX®



Tutte le azioni di installazione si devono eseguire dalla console con l'account del superutente (**root**).

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

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

```
sh ./<file_pacchetto>.run
```



Per eseguire il pacchetto d'installazione, è possibile utilizzare le opzioni della riga di comando. I parametri del comando di esecuzione sono riportati nel documento **Allegati**, p. [H11](#).



[Installer del Server Dr.Web per i SO della famiglia UNIX®](#)

Il nome predefinito dell'amministratore di rete antivirus è **admin**, la password predefinita è **root**.

2. In seguito viene riportato il testo del contratto di licenza. Per continuare l'installazione, si deve accettare il contratto di licenza.
3. Quando il programma domanda quale directory deve essere utilizzata per il backup, impostare il percorso della directory desiderata o confermare la directory predefinita – /var/tmp/drwcs.
4. Se nel sistema è stato rilevato un pacchetto supplementare (extra), verranno visualizzate le informazioni circa la necessità di rimuovere il pacchetto supplementare prima di iniziare a installare il pacchetto di Server. 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.



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

Utilizzare i comandi:

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



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

4.1.3. Installazione del pacchetto supplementare di Server Dr.Web

Il pacchetto supplementare (extra) deve essere installato su un computer su cui è già installato il pacchetto principale di Server Dr.Web. L'installazione del pacchetto principale di Server è descritta nella sezione [Installazione di Server Dr.Web per SO Windows®](#) e [Installazione di Server Dr.Web per SO della famiglia UNIX®](#).



Il pacchetto supplementare deve essere dello stesso tipo del pacchetto principale.

Per installare il pacchetto supplementare di Server Dr.Web su un computer con il SO Windows:

1. Avviare il file del pacchetto.
2. Si apre la finestra **Dr.Web ESuite Extra** con le informazioni sul prodotto da installare e con il testo del Contratto di licenza. Dopo aver letto i termini del Contratto di licenza, per continuare



l'installazione, selezionare **Accetto i termini del Contratto di licenza** e premere il pulsante **Installa**.

3. Inizia l'installazione del pacchetto supplementare. Se non si verificano errori nel processo di installazione, non viene richiesto l'intervento dell'utente.
4. Dopo la fine dell'installazione, premere il pulsante **Fine**. Non viene richiesto il riavvio del computer.

Per installare il pacchetto supplementare di Server Dr.Web su un computer con un SO della famiglia UNIX:

1. Avviare il file del pacchetto tramite il seguente comando:

```
sh ./<file_pacchetto>.run
```

2. In seguito viene riportato il testo del contratto di licenza. Per continuare l'installazione, si deve accettare il contratto di licenza.
3. In seguito il software viene installato.

4.1.4. Installazione dell'estensione del Pannello di controllo della sicurezza Dr.Web



L'installazione dell'Estensione del Pannello di controllo della sicurezza Dr.Web per i browser Mozilla Firefox, Opera e Chrome è possibile solo per le versioni che funzionano sotto i SO Windows e i SO della famiglia Linux.

L'Estensione del Pannello di controllo della sicurezza Dr.Web è necessaria per l'utilizzo delle complete funzionalità del Pannello di controllo (v. inoltre [Requisiti di sistema del Pannello di controllo della sicurezza Dr.Web](#)).

L'estensione viene fornita insieme al pacchetto d'installazione di Server e può essere installata:

1. Automaticamente, a richiesta del browser nel processo di utilizzo del Pannello di controllo, in particolare degli elementi che necessitano del caricamento dell'estensione (per lo Scanner di rete in caso di installazione remota dei componenti antivirus).
2. Manualmente, attraverso l'installer dell'estensione del Pannello di controllo della sicurezza Dr.Web.

Installazione manuale dell'estensione del Pannello di controllo della sicurezza Dr.Web

Per scaricare l'installer dell'estensione del Pannello di controllo della sicurezza Dr.Web per un'installazione manuale:

1. Aprire il Pannello di controllo. Se l'Estensione del Pannello di controllo della sicurezza Dr.Web non è ancora installata nel browser in uso, sotto il menu principale viene visualizzata una raccomandazione su installazione dell'estensione.



- Utilizzare il link **Installa l'estensione di browser per il Pannello di controllo della sicurezza Dr.Web**.

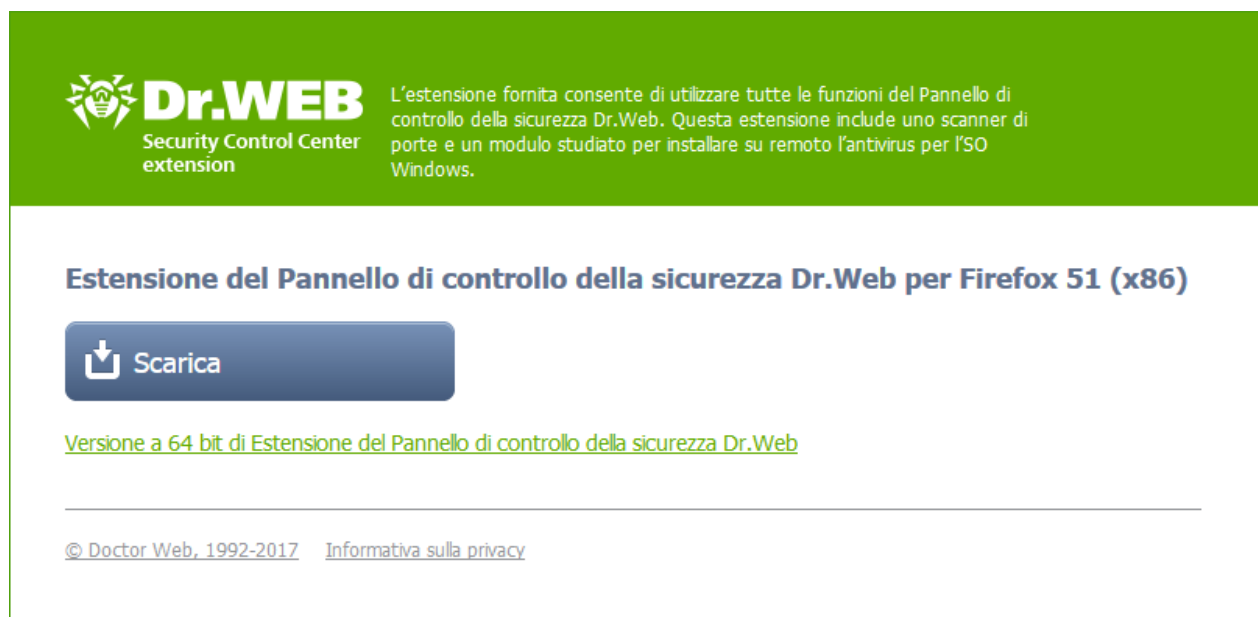


Immagine 4-2. Sezione per il download dell'estensione del Pannello di controllo della sicurezza Dr.Web

- Nella sezione del download dell'estensione sono specificati la versione del browser web attuale e il proposto numero di bit (x86 o x64) dell'estensione.
Per i SO della famiglia UNIX, è disponibile una lista a cascata da cui si può selezionare la versione del pacchetto per il SO corrispondente.
- Per scaricare e salvare l'estensione, premere il pulsante **Scarica**. È quindi possibile installarla [manualmente](#).
- Per cambiare ad una versione con un altro numero di bit, fare clic sul link sotto il pulsante di download, dopodiché l'installer può essere scaricato come viene descritto nel passaggio **4**.

Per installare l'estensione del Pannello di controllo della sicurezza Dr.Web sotto il SO Windows:

- Avviare il file del pacchetto. Si apre la finestra **InstallShield Wizard** che avvisa sul prodotto da installare. Premere il pulsante **Avanti**.
- 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**.
- Si apre la finestra di scelta della directory di installazione. Se è necessario cambiare la directory di installazione predefinita, premere il pulsante **Modifica** e selezionare una directory per l'installazione. Premere il pulsante **Avanti**.
- Nella finestra successiva premere il pulsante **Installa** per iniziare il processo di installazione. Le azioni successive del programma di installazione non richiedono l'intervento dell'utente.
- Dopo il completamento dell'installazione, premere il pulsante **Finito**.



Per installare l'estensione del Pannello di controllo della sicurezza Dr.Web sotto il SO della famiglia UNIX:

Eeguire il seguente comando:

- per pacchetti **deb**:

```
dpkg -i drweb-esuite-plugins-linux-<versione_pacchetto>.deb
```

- per i pacchetti **rpm**:

```
rpm -i drweb-esuite-plugins-linux-<versione_pacchetto>.rpm
```

- per gli altri sistemi (pacchetti **tar.bz2** e **tar.gz**):

1. Decomprimere l'archivio contenente l'estensione.
2. Creare una directory per le estensioni se non è ancora creata.

Per esempio, in caso del browser Mozilla Firefox:

```
mkdir /usr/lib/mozilla/plugins
```

3. Copiare nella directory per le estensioni la libreria decompressa al passaggio 1.

Per esempio, in caso del browser Mozilla Firefox:

```
cp libnp*.so /usr/lib/mozilla/plugins
```



Dopo aver installato l'estensione del Pannello di controllo della sicurezza Dr.Web sotto il SO della famiglia UNIX, riavviare il web browser se era in esecuzione.

4.2. 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.

Se sulla postazione è già installato l'Antivirus, prima di iniziare la nuova installazione, è necessario [rimuovere](#) l'Antivirus installato.

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. [Su remoto](#).

L'installazione remota è disponibile soltanto per le postazioni SO Windows e viene eseguita nel Pannello di controllo attraverso la rete locale. Viene eseguita dall'amministratore della rete antivirus. L'intervento dell'utente non è richiesto.



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

Se sulla postazione SO Windows è disponibile il prodotto standalone Dr.Web versione 7/8/9/10/11, l'installazione di Agent di Dr.Web Enterprise Security Suite versione 10 avviene secondo il seguente schema:

- Se l'installer o il pacchetto d'installazione di Agent viene avviato in modalità GUI su una postazione con un prodotto standalone installato versione 7.0/8.0/9.0/9.1/10.0, verrà avviato l'installer del prodotto installato. Dopo cui all'utente verrà richiesto di immettere il codice di conferma delle azioni e di rimuovere il prodotto. Dopo il riavvio del sistema operativo, verrà avviato l'installer in versione GUI che è stato avviato inizialmente per l'installazione dell'Agent per Dr.Web Enterprise Security Suite versione 10.
- Se l'installer di Agent viene avviato in modalità silenziosa su una postazione con un prodotto standalone installato versione 7.0/8.0/9.0/9.1/10.0, nessun'azione verrà eseguita. In caso di un'[installazione remota](#), l'installer restituirà al Pannello di controllo un messaggio sulla disponibilità di prodotti standalone versioni precedenti. In tale caso è necessario rimuovere manualmente il prodotto standalone e installare l'Agent per Dr.Web Enterprise Security Suite versione 10 in qualsiasi dei modi possibili.
- Se l'installer di Agent viene avviato su una postazione con il prodotto standalone installato versione 11.0, il prodotto installato verrà cambiato da modalità standalone a modalità di protezione centralizzata. Dopo la connessione e l'autenticazione sul Server, è possibile ricevere aggiornamenti, nuove impostazioni e liste dei componenti da installare, a seconda di cui potrebbe 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 sui computer che svolgono il ruolo di terminal server (nel SO Windows sono installati i servizi **Terminal Services**), per assicurare l'operazione degli Agent nelle sessioni terminale utente, l'installazione degli Agent deve essere eseguita solo localmente tramite la procedura guidata di installazione e di eliminazione dei programmi nel **Pannello di controllo** SO Windows.
- Sui server che svolgono le funzioni di rete critiche (controller di dominio, server di distribuzione licenze ecc.), non è consigliabile installare i componenti SplDer Gate, Office control, SplDer Mail e Dr.Web Firewall per evitare eventuali conflitti dei servizi di rete e dei componenti interni dell'antivirus Dr.Web.
- L'installazione di Agent su cluster deve essere eseguita separatamente su ogni nodo del cluster.
- I principi di funzionamento dell'Agent e dei componenti del pacchetto antivirus su un nodo del cluster sono uguali a quelli su un server standard di LAN, quindi non è consigliabile installare i componenti SplDer Gate, SplDer Mail e Dr.Web Firewall sui nodi del cluster.
- Se l'accesso alla risorsa quorum del cluster è strettamente limitato, si consiglia di escluderlo dal controllo da parte della guardia SplDer Guard e di limitarsi ai controlli regolari della risorsa tramite lo Scanner avviato nel modo programmato o manualmente.



