Dr.WEB

Enterprise Security Suite

Guida all'installazione

Dr.Web Enterprise Security Suite
Versione 12.0
Guida all'installazione
20/02/2021

Doctor Web, Sede centrale in Russia

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

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

Telefono +7 (495) 789-45-87

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

Doctor Web

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

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

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

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

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

Sommario

Capitolo 1: Introduzione

1.1. Scopo del documento

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

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

1. **Guida all'installazione** (**drweb-12.0-esuite-install-manual-it.pdf**)

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

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

2. **Manuale dell'amministratore** (**drweb-12.0-esuite-admin-manual-it.pdf**)

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

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

3. **Allegati** (**drweb-12.0-esuite-appendices-it.pdf**)

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

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

Inoltre, sono forniti i seguenti Manuali:

1. **Guida rapida all’installazione della rete antivirus**

   Contiene brevi informazioni sull'installazione e sulla configurazione iniziale dei componenti della rete antivirus. Per informazioni dettagliate consultare la documentazione dell'amministratore.

2. **Manuale dell’amministratore per la gestione delle postazioni**

   Contiene informazioni sulla configurazione centralizzata dei componenti del software antivirus delle postazioni attraverso il Pannello di controllo della sicurezza Dr.Web da parte dell'amministratore della rete antivirus.

3. **Manuali dell'utente**

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

4. **Guida alle Web API**

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

5. **Guida al database del Server Dr.Web**

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

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

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

1.2. Segni convenzionali e abbreviazioni

Segni convenzionali

In questo manuale vengono utilizzati i seguenti simboli:

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

Abbreviazioni

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

- ACL — lista di controllo degli accessi (Access Control List),
- CDN — rete di distribuzione di contenuti (Content Delivery Network),
- DFS — file system distribuito (Distributed File System),
- DNS — sistema dei nomi a dominio (Domain Name System),
- FQDN — nome di dominio completo (Fully Qualified Domain Name),
- GUI — interfaccia utente grafica (Graphical User Interface), versione del programma con la GUI — una versione che utilizza gli strumenti della GUI,
- MIB — database delle informazioni di gestione (Management Information Base),
- MTU — dimensione massima di un pacchetto dati (Maximum Transmission Unit),
- NAP — Network Access Protection,
- TTL — tempo di vita pacchetto (Time To Live),