4.2.1. File di installazione

Pacchetti di installazione

Pacchetto d'installazione personale

Quando viene creato un nuovo account di postazione nel Pannello di controllo viene generato un pacchetto d'installazione personale per l'installazione di Agent Dr.Web. Il pacchetto d'installazione personale include l'installer di Agent Dr.Web e un set di impostazioni per la connessione al Server Dr.Web e per l'approvazione della postazione sul Server Dr.Web.

I pacchetti d'installazione personali per le postazioni protette sono disponibili per tutti i sistemi operativi supportati da Dr.Web Enterprise Security Suite. In particolare:

- Per le postazioni SO Windows è disponibile un pacchetto d'installazione personale generato nel Pannello di controllo sulla base dell'[installer di rete](#) di Agent. Le impostazioni della connessione al Server e le impostazioni dell'approvazione della postazione sul Server sono incluse direttamente nel pacchetto d'installazione personale.
- Per le postazioni SO Android, SO Linux, OS X il pacchetto d'installazione personale consiste in un [installer](#) per l'installazione di Agent e in un file di configurazione con le impostazioni di connessione al Server e con le impostazioni di approvazione della postazione sul Server.



Per ottenere i pacchetti d'installazione personali sotto i sistemi operativi diversi da SO Windows, è necessario [installare il pacchetto supplementare \(extra\)](#) di Server Dr.Web.

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

1. Subito dopo la creazione di una nuova postazione (v. passo **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.

Installer

L'Installer di Agent è diverso dal pacchetto di installazione in quanto non include le impostazioni della connessione a Server e dell'autenticazione della postazione su Server.



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

- Per le postazioni SO Windows sono disponibili due tipi di installer:
 - *L'installer di rete* `drwinst.exe` installa addirittura Agent. Dopo la connessione a Server Agent 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 `drwinst.exe` si trova nella directory `Installer` (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 10](#) dell'installazione di Server Dr.Web. In seguito, è possibile cambiare questa risorsa a propria discrezione.
 - *L'installer completo* `drweb-esuite-agent-full-<versione_di_Agent>-<versione_di_build>-windows.exe` installa contemporaneamente Agent e il pacchetto antivirus.
- Per le postazioni SO Android, Linux, OS X è disponibile un installer di Agent Dr.Web simile all'installer della versione standalone.

Gli Installer per l'Antivirus 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, è necessario [installare il pacchetto supplementare \(extra\)](#) di Server Dr.Web.

Pagina di installazione

Dalla pagina di installazione del Pannello di controllo della sicurezza Dr.Web è possibile scaricare:

1. Installer di Agent Dr.Web.

L'Installer per le postazioni protette sotto tutti gli SO supportati da Dr.Web Enterprise Security Suite, si trovano nelle directory con i nomi che corrispondono al nome del determinato SO.

2. La chiave di cifratura pubblica `drwcsd.pub`.

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

```
http://<indirizzo_server>:<numero_porta>/install/
```

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

4.2.2. 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 del Server (v. **Manuale dell'amministratore**, p. [Aggiornamento manuale dei componenti di Dr.Web Enterprise Security Suite](#), p. **Verifica disponibilità aggiornamenti**).

Postazioni SO Android, SO Linux, OS X

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

- [Pacchetto d'installazione personale](#) 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 d'installazione personale, viene messo a disposizione un installer di Agent Dr.Web, mentre le impostazioni di connessione al Server e quelle di autenticazione della postazione sul Server vengono messe a disposizione in un file di configurazione.
- b) In caso di installazione tramite l'installer, l'Agent Dr.Web viene installato, ma le impostazioni di connessione al Server e quelle di autenticazione della postazione sul Server non vengono messe a disposizione.

Postazioni SO Windows

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

- [Pacchetto d'installazione personale](#) creato nel Pannello di controllo `drweb-ess-installer.exe`.
- [L'installer completo](#) di Agent Dr.Web `drweb-esuite-agent-full-<versione_di_Agent>-<versione_di_build>-windows.exe`.
- [Installer di rete](#) di Agent Dr.Web `drwinst.exe`.

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

- a) Quando il software viene installato dal pacchetto d'installazione personale, le impostazioni di connessione al Server e quelle di autenticazione della postazione sul Server sono incluse nel pacchetto d'installazione. L'installazione tramite il pacchetto d'installazione personale viene eseguita sulla base dell'installer di rete da cui l'Agent viene installato direttamente. Dopo che si è connesso al Server, l'Agent scarica ed installa i componenti del pacchetto antivirus.
- b) In caso di installazione tramite il pacchetto completo, vengono installati contemporaneamente Agent e il pacchetto antivirus. Le impostazioni di connessione a Server e quelle di autenticazione della postazione su Server non vengono messe a disposizione.
- c) In caso di installazione tramite l'installer di rete, soltanto Agent viene installato. Dopo che si è connesso a Server, Agent scarica ed installa i componenti corrispondenti del pacchetto antivirus. Le impostazioni di connessione a Server e quelle di autenticazione della postazione su Server non vengono messe a disposizione.



Caratteristiche comparative dei file di installazione

File di installazione		Installazione di Agent	Installazione del pacchetto antivirus	Parametri della connessione al Server	Parametri dell'autenticazione sul server
Pacchetto d'installazione personale		+	-	+	+
Installer	Di rete	+	-	-	-
	Completo	+	+	-	-



Per ottenere i pacchetti d'installazione e gli installer per postazioni sotto i sistemi operativi diversi da SO Windows, nonché l'installer completo per postazioni SO Windows, è necessario [installare il pacchetto supplementare \(extra\)](#) di Server Dr.Web.



Inoltre, è possibile eseguire tutti i tipi di file di installazione di Agent dalla riga di comando con utilizzo delle opzioni riportate nel documento **Allegati**, p. [H2. Installer di rete](#).

4.2.2.1. Installazione di Agent Dr.Web attraverso il pacchetto d'installazione personale

Per installare l'Agent Dr.Web su postazioni protette attraverso un pacchetto d'installazione personale:

1. Tramite il Pannello di controllo [creare un account](#) di nuovo utente sul Server Dr.Web.
2. Inviare all'utente un link del pacchetto d'installazione personale di Agent Dr.Web corrispondente al sistema operativo del computer o del dispositivo mobile, se il software Agent Dr.Web verrà installato dall'utente stesso. Se il software viene installato su una postazione con un sistema operativo diverso dal SO Windows, è anche necessario inviare all'utente il file di configurazione con le impostazioni di connessione al Server Dr.Web (v. passo **11** della procedura [Creazione del nuovo account di postazione](#)).



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 l' Agent Dr.Web su 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 il software antivirus, l'installer cercherà di eliminarlo prima di cominciare l'installazione. Se il tentativo non è riuscito, l'utente dovrà per contro proprio eliminare il software antivirus utilizzato sulla postazione.

4. [Configurare le impostazioni di connessione](#) al Server Dr.Web direttamente sulla postazione.

Creazione del nuovo account di postazione

Per creare un account o diversi account di nuovi utenti, utilizzare il Pannello di controllo della sicurezza Dr.Web.



Creando l'account utente, prestare attenzione al nome del Server impostato nelle seguenti sezioni del Pannello di controllo:

1. **Amministrazione** → **Configurazione del web server** → campo **Server** (viene custodito nel parametro `<server-name />` nel file di configurazione `webmin.conf`). Il valore di questo parametro viene sostituito quando viene generato un link di un pacchetto d'installazione di Agent.

Se il valore di questo parametro non è impostato in nessuno posto, come il nome del Server per la generazione del link al download dell'installer Agent, 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 **Server** (viene custodito nel parametro `<name />` nel file di configurazione `download.conf`). Il valore di questo parametro viene trascritto nei pacchetti d'installazione di Agent e determina a quale Server si conatterà l'Agent ad installazione.

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

Per creare un nuovo utente tramite il Pannello di controllo della sicurezza Dr.Web:

1. Selezionare la voce **Rete antivirus** del menu principale del Pannello di controllo.
2. Nella barra degli strumenti premere il pulsante **+** **Aggiungi una postazione o un gruppo**. Dal sottomenu che si è aperto, selezionare la voce **+** **Crea una postazione**. Nella parte destra della finestra del Pannello di controllo si apre una barra per la creazione di nuovo account utente.
3. Nel campo **Numero** indicare il numero di utenti da creare.



4. Nel campo **Identificatore** viene generato automaticamente l'identificatore unico 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 è connessa al Server, questo nome può essere sostituito automaticamente al nome impostato localmente sulla postazione.
6. Nei campi **Password** e **Digitare di nuovo la password** si può impostare una password con cui la postazione accede al Server. Se non viene indicata, la password verrà generata automaticamente.



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

7. Nel campo **Descrizione** inserire le informazioni supplementari su utente. 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, si può includerci la postazione che viene creata, senza limitazioni sul numero di gruppi in cui rientra la postazione. Per farlo, spuntare i flag di fronte ai gruppi desiderati nella lista **Appartenenza**.



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**.


9. Se necessario, compilare la sezione **Sicurezza**. La descrizione delle impostazioni di questa sezione è riportata nel **Manuale dell'amministratore** sezione [Sicurezza](#).
10. Se necessario, compilare la sezione **Posizione**.
11. Premere su **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 dell'installer di Agent.



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

Per ottenere i pacchetti d'installazione sotto i sistemi operativi diversi da SO Windows, è necessario [installare il pacchetto supplementare \(extra\)](#) di Server 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 Android, OS X e Linux.
- Nel punto **Password** verrà riportata la password di accesso al Server per questa postazione. Per visualizzare la password, premere .



I link al download dell'installer di Agent 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.

- In questa finestra è inoltre disponibile il pulsante **Installa** progettato per l'[installazione remota di Agent Dr.Web tramite il Pannello di controllo della sicurezza Dr.Web](#).

12. Le azioni di installazione di Agent Dr.Web su postazione sono riportate nel **Manuale dell'utente** per il sistema operativo corrispondente.

Configurazione della connessione al Server Dr.Web

• Postazioni SO Windows

Quando l'Agent Dr.Web viene installato sulle postazioni SO Windows tramite il pacchetto d'installazione personale, non è richiesta alcuna configurazione aggiuntiva. Le impostazioni di connessione al Server e le impostazioni di autenticazione della postazione sul Server sono incluse direttamente nel pacchetto d'installazione personale. Dopo l'installazione dell'Agent, la postazione si conetterà al Server in modo automatico.

• Postazioni SO Android

1. Sulla schermata principale del dispositivo mobile richiamare il menu dell'applicazione Antivirus Dr.Web e selezionare la voce **Impostazioni**.
2. Sulla schermata **Dr.Web – Impostazioni** sezione **Modalità** spuntare il flag **Agent Dr.Web**.
3. Le impostazioni di connessione al Server, per esempio l'indirizzo IP e le impostazioni di autenticazione sul Server vengono configurate automaticamente secondo il file di configurazione `install.cfg`.

Per utilizzare il file, memorizzarlo in una directory del primo livello di nidificazione sulla scheda SD. Se il file è stato caricato sul dispositivo, i campi di input delle impostazioni di connessione al Server verranno compilati automaticamente.

4. Premere il pulsante **Connettiti**.

• Postazioni OS X

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, per esempio l'indirizzo IP e le impostazioni di autenticazione sul Server vengono configurate automaticamente secondo il file di configurazione `install.cfg`.



Per utilizzare il file:

- a) Nel Gestore 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 l'installazione del file, i campi di input delle impostazioni di connessione al Server verranno compilati automaticamente.

• Postazioni SO famiglia Linux

1. Nel menu dell'applicazione Dr.Web per Linux fare clic sulla voce **Impostazioni** e selezionare la sezione **Modalità**.
2. Spuntare il flag **Attiva la modalità di protezione centralizzata**.
3. Dalla lista a cascata selezionare la voce **Carica da file** e indicare il percorso del file di configurazione `install.cfg`. In tale caso le impostazioni di connessione al Server, quale l'indirizzo IP e le impostazioni di autenticazione sul Server, verranno compilate in modo automatico.
4. Premere il pulsante **Connetti**.

4.2.2.2. Installazione di Agent Dr.Web attraverso installer

L'Installer di Agent è diverso dal pacchetto di installazione in quanto non include le impostazioni della connessione a Server e dell'autenticazione della postazione su Server.

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, è necessario [installare il pacchetto supplementare \(extra\)](#) di Server Dr.Web.

Installazione locale su postazioni Android, Linux, OS X

Per le postazioni SO Android, Linux, OS X 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 per la connessione della postazione.



Le impostazioni di autenticazione possono essere impostate manualmente o si può omettere di impostarle. Sono possibili le seguenti varianti di connessione al Server:

Variante del task	Impostazioni di autenticazione
Viene impostato manualmente	La postazione cerca di autenticarsi automaticamente secondo le impostazioni di autenticazione.
Non viene impostato	Il principio di autenticazione sul Server dipende dalle impostazioni del Server per la connessione delle postazioni nuove (per maggiori informazioni v. Manuale dell'amministratore , p. Criteri di approvazione delle postazioni).



Per indicare le impostazioni di autenticazione manualmente, è necessario prima creare un nuovo account di postazione nel Pannello di controllo. In tale caso sarà disponibile il [pacchetto d'installazione](#) che include un file di configurazione con le impostazioni di connessione e di autenticazione. Si consiglia di utilizzare il pacchetto d'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 soltanto Agent. Dopo la connessione a Server Agent scarica e installa i componenti corrispondenti del pacchetto antivirus.
- *l'installer completo* `drweb-esuite-agent-full-<versione_di_Agent>-<versione_di_build>-windows.exe` installa contemporaneamente Agent e il pacchetto antivirus.

Nelle installazioni attraverso questi installer è possibile non indicare le impostazioni di connessione a Server e di autenticazione o impostarle manualmente.



Per indicare le impostazioni di autenticazione manualmente, è necessario prima creare un nuovo account di postazione nel Pannello di controllo. In tale caso sarà disponibile il [pacchetto d'installazione](#). Se non c'è necessità di installare il software tramite il pacchetto completo o l'installer di rete, si consiglia di utilizzare il pacchetto d'installazione invece dell'installer.

Sono possibili le seguenti varianti di connessione al Server:

Variante del task	Indirizzo del Server	Impostazioni di autenticazione
Viene impostato manualmente	La postazione si connette direttamente al Server impostato.	La postazione cerca di autenticarsi automaticamente secondo le impostazioni di autenticazione.



Variante del task	Indirizzo del Server	Impostazioni di autenticazione
Non viene impostato	Agent cerca Server nella rete utilizzando il <i>Servizio di rilevamento Server</i> . Cerca di connettersi al primo Server trovato.	Il principio di autenticazione sul Server dipende dalle impostazioni del Server per la connessione delle postazioni nuove (per maggiori informazioni v. Manuale dell'amministratore , p. Criteri di approvazione delle postazioni).



Nel **Manuale dell'utente** per SO Windows, sono descritte le varianti dell'installazione di Agent Dr.Web tramite l'installer completo e tramite il pacchetto d'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 `drwinst.exe` è disponibile per l'installazione di Agent soltanto in SO Windows.

Se l'installer di rete viene avviato in modalità di installazione standard (cioè senza l'opzione `/installMode remove`) su una postazione su cui il software è stato installato in precedenza, nessuna azione verrà eseguita. L'Installer finisce di operare 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 silenziosa* – si avvia se è stata impostata l'opzione di modalità silenziosa.
2. *Modalità grafica* – la modalità predefinita. Si avvia se non è stata impostata l'opzione di modalità silenziosa.

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 silenziosa dell'installer:

1. Dal computer su cui verrà installato il software antivirus accedere alla directory di rete d'installazione di Agent (durante l'installazione di Server è la sottodirectory `Installer` della directory di installazione di Server, in seguito è possibile spostarla) o scaricare dalla [pagina di installazione del](#) Pannello di controllo il file eseguibile dell'installer `drwinst.exe` e la chiave di cifratura pubblica `drwcsd.pub`. Eseguire il file `drwinst.exe` con l'opzione della modalità silenziosa `/silent yes`.

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



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

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

- Quando non viene utilizzata la modalità *Multicast*, nel corso dell'installazione di Agent si consiglia di indicare esplicitamente il nome del Server (previa registrazione del nome nel servizio DNS):

```
drwinst /silent yes /server <nome_DNS_Server>
```

Questo semplificherà il processo di configurazione della rete antivirus nel caso si dovrà reinstallare il Server Dr.Web su un altro computer.

- Inoltre, si può indicare esplicitamente l'indirizzo del Server, ad esempio:

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

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



La lista completa dei parametri dell'Installer di rete è riportata nel documento **Allegati**, p. [H2. Installer di rete](#).

2. Dopo la fine del funzionamento dell'installer, sul computer verrà installato il software Agent (ma non il pacchetto antivirus).
3. Dopo che la postazione è stata approvata sul Server (se lo richiedono le impostazioni del Server), viene automaticamente installato il pacchetto antivirus.
4. Riavviare il computer a richiesta di Agent.

Per installare Agent Dr.Web su una postazione in modalità grafica dell'installer:

Dal computer su cui verrà installato il software antivirus accedere alla directory di rete d'installazione di Agent (durante l'installazione di Server è la sottodirectory `Installer` della directory di installazione di Server, in seguito è possibile spostarla) o scaricare dalla [pagina di installazione](#) del Pannello di controllo il file eseguibile dell'installer `drwinst.exe` e la chiave di cifratura pubblica `drwcsd.pub`. Eseguire il file `drwinst.exe`.

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



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



4.2.3. Rimozione di Agent Dr.Web per SO Windows®

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

L'installazione remota è possibile nelle seguenti varianti:

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



L'installazione remota di Agent Dr.Web è possibile soltanto sulle postazioni sotto i SO della famiglia Windows (v. documento **Allegati**, p. [Allegato A. Lista completa delle versioni supportate dei SO](#)), ad eccezione delle edizioni Starter e Home.

L'installazione remota di Agent Dr.Web è possibile soltanto dal Pannello di controllo avviato sotto un SO della famiglia Windows (v. documento **Allegati**, p. [Allegato A. Lista completa delle versioni supportate dei SO](#)).

Per installare l'Agent Dr.Web in remoto su postazioni, si devono avere privilegi di amministratore sulle postazioni corrispondenti.

Per l'installazione remota tramite il Pannello di controllo, 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 file e stampanti (consultare la tabella sotto per la posizione dell'impostazione in diverse versioni del SO Windows).

Se le postazioni remote non fanno parte del dominio o per l'installazione viene utilizzato l'account locale, in alcune versioni del SO Windows è necessaria la configurazione aggiuntiva delle postazioni remote.

Configurazione aggiuntiva da eseguire quando il software viene installato su remoto sulle postazioni fuori dominio o con l'utilizzo dell'account locale



Le impostazioni indicate potrebbero abbassare la sicurezza della postazione remota. Si consiglia vivamente di scoprire la destinazione delle impostazioni indicate prima di apportare modifiche al sistema oppure di rinunciare all'installazione remota e di installare l'Agent [in maniera manuale](#).

Dopo aver configurato la postazione remota, si consiglia di ripristinare tutte le impostazioni personalizzate ai valori che sono stati impostati prima della modifica per non violare i criteri di sicurezza fondamentali del sistema operativo.



Se l'Agent viene installato in remoto su una postazioni di fuori del dominio e/o con l'utilizzo dell'account locale, sul computer su cui verrà installato l'Agent, si devono eseguire le seguenti azioni:

SO	Impostazione	
Windows XP	Configurare la modalità di accesso ai file condivisi	Stile nuovo: Start → Impostazioni → Pannello di controllo → Aspetto e temi → Proprietà cartelle → Scheda Aspetto → togliere il flag Utilizza condivisione file semplice (scelta consigliata)
		Stile classico: Start → Impostazioni → Pannello di controllo → Proprietà cartelle → Scheda Aspetto → togliere il flag Utilizza condivisione file semplice (scelta consigliata)
	Impostare autenticazione a livello di rete nei criteri locali	Stile nuovo: 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.
	Stile classico: 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.	
	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: Start → Impostazioni → Pannello di controllo → Rete e Internet → Centro connessioni di rete e condivisione → Condivisione e individuazione → Condivisione di file → Attiva.
		Stile classico:



SO	Impostazione	
		Start → Impostazioni → Pannello di controllo → Centro connessioni di rete e condivisione → Condivisione e individuazione → Condivisione di file → Attiva.
	Impostare autenticazione a livello di rete nei criteri locali	Stile nuovo: Start → Impostazioni → Pannello di controllo → Il 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. Stile classico: 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.
	Creare la chiave LocalAccountTokenFilterPolicy : a) Nell'editor del registro di sistema, aprire il ramo HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System . Se il record LocalAccountTokenFilterPolicy non esiste, nel menu Modifica selezionare Nuovo ed impostare il valore DWORD . Immettere il valore LocalAccountTokenFilterPolicy e premere INVIO. b) Nel menu contestuale della voce LocalAccountTokenFilterPolicy selezionare Modifica . c) Nel campo Valore impostare il valore 1 e fare clic su OK . Il riavvio non è richiesto.	
Windows 7 Windows Server 2008 R2	Attivare Condivisione file e stampanti	Stile nuovo: 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. Stile classico: Start → Pannello di controllo → Centro connessioni di rete e condivisione → Modifica impostazioni di condivisione avanzate → Condivisione file e stampanti → Attivare Condivisione file e stampanti.



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



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

Se per l'account sulla postazione remota è stata impostata una password vuota, impostare nei criteri locali il criterio di accesso con 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**.



Si devono collocare il file dell'installer di Agent `drwinst.exe` e la chiave di cifratura pubblica `drwcsd.pub` su una risorsa condivisa.

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

Sono possibili i seguenti modi dell'installazione su remoto degli Agent 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 opportuno se si conosce in anticipo l'indirizzo della postazione o del gruppo di postazioni sulle quali verranno installati gli Agent.

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

Consente di installare gli Agent su postazioni o in gruppi di postazioni per gli account selezionati (anche per tutti gli account nuovi disponibili) con gli ID e le password di accesso al Server 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 su postazioni, si consiglia di utilizzare Scanner di rete (v. **Manuale dell'amministratore**, p. [Scanner di rete](#)), il quale cerca computer per indirizzo IP.

Per installare Agent, utilizzando Scanner di rete:

1. Aprire Scanner di rete. Per farlo, selezionare la voce **Amministrazione** del menu principale del Pannello di controllo, nella finestra che si è aperta, selezionare la voce del menu di gestione Scanner di rete. Si apre la finestra con lo stesso nome senza i dati caricati.
2. Spuntare il flag **Ricerca per indirizzo IP** per cercare postazioni nella rete a seconda degli indirizzi IP impostati. Nel campo **Reti** specificare una lista delle reti nel formato:
 - separati da trattino (per esempio, 10.4.0.1-10.4.0.10),
 - separati da virgola e spazio (per esempio, 10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90),
 - con il prefisso di rete (per esempio, 10.4.0.0/24).
3. In caso di SO Windows: spuntare il flag **Cerca le postazioni nel dominio di Active Directory** per cercare le postazioni nel dominio di Active Directory. Inoltre, impostare i seguenti parametri:
 - **Domini** – lista dei domini in cui verranno cercate le postazioni. Utilizzare una virgola come separatore per diversi domini.
 - **Controller di Active Directory** – controller di Active Directory, ad esempio, [dc.example.com](#).



Per cercare postazioni in un dominio di Active Directory per mezzo di Scanner di rete, è necessario che il web browser, in cui è aperto il Pannello di controllo, sia avviato da un utente di dominio con i permessi di ricerca di oggetti in Active Directory.

Le impostazioni avanzate sono descritte dettagliatamente nella sezione del **Manuale dell'amministratore**, p. [Scanner di rete](#).

4. Premere il pulsante **Scansiona**. Nella finestra viene caricata una directory (lista gerarchica) dei computer in cui è indicato su quali computer il software antivirus è installato e su quali non è installato.
5. 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 4-1. Possibili tipi di icone

Icona	Descrizione
Gruppi di lavoro	
	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.
Postazioni	
	La postazione trovata è registrata nel database ed è attiva (postazioni attive con il software antivirus installato).
	La postazione trovata è registrata nel database nella tabella di postazioni eliminate.
	La postazione trovata non è registrata nel database (sul computer non è installato il software antivirus).
	La postazione trovata non è registrata nel database (la postazione è connessa a un altro Server).
	La postazione trovata è registrata nel database, non è attiva, e la porta è chiusa.

Si possono espandere inoltre gli elementi della directory corrispondenti alle postazioni con le icone o per visualizzare una lista dei componenti installati.

6. Nella finestra di **Scanner di rete** scegliere il computer non protetto (oppure più computer non protetti utilizzando i tasti CTRL o MAIUSCOLO).
7. Nella barra degli strumenti premere il pulsante **Installa Agent Dr.Web**.
8. Si apre la finestra **Installazione via rete** per creare un task di installazione dell'Agent.
9. 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.

Per installare il software Agent contemporaneamente su più computer, si possono indicare più indirizzi IP dei computer nel seguente formato:

- separati da trattino (per esempio 10.4.0.1-10.4.0.10),
- separati da virgola e spazio (per esempio, 10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90),
- con il prefisso di rete (per esempio, 10.4.0.0/24).

10. Di default, il software Agent 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.

11. Di default nel campo **Server Dr.Web** viene 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 da cui verrà installato il software antivirus. Quando vengono impostati diversi Server, 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.

12. Nel campo **Chiave di cifratura pubblica** indicare il percorso della chiave di cifratura pubblica di Server Dr.Web.

13. Nel campo **File eseguibile di Installer di rete** impostare il percorso di Installer di rete di Agent Dr.Web.



Se la chiave di cifratura pubblica e il file eseguibile di Installer di rete si trovano su una risorsa condivisa, i percorsi devono essere indicati nel formato di indirizzi di rete.

14. Dalla lista a cascata **Lingua** selezionare la lingua di interfaccia per Antivirus Dr.Web che verrà installato sulle postazioni.

15. Se necessario, inserire nel campo **Avanzate** i parametri da riga di comando per l'avvio di Installer di rete (per maggiori informazioni v. documento **Allegati**, p. [H2. Installer di rete](#)).

16. Nel campo **Time-out dell'installazione (sec)** impostare il tempo massimo di attesa del completamento di installazione di Agent in secondi. Valori ammissibili: 1-600. Di default, è impostato il valore di 180 secondi. Con capacità bassa del canale di comunicazione tra il Server e l'Agent, si consiglia di aumentare il valore di questo parametro.


17. Se necessario, spuntare il flag **Registra Agent Dr.Web nella lista dei programmi installati**.

18. Nella sezione **Componenti da installare** selezionare i componenti del pacchetto antivirus che verranno installati sulla postazione.

19. Nelle sezioni **Compressione** e **Cifratura** impostare i parametri di compressione e di cifratura del traffico dati, utilizzati da Installer di rete durante l'installazione dell'Agent e del pacchetto antivirus. Queste impostazioni verranno inoltre utilizzate dall'Agent per l'interazione con il Server dopo l'installazione.



20. Nella sezione **Autenticazione sul computer remoto** indicare le impostazioni di autenticazione per l'accesso ai computer remoti su cui verrà installato Agent.

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, prima viene utilizzato il primo account nella lista. Se l'installazione sotto questo account fallisce, viene utilizzato l'account successivo e così via.

21. Dopo aver inserito tutti i parametri necessari, premere **Installa**.



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

22. L'Agent Dr.Web verrà installato sulle postazioni indicate. Dopo l'approvazione della postazione sul Server (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 in modo automatico.

23. Riavviare il computer a richiesta dell'Agent.

Utilizzo dello strumento Installazione via rete

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

Per l'installazione attraverso la rete:


1. Selezionare la voce **Amministrazione** del menu principale, nella finestra che si è aperta selezionare la voce del menu di gestione **Installazione via rete**.
2. I passi successivi di installazione sono uguali ai passi **8-22** della procedura [sopra](#).

Installazione per account con gli ID specificati

Per installare gli Agent su remoto per account con gli ID specificati:

1. Se viene creato un nuovo account di postazione:
 - a) Creare un nuovo account o diversi nuovi account di postazioni (v. p. [Creazione di nuovo account](#)).
 - b) 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**.
 - c) Si apre la finestra di Scanner di rete.
 - d) I passi successivi di installazione sono uguali ai passi **2-22** della procedura [sopra](#).
 - e) Dopo la fine dell'installazione, controllare se nella lista gerarchica sono cambiate le [icone](#) delle postazioni corrispondenti.



2. Se viene utilizzato un account di postazione già esistente:
 - a) Nella lista gerarchica della rete antivirus selezionare una nuova postazione o un gruppo di postazioni su cui non sono ancora stati installati gli Agent, oppure selezionare il gruppo **New** (per installare su tutti i nuovi account disponibili).
 - b) Nella barra degli strumenti premere il pulsante  **Installa Agent Dr.Web**.
 - c) Si apre la finestra di Scanner di rete.
 - d) I passi successivi di installazione sono uguali ai passi **2-22** della procedura [sopra](#).
 - e) Dopo la fine dell'installazione, controllare se nella lista gerarchica sono cambiate le [icone](#) delle postazioni corrispondenti.



L'installazione dell'Agent sulle postazioni con ID selezionati è accessibile anche per l'amministratore di gruppi.



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

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

Se nella rete locale protetta si utilizza il servizio **Active Directory**, si può installare l'Agent Dr.Web sulle postazioni su remoto.



L'installazione di Agent con utilizzo di Active Directory è inoltre possibile se viene utilizzato il file system distribuito DFS (v. documento **Allegati**, p. [Utilizzo di DFS nell'installazione di Agent via Active Directory](#)).

Installazione di Agent

Per installare Agent, utilizzando il servizio Active Directory:

1. Scaricare dal sito <http://download.drweb.com/esuite/> il programma di installazione di Agent Dr.Web per le reti con **Active Directory**.
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, non è necessario aggiornare l'installer di Agent Dr.Web per le reti con Active Directory. Dopo l'aggiornamento del software Server, gli Agent e il software antivirus sulle postazioni vengono 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 d'installazione di Agent Dr.Web per le reti con **Active Directory** di solito ha il seguente formato:

```
drweb-esuite-agent-activedirectory-<versione>-<data-del-rilascio>.msi
```

Parametri

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

- **ESSERVERADDRESS=<nome_DNS>** – l'indirizzo del Server Dr.Web a cui si conetterà l'Agent. Per i formati possibili, consultare il documento **Allegati**, p. [Allegato E2](#).
- **ESSERVERPATH=<percorso_nome_file>** – il percorso completo della chiave di cifratura pubblica del Server Dr.Web e il nome del file (di default, è il file `drwcsd.pub` nella sottodirectory `Installer` della directory di installazione del Server Dr.Web).
- **TARGETDIR** – la directory di rete per l'immagine di Agent (il pacchetto d'installazione di Agent modificato), che viene selezionata attraverso l'editor Criteri di gruppo per un'installazione stabilita. Tale directory deve essere disponibile per lettura e scrittura. Il percorso della directory deve essere scritto nel formato di indirizzi di rete, anche quando è disponibile localmente; la directory deve essere obbligatoriamente accessibile dalle postazioni di destinazione.



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

Se è necessario eseguire l'installazione amministrativa da diversi Server, si consiglia di impostare una directory target diversa per ciascun Server.



Dopo la distribuzione del pacchetto amministrativo, nella directory <directory_target>\Program Files\DrWeb deve trovarsi soltanto il file `README.txt`.



Esempi:

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

```
msiexec /a ES_Agent.msi /qn ESSERVERADDRESS=192.168.14.1 ESSERVERPATH="C:\Program Files\DrWeb Server\Installer\drwcsd.pub" 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 target dell'immagine Agent non comprenda l'installer di Agent Dr.Web per le reti con **Active Directory** (<nome_pacchetto>.msi).



Dopo la distribuzione del pacchetto amministrativo, nella directory:

```
<directory_target>\Program Files\DrWeb
```

deve trovarsi soltanto 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 le informazioni sul prodotto. Premere il pulsante **Avanti**.



L'installer di Agent 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**, p. [Allegato E2](#)). Indicare il percorso della chiave pubblica del Server Dr.Web (drwcsd.pub). Premere il pulsante **Avanti**.
4. Nella finestra successiva, indicare la directory di rete in cui verrà scritto l'immagine di Agent. 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 target. 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 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 del SO Windows 2000 Server – **Unità organizzativa**) con il nome, come esempio, **ESS**. Per farlo, 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.
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. In seguito assegnare il pacchetto d'installazione Agent. Per farlo, indicare l'indirizzo della risorsa di rete condivisa (l'immagine Agent) 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 programma di installare l'Agent Dr.Web tramite il pacchetto msi configurabile sui sistemi operativi a 64 bit, spuntare il flag **Rendere quest'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 a seconda delle installazioni precedenti dell'Agent

Quando vengono assegnati i criteri di Active Directory per l'installazione di Agent, si deve tenere presente che l'Agent potrebbe essere già 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 installato rimane sulla postazione.



In questo caso, l'Agent è installato sulla postazione, però Active Directory considera l'Agent come non installato. Pertanto, dopo ogni caricamento della postazione, viene ripetuto il tentativo infruttuoso di installazione dell'Agent tramite Active Directory.

Per installare l'Agent via Active Directory, si deve eliminare manualmente (o tramite il Pannello di controllo) l'Agent 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.

4.3. Installazione di NAP Validator

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



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

Per installare NAP Validator, eseguire le seguenti azioni:

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** che avvisa sul prodotto da installare. 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**.

4.4. Installazione del Server proxy

Uno o più Server proxy possono far parte della rete antivirus.

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



L'installazione del Server proxy deve essere eseguita dall'utente con i permessi dell'amministratore di tale computer.

Per stabilire una connessione tra il Server e i client attraverso il Server proxy, si consiglia di disattivare la cifratura del traffico. Per farlo, basta impostare il valore **no** per il parametro **Crittografia** nella sezione **Configurazione del Server Dr.Web** (v. **Manuale dell'amministratore**, sezione [Configurazione del Server Dr.Web → Generali](#)).

Di seguito viene descritta l'installazione del Server proxy. I passi e la loro sequenza possono variare leggermente a seconda della versione del pacchetto.



Per installare il Server proxy su un computer con SO Windows:

1. Avviare il file del pacchetto. Si apre la finestra **InstallShield Wizard** che avvisa sul prodotto da installare. Premere il pulsante **Next**.
2. Si apre la finestra con il testo del Contratto di licenza. Dopo aver letto i termini del Contratto di licenza, selezionare la voce **Accetto i termini del Contratto di licenza** e premere il pulsante **Next**.
3. Si apre la finestra di configurazione dei parametri principali del Server proxy:
 - Nel campo **Listen to** impostare l'indirizzo IP su cui il Server proxy "è in ascolto". Di default è any (0.0.0.0) – cioè "sii in ascolto" su tutte le interfacce.



Gli indirizzi vengono impostati nel formato di indirizzo di rete riportato nel documento **Allegati**, nella sezione [Allegato E. Specifica di indirizzo di rete](#).

- Nel campo **Port** impostare il numero di porta su cui il Server proxy "è in ascolto". Di default è la porta 2193.
- Spuntare il flag **Enable discovery** per attivare la modalità di simulazione del Server. Questa modalità consente a Scanner di rete di rilevare il Server proxy come Server Dr.Web. Per la modalità di simulazione del Server sono disponibili le seguenti impostazioni:
 - Spuntare il flag **Enable multicasting**, affinché il Server proxy risponda alle query multicast indirizzate al Server.
 - Nel campo **Multicast group** impostare l'indirizzo IP del gruppo multicast di cui farà parte il Server proxy. Sull'interfaccia indicata il Server proxy sarà in ascolto per interagire con gli Installer di rete durante la ricerca dei Server Dr.Web attivi nella rete. Se il campo viene lasciato vuoto, il Server proxy non farà parte di alcun gruppo multicast. Di default il gruppo multicast di cui il Server fa parte è 231.0.0.1.
- Dalla lista a cascata **Compression mode** selezionare la modalità di compressione di traffico per i canali tra il Server proxy e i client: Agent ed installer di Agent. Nel campo **Level** impostare il livello di compressione. Sono permessi i numeri interi da 1 a 9.

Dopo aver configurato le impostazioni principali, premere il pulsante **Next**.

4. Si apre la finestra di configurazione della memorizzazione nella cache del Server proxy:

Spuntare il flag **Enable caching** per memorizzare nella cache i dati trasmessi dal Server proxy ed impostare i seguenti parametri:

 - Per cambiare la directory predefinita di memorizzazione della cache, premere il pulsante **Browse** e selezionare una nuova directory nel visualizzatore di file system.
 - Nel campo **Maximum revisions number** impostare il numero massimo di revisioni conservate. Di default, vengono conservate 3 ultime revisioni, le revisioni più vecchie vengono rimosse.
 - Nel campo **Cleanup interval** specificare l'intervallo di tempo in minuti che intercorre tra una rimozione delle vecchie revisioni e un'altra. Di default è di 60 minuti.
 - Nel campo **Unload interval** specificare l'intervallo di tempo in minuti che intercorre tra uno scaricamento da memoria dei file non utilizzati e un altro. Di default è di 10 minuti.



- Dalla lista a cascata **Integrity check mode** selezionare la modalità di verifica dell'integrità della cache:
 - **At startup** – al momento dell'avvio del Server proxy (può richiedere molto tempo).
 - **Idle** – in modalità background del Server proxy.

Dopo aver configurato la memorizzazione nella cache, premere il pulsante **Next**.

5. Si apre la finestra di configurazione del reindirizzamento delle connessioni:

Nel blocco **Redirection settings** impostare l'indirizzo o una lista degli indirizzi dei Server Dr.Web su cui verranno reindirizzate le connessioni stabilite dal Server proxy.



Gli indirizzi vengono impostati nel formato di indirizzo di rete riportato nel documento **Allegati**, nella sezione [Allegato E. Specifica di indirizzo di rete](#).

Dalle liste a cascata **Compression mode** selezionare le modalità di compressione dei dati trasmessi su canali di comunicazione tra il Server proxy e ciascuno dei Server Dr.Web impostati.

Dopo aver configurato il reindirizzamento, premere il pulsante **Next**.

6. Si apre la finestra di scelta della directory di installazione. Se è necessario cambiare la directory di installazione predefinita, premere il pulsante **Change** e selezionare una directory per l'installazione.

Premere il pulsante **Next**.

7. Si apre una finestra che avvisa che il Server proxy è pronto per l'installazione. Per iniziare l'installazione del Server proxy, premere il pulsante **Install**.

8. Dopo il completamento del processo di installazione premere il pulsante **Finish**.

Dopo la fine dell'installazione, se necessario, si possono modificare le impostazioni del Server proxy. A questo fine si usa il file di configurazione `drwcsd-proxy.xml` che si trova nella seguente directory:

- in SO Windows: `C:\ProgramData\Doctor Web\drwcsd-proxy\`
- in SO Linux e SO Solaris: `/var/opt/drwcs/etc`
- in SO FreeBSD: `/var/drwcs/etc`

Le impostazioni del file di configurazione sono elencate nel documento **Allegati**, p. [Allegato G4](#).

Per installare il Server proxy su un computer con un SO della famiglia UNIX:

Eeguire il seguente comando:

```
sh ./<file_pacchetto>.run
```



Nel corso di installazione del software sotto SO **FreeBSD** viene creato uno script `rc /usr/local/etc/rc.d/0.dwcp-proxy.sh`.

Utilizzare i comandi:



- `/usr/local/etc/rc.d/0.dwcp-proxy.sh stop` – per l'arresto manuale del Server proxy;
- `/usr/local/etc/rc.d/0.dwcp-proxy.sh start` – per l'avvio manuale del Server proxy.

Durante l'installazione del software sotto SO **Linux** e SO **Solaris** verrà creato uno script `init` per l'avvio e per l'arresto del Server proxy `/etc/init.d/dwcp-proxy`.



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

5.1. Rimozione di Server Dr.Web

5.1.1. Rimozione di Server Dr.Web per SO Windows®

Per rimuovere il software Server Dr.Web (pacchetto principale e quello supplementare) o l'estensione del Pannello di controllo della sicurezza Dr.Web, avviare il pacchetto d'installazione corrispondente al prodotto di quella versione che è installata. L'installer determina automaticamente il prodotto di programma e propone di rimuoverlo. Per rimuovere il software, premere il pulsante **Elimina**.

Inoltre, si può rimuovere il software Server Dr.Web (pacchetto principale e quello supplementare) o l'estensione del Pannello di controllo della sicurezza Dr.Web tramite i mezzi standard del SO Windows tramite l'elemento **Pannello di controllo** → **Installazione e eliminazione programmi**.



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

5.1.2. Rimozione di Server Dr.Web per SO della famiglia UNIX®



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

Rimozione del pacchetto principale di Server Dr.Web

1. La procedura di eliminazione del Server dipende dal sistema operativo e dalla versione installata del Server.

a) Per rimuovere un Server versione 6 e inferiori, eseguire le seguenti azioni:

SO Server		Azione
FreeBSD		Eseguire il comando: <code>pkg_delete drweb-esuite</code>
Solaris		1. Terminare il Server: <code>/etc/init.d/drwcsd stop</code> 2. Eseguire il comando: <code>pkgrm DWEBesuit</code>
Linux	Debian Ubuntu	Eseguire il comando: <code>dpkg -r drweb-esuite</code>



SO Server		Azione
	pacchetto rpm	Eseguire il comando: <code>rpm -e drweb-esuite</code>
	pacchetto generic	Avviare lo script <code>/opt/drwcs/bin/drweb-esuite-uninstall.sh</code>

b) Per rimuovere il Server versione 10, eseguire le seguenti azioni:

SO Server		Azione
FreeBSD		Avviare lo script <code>/usr/local/etc/opt/software/drweb-esuite.remove</code>
Solaris		1. Terminare il Server: <code>/etc/init.d/drwcsd stop</code> 2. Eseguire il comando: <code>pkgrm drweb-esuite</code>
Linux	Debian	Eseguire il comando: <code>dpkg -P drweb-esuite</code>
	Ubuntu	
	pacchetto rpm	Eseguire il comando: <code>rpm -e drweb-esuite</code>
	pacchetto generic	Avviare lo script <code>/etc/opt/drweb.com/software/drweb-esuite.remove</code>

2. Nel SO **Solaris** è necessario confermare la propria intenzione di eliminazione del software, nonché accettare la necessità di eseguire gli script di eliminazione dall'account amministratore (**root**).



Quando il Server viene eliminato nei SO **FreeBSD** e **Linux**, i processi server verranno terminati automaticamente, il database e i file delle chiavi e di configurazione verranno copiati nella directory predefinita – `/var/tmp/drwcs`.

Rimozione del pacchetto supplementare di Server Dr.Web

1. Per rimuovere il pacchetto supplementare di Server versione 10, eseguire le seguenti azioni:

SO Server		Azione
FreeBSD		Avviare lo script <code>/usr/local/etc/opt/software/drweb-esuite-extra.remove</code>
Solaris		1. Terminare il Server: <code>/etc/init.d/drwcsd stop</code> 2. Eseguire il comando: <code>pkgrm drweb-esuite-extra</code>



SO Server		Azione
Linux	Debian	Eseguire il comando: <code>dpkg -P drweb-esuite-extra</code>
	Ubuntu	
	pacchetto rpm	Eseguire il comando: <code>rpm -e drweb-esuite-extra</code>
	pacchetto generic	Avviare lo script <code>/etc/opt/drweb.com/software/drweb-esuite-extra.remove</code>

2. Nel SO **Solaris** è necessario confermare la propria intenzione di eliminazione del software, nonché accettare la necessità di eseguire gli script di eliminazione dall'account amministratore (**root**).

Rimozione dell'estensione del Pannello di controllo della sicurezza Dr.Web

Per rimuovere l'estensione del Pannello di controllo della sicurezza Dr.Web, eseguire il seguente comando:

Tipo di pacchetto	Comando
pacchetto deb	<code>dpkg -P drweb-esuite-plugins</code>
pacchetto rpm	<code>rpm -e drweb-esuite-plugins</code>
gli altri pacchetti (tar.bz2 e tar.gz)	<code>rm -f <directory_plugin>/libnp*.so</code> Per esempio, in caso del browser Mozilla Firefox: <code>rm -f /usr/lib/mozilla/plugins/libnp*.so</code>

5.2. 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 è stato installato attraverso questo servizio.
- In caso delle postazioni SO Android, SO Linux, OS X – localmente sulla postazione.



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



5.2.1. Rimozione di Agent Dr.Web per SO Windows®

Rimozione di Agent Dr.Web e del pacchetto antivirus attraverso la rete



L'installazione e l'eliminazione del software Agent su remoto è possibile solamente nella rete locale e richiedono i privilegi di amministratore in questa rete.



Se Agent e il pacchetto antivirus vengono eliminati tramite il Pannello di controllo, dalla postazione non verrà eliminata la Quarantena.

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

1. Selezionare la voce **Rete antivirus** del 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. Il software Agent e il pacchetto antivirus verranno rimossi dalle postazioni selezionate.



Se il comando di avviare il processo di eliminazione viene dato quando non c'è la connessione tra il Server Dr.Web e la postazione antivirus, il software Agent verrà eliminato sulla postazione selezionata non appena la connessione verrà ripristinata.

Rimozione di Agent Dr.Web e del pacchetto antivirus localmente



Per poter eliminare localmente Agent e il pacchetto antivirus, questa opzione deve essere abilitata sul Server nella sezione **Permessi** (v. **Manuale dell'amministratore**, p. [Permessi dell'utente della postazione](#)).

L'eliminazione del software antivirus (Agent e pacchetto antivirus) sulla postazione può essere eseguita in due modi:

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



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



Eliminazione tramite i mezzi standard di SO Windows



Questo metodo di rimozione è solo possibile se durante l'installazione di Agent tramite l'installer grafico, è stato spuntato il flag **Registra l'agent nella lista dei programmi installati**.

Se Agent è stato installato in modalità silenziosa, la rimozione di software antivirus tramite i mezzi standard sarà disponibile solo se nell'installazione è stata utilizzata l'opzione `/register-agent yes`.

Per eliminare Agent 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).

Eliminazione tramite l'installer

• Modulo cliente `win-es-agent-setup.exe`

Per eliminare il software Agent e il pacchetto antivirus tramite il modulo client che viene creato durante l'installazione di Agent, eseguire il file d'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 d'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 e superiori e SO Windows Server 2008:
`%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 `drweb-ess-installer.exe`

Per eliminare il software Agent e il pacchetto antivirus tramite il pacchetto d'installazione, avviare il file d'installazione `drweb-ess-installer.exe` della versione del prodotto che è installata.

• L'installer completo `drweb-esuite-agent-full-<versione_di_Agent>-<versione_di_build>-windows.exe`

Per eliminare il software Agent e il pacchetto antivirus tramite l'installer completo, avviare il file d'installazione `drweb-esuite-agent-full-<versione_di_Agent>-<versione_di_build>-windows.exe` della versione del prodotto che è installata.



• Installer di rete drwinst.exe

Per eliminare il software Agent e il pacchetto antivirus tramite l'installer di rete sulla postazione localmente, è necessario nella directory d'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
```



Quando viene avviato il pacchetto di installazione `drweb-ess-installer.exe`, l'installer completo `drweb-esuite-agent-full-<versione_di_Agent>-<versione_di_build>-windows.exe` e l'installer di rete `drwinst.exe`, viene avviato il modulo client `win-es-agent-setup.exe` il quale esegue addirittura la rimozione.

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

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

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 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.



5.3. Eliminazione del Server proxy

Eliminazione del server proxy in caso di SO Windows



Quando viene eliminato il Server proxy, viene eliminato il file di configurazione `drwcsd-proxy.xml`. Se necessario, salvare il file di configurazione manualmente prima di eliminare il Server proxy.

Il software Server proxy viene eliminato tramite i mezzi standard del SO Windows attraverso la sezione **Pannello di controllo** → **Installazione e eliminazione programmi (Programmi e componenti** in caso del SO Windows 2008).

Eliminazione del server proxy in caso del SO della famiglia UNIX

SO del Server proxy		Azione
FreeBSD		Avviare lo script <code>/usr/local/etc/opt/software/drweb-proxy.remove</code>
Solaris		Eeguire il comando: <code>pkgrm drweb-esuite-proxy</code>
Linux	pacchetto deb	Eeguire il comando: <code>dpkg -P drweb-esuite-proxy</code>
	pacchetto rpm	Eeguire il comando: <code>rpm -e drweb-esuite-proxy</code>
	pacchetto generic	Avviare lo script <code>/etc/opt/drweb.com/software/drweb-proxy.remove</code>



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

Prima di cominciare ad aggiornare Dr.Web Enterprise Security Suite e singoli componenti, notare le seguenti importanti caratteristiche:

- Prima di iniziare l'aggiornamento, si consiglia vivamente di controllare se le impostazioni di accesso ad Internet del protocollo TCP/IP sono corrette. In particolare, il servizio DNS deve essere attivo ed avere le impostazioni corrette.
- Se la configurazione della rete include diversi server, si deve tenere presente che tra i Server versione 10 e i Server versione 6 non è possibile la trasmissione degli aggiornamenti tra i server e la comunicazione tra i server viene utilizzata soltanto per la trasmissione delle statistiche. Per assicurare la trasmissione degli aggiornamenti tra i server, è necessario aggiornare tutti i Server. Se è necessario lasciare nella rete antivirus i Server delle versioni precedenti per la connessione degli Agent installati sotto i SO non supportati dalla versione 10 (v. p. [Aggiornamento di Agent Dr.Web](#)), i Server versione 6 e i Server versione 10 devono ricevere gli aggiornamenti in modo indipendente.
- Se il Server viene aggiornato dalla versione 6 alla versione 10, le impostazioni del funzionamento di Server attraverso il server proxy non vengono salvate. Dopo aver installato la versione 10, è necessario configurare manualmente la connessione attraverso il server proxy (v. **Manuale dell'amministratore**, p. [Proxy](#)).
- Nel corso dell'aggiornamento automatico degli Agent, viene rimossa la vecchia versione di Agent e viene installata la nuova versione. La nuova versione di Agent viene installata secondo un task nel calendario di Server che verrà eseguito dopo il riavvio della postazione. Le postazioni devono essere riavviate manualmente dopo la rimozione della vecchia versione di Agent.



Dopo la rimozione di Agent, l'avviso di necessità di riavvio di postazione non viene visualizzato. L'amministratore deve lanciare manualmente il riavvio della postazione.

Nell'intervallo tra la rimozione della vecchia versione di Agent e l'installazione della nuova versione, le postazioni saranno senza protezione antivirus.

6.1. Aggiornamento di Server Dr.Web per SO Windows®

L'aggiornamento di Server dalla versione 6 alla versione 10 e all'interno della versione 10 viene eseguito automaticamente tramite l'installer.



Prima di rimuovere il Server di versione precedente, prestare attenzione alla sezione [Aggiornamento di Agent Dr.Web](#).



L'aggiornamento di Server all'interno della versione 10 inoltre può essere eseguito tramite il Pannello di controllo. La procedura viene descritta nel **Manuale dell'amministratore**, nella



sezione [Aggiornamento di Server Dr.Web e ripristino da copia di backup](#).

Non tutti gli aggiornamenti di Server all'interno della versione 10 contengono un file di pacchetto. Alcuni di essi possono essere installati soltanto tramite il Pannello di controllo.

Salvataggio dei file di configurazione

Quando viene rimosso un Server versione 6, vengono salvati automaticamente i seguenti file:

File	Descrizione	Directory
agent.key (il nome può essere diverso)	chiave di licenza di Agent	etc
certificate.pem	certificato per SSL	
drwcsd.conf (il nome può essere diverso)	file di configurazione del Server	
drwcsd.pri	chiave di cifratura privata	
enterprise.key (il nome può essere diverso)	chiave di licenza di Server	
private-key.pem	chiave privata RSA	
auth-ads.xml	file di configurazione per l'autenticazione esterna degli amministratori attraverso Active Directory	
auth-ldap.xml	file di configurazione per l'autenticazione esterna degli amministratori attraverso LDAP	
auth-radius.xml	file di configurazione per l'autenticazione esterna degli amministratori attraverso RADIUS	
dbinternal.dbs	database incorporato	var
drwcsd.pub	chiave di cifratura pubblica	<ul style="list-style-type: none">• Installer• webmin\install



Quando viene rimosso il Server versione 10, i seguenti file di configurazione vengono salvati nella:

File	Descrizione	Directory
<code>agent.key</code> (il nome può essere diverso)	chiave di licenza di Agent	etc
<code>enterprise.key</code> (il nome può essere diverso)	chiave di licenza di Server. Viene mantenuta soltanto se era presente dopo l'aggiornamento dalle versioni precedenti. Quando viene installato il nuovo Server 10, è assente	
<code>frontdoor.conf</code>	file di configurazione per l'utility di diagnostica remota di Server	
<code>auth-ads.xml</code>	file di configurazione per l'autenticazione esterna degli amministratori attraverso Active Directory	
<code>auth-ldap.xml</code>	file di configurazione per l'autenticazione esterna degli amministratori attraverso LDAP	
<code>auth-radius.xml</code>	file di configurazione per l'autenticazione esterna degli amministratori attraverso RADIUS	
<code>download.conf</code>	impostazioni di rete per la generazione dei pacchetti d'installazione di Agent	
<code>drwcsd.conf</code> (il nome può essere diverso)	file di configurazione del Server	
<code>drwcsd.conf.distr</code>	template del file di configurazione di Server con i parametri di default	
<code>drwcsd.pri</code>	chiave di cifratura privata	
<code>openssl.cnf</code>	certificato del Server per HTTPS	
<code>webmin.conf</code>	file di configurazione del Pannello di controllo	
<code>dbexport.gz</code>	esportazione del database	
<code>drwcsd.pub</code>	chiave di cifratura pubblica	<ul style="list-style-type: none">• Installer• webmin\install



Se si prevede di utilizzare i file di configurazione dalla versione precedente di Server, notare:

1. La chiave di licenza di Server non viene più utilizzata (v. p. [Capitolo 2: Concessione delle licenze](#)).



2. Il database incorporato viene aggiornato e il file di configurazione di Server viene convertito attraverso l'installer. Questi file non possono essere sostituiti con le copie automaticamente salvate quando si passa al Server versione 10.

Se necessario, salvare altri file importanti in un percorso diverso dalla directory di installazione del Server, per esempio, template dei report che si trovano nella directory `\var\templates`.

Salvataggio del database



Il database MS SQL CE non è più supportato a partire dalla versione Server Dr.Web 10. Quando il Server viene aggiornato automaticamente tramite l'installer, il database MS SQL CE viene convertito automaticamente nel database incorporato IntDB.

Prima di aggiornare il software Dr.Web Enterprise Security Suite, si consiglia di eseguire il backup del database.

Per salvare il database:

1. Arrestare il Server.
2. Esportare il database nel file:

```
"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 dei Server 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 è disponibile una copia di backup del database, non sarà possibile ripristinare il Server in caso di circostanze di emergenza.

Aggiornamento di Server Dr.Web

Per aggiornare il Server Dr.Web:

1. Avviare il file del pacchetto.



Di default, come la 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 che avvisa della disponibilità del software Server installato di versione precedente e fornisce una breve descrizione del processo di aggiornamento alla nuova versione. Per iniziare a configurare la procedura di aggiornamento, premere il pulsante **Aggiorna**.



3. Si apre una finestra con le informazioni sul prodotto e con il testo del contratto di licenza. Dopo aver letto i termini del Contratto di licenza, per continuare l'aggiornamento, spuntare il flag **Accetto i termini del Contratto di licenza** e premere il pulsante **Avanti**.
4. Nei passi successivi dell'installazione guidata il Server, che viene aggiornato, viene configurato in un modo simile al processo di [Installazione di Server Dr.Web](#) sulla base dei file di configurazione dalla versione precedente (v. [sopra](#)). L'installer determina automaticamente la directory d'installazione di Server, la posizione dei file di configurazione e del database incorporato dall'installazione precedente. Se necessario, si possono modificare i percorsi dei file trovati automaticamente dall'installer.



Se viene utilizzato un database esterno di Server, selezionare inoltre nel corso dell'aggiornamento l'opzione **Utilizza il database esistente**.



Se si programma di utilizzare come il database esterno i database Oracle o PostgreSQL attraverso la connessione ODBC, nel corso dell'aggiornamento di Server nelle impostazioni dell'installer annullare l'installazione del client incorporato per il relativo DBMS (nella sezione **Supporto dei database**).

Altrimenti, l'utilizzo del database Oracle attraverso ODBC non sarà possibile per conflitto di librerie.

5. Per iniziare la rimozione del Server versione precedente e l'installazione del Server versione 10 premere il pulsante **Installa**.



Finito l'aggiornamento dei Server della rete antivirus, è necessario configurare nuovamente la cifratura e la compressione di dati per i Server associati (v. **Manuale dell'amministratore**, sezione [Configurazione delle relazioni tra i Server Dr.Web](#)).

Dopo aver aggiornato il software Server Dr.Web, eseguire le seguenti azioni, necessarie per il normale funzionamento del Pannello di controllo:

1. Cancellare la cache del browser utilizzato per la connessione al Pannello di controllo.
2. [Aggiornare](#) l'estensione del Pannello di controllo della sicurezza Dr.Web.

6.2. Aggiornamento di Server Dr.Web per SO della famiglia UNIX®



Tutte le azioni di aggiornamento devono essere eseguite dall'account amministratore **root**.

L'aggiornamento delle versioni precedenti di Server alla versione 10 sopra la versione installata è possibile solo per alcuni SO della famiglia UNIX. Pertanto, in SO della famiglia UNIX in cui non è possibile aggiornare il software sopra il pacchetto già installato, è necessario prima rimuovere il software Server delle versioni precedenti, salvando una copia di backup, e quindi installare il software versione 10 sulla base della copia di backup salvata.



L'aggiornamento di Server all'interno della versione 10 per i tipi di pacchetti uguali viene eseguito automaticamente per tutti gli SO della famiglia UNIX.



Prima di rimuovere il Server di versione precedente, prestare attenzione alla sezione [Aggiornamento di Agent Dr.Web](#).



L'aggiornamento di Server all'interno della versione 10 inoltre può essere eseguito tramite il Pannello di controllo. La procedura viene descritta nel **Manuale dell'amministratore**, nella sezione [Aggiornamento di Server Dr.Web e ripristino da copia di backup](#).

Non tutti gli aggiornamenti di Server all'interno della versione 10 contengono un file di pacchetto. Alcuni di essi possono essere installati soltanto tramite il Pannello di controllo.

Salvataggio dei file di configurazione

Quando viene rimosso un Server versione 6, vengono salvati automaticamente i seguenti file:

File	Descrizione	Directory predefinita
agent.key (il nome può essere diverso)	chiave di licenza di Agent	<ul style="list-style-type: none">• in caso di SO Linux e SO Solaris: /var/opt/drwcs/etc• in caso di FreeBSD: /var/drwcs/etc
certificate.pem	certificato per SSL	
download.conf	impostazioni di rete per la generazione dei pacchetti d'installazione di Agent	
drwcsd.conf (il nome può essere diverso)	file di configurazione del Server	
drwcsd.pri	chiave di cifratura privata	
enterprise.key (il nome può essere diverso)	chiave di licenza di Server	
private-key.pem	chiave privata RSA	
webmin.conf	file di configurazione del Pannello di controllo	
common.conf	file di configurazione (per alcuni SO della famiglia UNIX)	
local.conf	impostazioni del log di Server	



File	Descrizione	Directory predefinita
dbinternal.dbs	database incorporato	<ul style="list-style-type: none">in caso di SO Linux e SO Solaris: /var/opt/drwcs/in caso di FreeBSD: /var/drwcs/
drwcsd.pub	chiave di cifratura pubblica	<ul style="list-style-type: none">in caso di SO Linux e SO Solaris: /opt/drwcs/Installer /opt/drwcs/webmin/installin caso di SO FreeBSD: /usr/local/drwcs/Installer /usr/local/drwcs/webmin/in stall

Quando viene rimosso il Server versione 10, i file di configurazione vengono salvati automaticamente nella directory predefinita per il backup:

File	Descrizione	Directory predefinita
agent.key (il nome può essere diverso)	chiave di licenza di Agent	/var/tmp/drwcs/
certificate.pem	certificato per SSL	
download.conf	impostazioni di rete per la generazione dei pacchetti d'installazione di Agent	
drwcsd.conf (il nome può essere diverso)	file di configurazione del Server	
drwcsd.pri	chiave di cifratura privata	
enterprise.key (il nome può essere diverso)	chiave di licenza di Server. Viene salvata soltanto se era presente dopo l'aggiornamento dalle versioni precedenti. Quando viene installato il nuovo Server 10, è assente.	
frontdoor.conf	file di configurazione per l'utility di diagnostica remota di Server	
private-key.pem	chiave privata RSA	
webmin.conf	file di configurazione del Pannello di controllo	
common.conf	file di configurazione (per alcuni SO della famiglia UNIX)	
local.conf	impostazioni del log di Server	
dbexport.gz	esportazione del database	



File	Descrizione	Directory predefinita
drwcsd.pub	chiave di cifratura pubblica	

In caso [dell'aggiornamento automatico](#) per SO **Linux** e SO **Solaris**, vengono anche salvati i seguenti file:

In caso del Server versione 6:

File	Descrizione	Directory predefinita
auth-ldap.xml	file di configurazione per l'autenticazione esterna degli amministratori attraverso LDAP	/var/opt/drwcs/etc
auth-radius.xml	file di configurazione per l'autenticazione esterna degli amministratori attraverso RADIUS	

In caso del Server versione 10:

File	Descrizione	Directory predefinita
auth-ldap.xml	file di configurazione per l'autenticazione esterna degli amministratori attraverso LDAP	/var/tmp/drwcs/
auth-pam.xml	file di configurazione per l'autenticazione esterna degli amministratori attraverso PAM	
auth-radius.xml	file di configurazione per l'autenticazione esterna degli amministratori attraverso RADIUS	



Se si prevede di utilizzare i file di configurazione dalla versione precedente di Server, notare:

1. La chiave di licenza di Server non viene più utilizzata (v. p. [Capitolo 2: Concessione delle licenze](#)).
2. Il database incorporato viene aggiornato e il file di configurazione di Server viene convertito attraverso l'installer. Questi file non possono essere sostituiti con le copie automaticamente salvate quando si passa al Server versione 10.

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 il Server.



2. Esportare il database nel file:

- In caso di SO FreeBSD:
/usr/local/etc/rc.d/drwcsd.sh exportdb /var/drwcs/etc/esbase.es
- In caso di SO Linux:
/etc/init.d/drwcsd exportdb /var/opt/drwcs/etc/esbase.es
- In caso di SO Solaris:
/etc/init.d/drwcsd exportdb /var/drwcs/etc/esbase.es

In caso dei Server 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 è disponibile una copia di backup del database, non sarà possibile ripristinare il Server in caso di circostanze di emergenza.

Aggiornamento automatico

Quando il Server viene aggiornato dalla versione 6 alla versione 10 per SO **Linux** e SO **Solaris**, invece di rimuovere la versione vecchia di Server e di installare quella nuova è possibile eseguire l'aggiornamento di pacchetto automatico di Server. Per farlo, avviare l'installazione del relativo pacchetto di Server.

In questo caso, tutti i [file](#) salvati in automatico verranno convertiti automaticamente e messi nelle directory richieste.

Aggiornamento manuale

Per aggiornare il Server Dr.Web in caso dell'utilizzo del database incorporato:

1. Arrestare il Server.
2. Se si vogliono utilizzare in seguito alcuni file (oltre ai [file](#) che verranno salvati in automatico nel corso della rimozione del Server al passo **4**), creare i backup di questi file manualmente, per esempio template dei report ecc.
3. Cancellare tutti i contenuti del repository.
4. Rimuovere il software Server (v. p. [Rimozione di Server Dr.Web per SO della famiglia UNIX®](#)). Il software offre automaticamente di salvare copie di backup dei file. Per questo fine, basta inserire il percorso per il salvataggio o accettare il percorso proposto di default.
5. Installare il Server Dr.Web versione 10 secondo la procedura di installazione standard (v. p. [Installazione di Server Dr.Web per SO della famiglia UNIX®](#)) sulla base della copia di backup creata al passaggio **4**). Tutti i file di configurazione salvati e il database incorporato verranno convertiti automaticamente per essere utilizzabili dal Server versione 10. Senza la conversione automatica, non è possibile utilizzare i database e alcuni file di configurazione del Server delle versioni precedenti.



Se alcuni file sono stati salvati manualmente, metterli nelle stesse directory in cui si trovavano nella versione precedente di Server.



Per tutti i file salvati dalla versione precedente del Server (v. passo 6), è necessario impostare come il proprietario dei file l'utente selezionato nel corso dell'installazione della nuova versione di Server (di default è **drwcs**).

6. Avviare il Server.
7. Configurare l'aggiornamento del repository ed aggiornarlo completamente.
8. Riavviare il Server.

Per aggiornare il Server Dr.Web in caso dell'utilizzo del database esterno:

1. Arrestare il Server.
2. Se si vogliono utilizzare in seguito alcuni file (oltre ai [file](#) che verranno salvati in automatico nel corso della rimozione del Server al passo 4), creare i backup di questi file manualmente, per esempio template dei report ecc.
3. Cancellare tutti i contenuti del repository.
4. Rimuovere il software Server (v. p. [Rimozione di Server Dr.Web per SO della famiglia UNIX®](#)). Il software offre automaticamente di salvare copie di backup dei file. Per questo fine, basta inserire il percorso per il salvataggio o accettare il percorso proposto di default.
5. Installare il Server Dr.Web versione 10 secondo la procedura di installazione standard (v. p. [Server Dr.Web per SO della famiglia UNIX®](#)).
6. Mettere i file salvati automaticamente (v. [sopra](#)):

- in caso di SO **Linux**:

```
chiave pub: /opt/drwcs/Installer/ e in /opt/drwcs/webmin/install  
il resto: /var/opt/drwcs/etc
```

- in caso di SO **FreeBSD**:

```
chiave pub: /usr/local/drwcs/Installer/ e in /usr/local/drwcs/webmin/install  
il resto: /var/drwcs/etc
```

- in caso di SO **Solaris**:

```
chiave pub: /opt/drwcs/Installer/ e in /opt/drwcs/webmin/install  
il resto: /var/drwcs/etc
```

Se alcuni file sono stati salvati manualmente, metterli nelle stesse directory in cui si trovavano nella versione precedente di Server.



Per tutti i file salvati dalla versione precedente del Server (v. passo 6), è necessario impostare come il proprietario dei file l'utente selezionato nel corso dell'installazione della nuova versione di Server (di default è **drwcs**).

7. Eseguire i comandi:
 - in caso di SO **Linux** e SO **Solaris**:
`/etc/init.d/drwcsd upgradedb`



- in caso di SO **FreeBSD**:
`/usr/local/etc/rc.d/drwcsd.sh upgradedb`
8. Avviare il Server.
 9. Configurare l'aggiornamento del repository ed aggiornarlo completamente.
 10. Riavviare il Server.



Finito l'aggiornamento dei Server della rete antivirus, è necessario configurare nuovamente la cifratura e la compressione di dati per i Server associati (v. **Manuale dell'amministratore**, sezione [Configurazione delle relazioni tra i Server Dr.Web](#)).

6.3. Aggiornamento dell'estensione del Pannello di controllo della sicurezza Dr.Web

Per aggiornare l'estensione del Pannello di controllo della sicurezza Dr.Web (viene utilizzata dal Pannello di controllo), è necessario rimuovere manualmente la versione precedente dell'estensione e installare la nuova estensione del Pannello di controllo della sicurezza Dr.Web.

La rimozione dell'estensione viene descritta in p. [Rimozione di Server Dr.Web per SO Windows®](#) e in p. [Rimozione di Server Dr.Web per SO della famiglia UNIX®](#).

Il processo di installazione viene descritto in p. [Installazione dell'estensione del Pannello di controllo della sicurezza Dr.Web](#).

6.4. Aggiornamento di Agent Dr.Web

L'aggiornamento degli Agent in seguito all'aggiornamento del software Server è descritto per le seguenti varianti:

1. [Aggiornamento di Agent Dr.Web per le postazioni SO Windows®](#),
2. [Aggiornamento degli Agent Dr.Web per le postazioni SO Linux, Android e OS X](#).

6.4.1. Aggiornamento di Agent Dr.Web per le postazioni SO Windows®

Aggiornamento automatico

Per poter eseguire l'aggiornamento automatico, è necessario soddisfare le seguenti condizioni:

1. Gli Agent devono essere installati sui computer gestiti dai SO della famiglia Windows supportati per l'installazione degli Agent per Dr.Web Enterprise Security Suite versione 10 (v. documento **Allegati**, p. [Allegato A. Lista completa delle versioni supportate dei SO](#)).
2. Quando si esegue l'aggiornamento automatico, sono possibili le seguenti varianti delle azioni a seconda delle impostazioni di Server:



- a) L'aggiornamento automatico viene eseguito se per l'aggiornamento del Server sono state salvate le chiavi di crittografia e le impostazioni di rete del Server precedente.
- b) Durante un aggiornamento automatico è necessaria una configurazione manuale se per l'aggiornamento di Server sono state impostate nuove chiavi di crittografia e impostazioni di rete di Server.



Nel corso dell'aggiornamento automatico, prestare attenzione alle seguenti caratteristiche:

1. Dopo la rimozione di Agent, l'avviso di necessità di riavvio di postazione non viene visualizzato. L'amministratore deve lanciare manualmente il riavvio della postazione.
2. Nell'intervallo tra la rimozione della vecchia versione di Agent e l'installazione della nuova versione, le postazioni saranno senza protezione antivirus.
3. Dopo un aggiornamento di Agent senza il riavvio della postazione, il software antivirus funziona in un modo limitato. In tale caso non viene assicurata la completa protezione antivirus della postazione. È necessario che l'utente riavvii la postazione a richiesta dell'Agent.

L'aggiornamento automatico di Agent viene eseguito secondo il seguente schema:

1. Quando viene lanciato l'aggiornamento, viene rimossa la vecchia versione di Agent.
2. La postazione viene riavviata manualmente.
3. Viene installata una nuova versione di Agent. Per farlo, viene creato automaticamente un task nel calendario del Server.
4. Dopo la fine dell'aggiornamento di Agent, la postazione si connette automaticamente al Server. Nella sezione **Stato** del Pannello di controllo per la postazione aggiornata verrà visualizzata una notifica di necessità di riavvio. È necessario riavviare la postazione.

L'aggiornamento automatico di Agent con una configurazione manuale viene eseguito secondo il seguente schema:

1. Modificare manualmente le impostazioni di connessione al nuovo Server e sostituire la chiave di cifratura pubblica sulla postazione.
2. Dopo la modifica delle impostazioni sulla postazione e la connessione della postazione al Server, viene avviato il processo di aggiornamento dell'Agent.
3. Quando viene lanciato l'aggiornamento, viene rimossa la vecchia versione di Agent.
4. La postazione viene riavviata manualmente.
5. Viene installata una nuova versione di Agent. Per farlo, viene creato automaticamente un task nel calendario del Server.
6. Dopo la fine dell'aggiornamento di Agent, la postazione si connette automaticamente al Server. Nella sezione **Stato** del Pannello di controllo per la postazione aggiornata verrà visualizzata una notifica di necessità di riavvio. È necessario riavviare la postazione.



Aggiornamento manuale

Se l'installazione di nuova versione di Agent durante un aggiornamento automatico non è riuscita per qualche ragione, non ci saranno altri tentativi di installazione. Il software antivirus non sarà installato sulla postazione e nel Pannello di controllo tale postazione verrà visualizzata come disattivata.

In questo caso, è necessario [installare l'Agent](#) manualmente. Dopo l'installazione del nuovo Agent, sarà necessario unire la postazione vecchia e quella nuova nel Pannello di controllo nella lista gerarchica della rete antivirus.

L'aggiornamento non è supportato

Se gli Agent sono installati sulle postazioni con i sistemi operativi non supportati per l'installazione di Agent per Dr.Web Enterprise Security Suite versione 10, non verranno eseguite alcune azioni di aggiornamento.

Gli Agent installati sotto i SO non supportati non potranno ricevere gli aggiornamenti (neanche gli aggiornamenti dei database dei virus) dal nuovo Server. Se è richiesta la presenza degli Agent sotto i SO non supportati, è necessario lasciare nella rete antivirus i Server delle versioni precedenti a cui sono connessi questi Agent. In tale caso i Server versione 6 e i Server versione 10 devono ricevere gli aggiornamenti in modo indipendente.



Le raccomandazioni su aggiornamento di Agent installati sulle postazioni che svolgono funzionalità LAN critiche sono riportate nel documento **Allegati**, sezione [Aggiornamento degli Agent sui server LAN](#).

6.4.2. Aggiornamento degli Agent Dr.Web per le postazioni SO Linux, Android e OS X

Gli Agent installati sulle postazioni SO famiglia Linux, Android e OS X si connettono al Server versione 10 con il pieno supporto del processo di aggiornamento nei seguenti casi:

1. Gli Agent devono essere installati sui computer gestiti dai SO supportati per l'installazione degli Agent per Dr.Web Enterprise Security Suite versione 10 (v. documento **Allegati**, p. [Allegato A. Lista completa delle versioni supportate dei SO](#)).
2. Sulle postazioni devono essere impostate le chiavi di cifratura e le impostazioni di rete del Server aggiornato.



6.5. Aggiornamento del Server proxy

Aggiornamento del server proxy per SO Windows

L'aggiornamento automatico del Server proxy non è supportato.

Quando l'installer viene avviato sul computer con il Server proxy installato:

- Se viene avviato un installer con lo stesso numero di bit del Server proxy installato, viene restituito un avviso di impossibilità di installazione.
- Se viene avviato un installer con il numero di bit diverso da quello del Server proxy installato, il Server proxy viene installato in una directory diversa da quella della versione già installata.



Se sullo stesso computer sono installati due Server proxy e per il loro funzionamento è configurata la stessa porta, questo porterà alla mancata operatività di entrambi i Server proxy.

Per aggiornare il Server proxy:

1. Se sul computer con il Server proxy è installato un Agent con l'autoprotezione attiva, disattivare il componente di autoprotezione Dr.Web attraverso le impostazioni dell'Agent.
2. Rimuovere il Server proxy secondo la procedura standard (v. p. [Eliminazione del server proxy](#)).



Quando viene eliminato il Server proxy, viene eliminato il file di configurazione `drwcsd-proxy.xml` (v. documento **Allegati**, p. [Allegato G4](#)). Se necessario, salvare il file di configurazione manualmente prima di eliminare il Server proxy.

3. Installare la nuova versione di Server proxy secondo la procedura standard (v. p. [Installazione del Server proxy](#)).
4. Se necessario, sostituire il file di configurazione con quello salvato della versione precedente.
5. Se al passo 1 è stato disattivato il componente di autoprotezione Dr.Web, riattivare questo componente attraverso le impostazioni dell'Agent.

Aggiornamento del Server proxy per i SO della famiglia UNIX

Per aggiornare il Server proxy:

1. Quando viene aggiornato il Server proxy, viene eliminato il file di configurazione `drwcsd-proxy.xml` (v. documento **Allegati**, p. [Allegato G4](#)). Se necessario, salvare il file di configurazione manualmente prima di aggiornare il Server proxy.
2. Per avviare il processo di aggiornamento, eseguire il seguente comando:

```
sh ./<file_pacchetto> .run
```
3. Se necessario, sostituire il file di configurazione `drwcsd-proxy.xml` con il file salvato prima dell'inizio dell'aggiornamento.



Indice analitico

A

- account
 - postazione, creazione 51
- Active Directory
 - installazione di Agent 68
 - rimozione dell'Agent 82
- Agent
 - aggiornamento 94
 - installazione 46, 55
 - installazione locale 49
 - installazione, Active Directory 68
 - installazione, su remoto 59, 63, 68
 - rimozione, Active Directory 82
 - rimozione, in caso di SO Windows 80
- aggiornamento
 - Agent 94
 - estensione del Pannello di controllo della sicurezza Dr.Web 84, 94
 - server proxy 97
 - Server, per SO UNIX 88
 - Server, per SO Windows 84

C

- chiavi 26
 - demo 27
 - ottenimento 26
 - vedi anche registrazione 26
- chiavi demo 27
- concessione delle licenze 26
- contenuti del pacchetto 23

E

- estensione del Pannello di controllo della sicurezza Dr.Web
 - aggiornamento 94
 - aggiornamento, per SO Windows 84
 - installazione 44
 - rimozione, in caso del SO Windows 77
 - rimozione, in caso di SO UNIX 79

I

- icone
 - scanner di rete 65
- installazione
 - estensione del Pannello di controllo della sicurezza Dr.Web 44
 - NAP Validator 72

- pacchetto antivirus 46
- server proxy 73
- installazione di Agent 46
 - Active Directory 68
 - installer 55
 - localmente 49
 - pacchetto d'installazione 51
 - su remoto 59, 63, 68
- installazione di Server Dr.Web
 - pacchetto principale, per SO UNIX 42
 - pacchetto principale, per SO Windows 36
 - pacchetto supplementare 43
- installer
 - contenuti 48
 - installazione 55
 - rimozione, in caso di SO Windows 81
 - tipi 48

N

- NAP Validator
 - installazione 72

P

- pacchetto 23
- pacchetto antivirus
 - installazione 46, 68
 - rimozione 80
- pacchetto d'installazione
 - contenuti 48
 - installazione 51
 - rimozione, in caso di SO Windows 81
- pacchetto principale di Server Dr.Web
 - contenuti 23
 - installazione, per SO UNIX 42
 - installazione, per SO Windows 36
 - rimozione, in caso del SO Windows 77
 - rimozione, in caso di SO UNIX 77
- pacchetto supplementare di Server Dr.Web
 - contenuti 23
 - installazione 43
 - rimozione, in caso del SO Windows 77
 - rimozione, in caso di SO UNIX 78
- pagina di installazione 48
- postazione
 - creazione record 51



Indice analitico

R

- registrazione
 - di prodotto Dr.Web 26
- requisiti di sistema 18
- rete antivirus
 - programmazione 28
- rimozione
 - componenti 80
 - estensione del Pannello di controllo della sicurezza Dr.Web 77, 79
 - pacchetto antivirus 80
 - server proxy 83
- rimozione dell'Agent
 - Active Directory 82
- rimozione di Agent
 - in caso di SO Windows 80
 - installer, per SO Windows 81
 - pacchetto d'installazione, in caso di SO Windows 81
- rimozione di Server Dr.Web
 - pacchetto principale, per SO UNIX 77
 - pacchetto principale, per SO Windows 77
 - pacchetto supplementare, per SO UNIX 78
 - pacchetto supplementare, per SO Windows 77

S

- scanner di rete 63
- Server Dr.Web
 - aggiornamento, per SO UNIX 88
 - aggiornamento, per SO Windows 84
 - installazione, per SO UNIX 42
 - installazione, per SO Windows 36
 - rimozione, in caso del SO Windows 77
 - rimozione, in caso di SO UNIX 77
- server proxy
 - aggiornamento 97
 - installazione 73
 - rimozione 83