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

Capitolo 2: Dr.Web Enterprise Security Suite

2.1. Sul prodotto

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

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

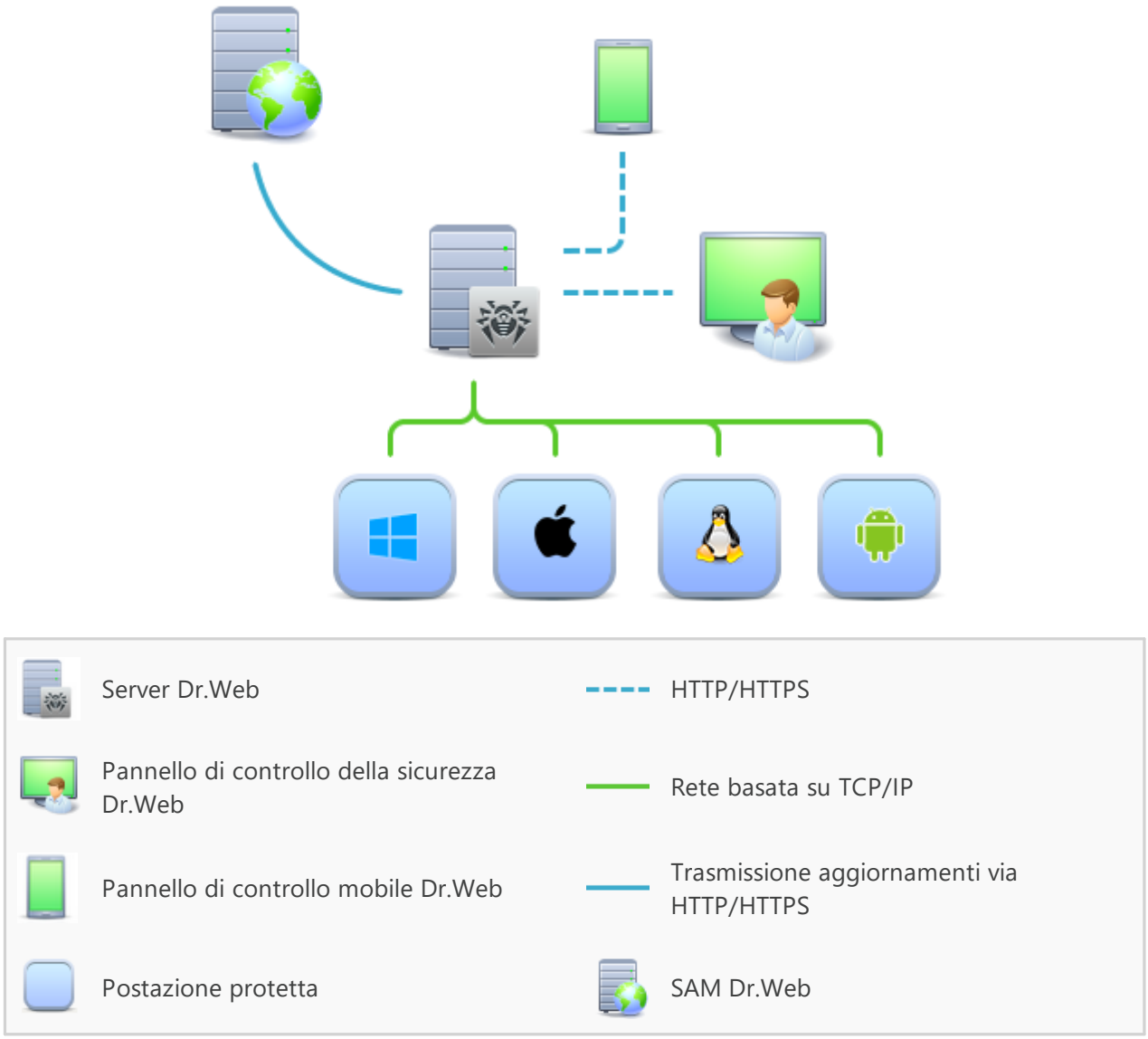

Immagine 1-1. Struttura logica della rete antivirus

La rete antivirus Dr.Web Enterprise Security Suite ha l'architettura *client-server*. I suoi componenti vengono installati sui computer e dispositivi mobili degli utenti e degli amministratori, nonché sui computer che svolgono le funzioni server della rete locale. I componenti della rete antivirus

scambiano le informazioni attraverso i protocolli di rete TCP/IP. Si può installare (e successivamente gestire) il software antivirus sulle postazioni protette sia via LAN che via internet.

Server di protezione centralizzata

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

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

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

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

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. Viene fornito il database SQLite3 incorporato direttamente nel Server di protezione centralizzata.

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

- MySQL,
- Oracle,
- PostgreSQL (incluso Postgres Pro),
- 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,
- Microsoft Edge,
- 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 informazioni dettagliate v. sezione Installazione di Agent Dr.Web).
- Gestione semplificata delle postazioni della rete antivirus attraverso il metodo di gruppi.
- Possibilità di gestire i pacchetti antivirus delle postazioni in modo centralizzato, in particolare, è possibile: rimuovere sia singoli componenti che l'intero Antivirus su postazioni SO Windows; configurare le impostazioni dei componenti dei pacchetti antivirus; assegnare i permessi per configurare e gestire i pacchetti antivirus dei computer protetti agli utenti di questi computer.
- Gestione centralizzata della scansione antivirus delle postazioni, in particolare è possibile: avviare la scansione antivirus su remoto sia secondo un calendario prestabilito che su una richiesta diretta dell'amministratore dal Pannello di controllo; configurare in modo centralizzato le impostazioni di scansione antivirus che vengono trasmesse sulle postazioni per il successivo avvio di una scansione locale con queste impostazioni.
- Ottenimento di informazioni statistiche sullo stato delle postazioni protette, di statistiche di virus, di informazioni sullo stato del software antivirus installato, sullo stato dei componenti antivirus in esecuzione, nonché di un elenco degli hardware e dei software della postazione protetta.
- Sistema flessibile dell'amministrazione del Server e della rete antivirus grazie alla possibilità di delimitare i privilegi per diversi amministratori, nonché la possibilità di connettere

amministratori attraverso i sistemi di autenticazione esterni, come Active Directory, LDAP, RADIUS, PAM.

- Gestione delle licenze di protezione antivirus delle postazioni con un sistema ramificato di assegnazione delle licenze a postazioni e gruppi di postazioni, nonché di trasferimento delle licenze tra diversi Server in caso di una configurazione della rete antivirus con diversi server.
- Un vasto set di impostazioni da utilizzare per configurare il Server e i suoi componenti separati, tra le altre cose, è possibile: impostare un calendario per la manutenzione del Server; connettere procedure personalizzate; configurare in modo flessibile l'aggiornamento da SAM di tutti i componenti della rete antivirus e la successiva distribuzione degli aggiornamenti alle postazioni; configurare l'avviso amministratore di eventi della rete antivirus tramite diversi metodi di consegna di messaggi; configurare le relazioni tra i server per una configurazione della 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 componente separato, viene fornito un Pannello di controllo mobile progettato per l'installazione e l'avvio su dispositivi mobili iOS e Android. I requisiti di base per l'applicazione sono riportati in p. Requisiti di sistema.

Il Pannello di controllo mobile viene connesso al Server sulla base delle credenziali dell'amministratore di rete antivirus, anche attraverso il protocollo criptato. 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;
   - aggiunzione 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 multipiattaforma del software permette di proteggere contro i virus i computer e dispositivi mobili gestiti dai seguenti sistemi operativi:

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

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

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

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

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

Postazioni SO Windows

Scansione antivirus

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

Monitoraggio di file

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

Monitoraggio di email

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

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

Monitoraggio del traffico web

Controllo di 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 applicazioni.

Quarantena

Isolamento di oggetti dannosi e sospetti in una directory speciale.

Auto-protezione

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

Protezione preventiva

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

Controllo delle applicazioni

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

Postazioni con SO della famiglia UNIX

Scansione antivirus

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

Scansione antivirus, gestione della quarantena

Componente per la verifica degli oggetti del file system e la gestione della quarantena. Accetta task di scansione file da altri componenti di Dr.Web per UNIX. Monitora le directory del file system in base al task, trasferisce i file al motore di scansione per la verifica. Esegue la rimozione dei file infetti, il loro spostamento in quarantena e il ripristino dalla quarantena, gestisce le directory di quarantena. Organizza e mantiene aggiornata una cache che memorizza informazioni sui file precedentemente scansionati e un registro delle minacce rilevate.

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

Controllo del traffico web

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

Monitoraggio di file per i sistemi GNU/Linux

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

Monitoraggio di file per le directory Samba

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

Monitoraggio di file NSS

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

Controllo delle connessioni di rete

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

Monitoraggio di email

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

1. Filtro per server di posta (Sendmail, Postfix, ecc.), che è connesso tramite l'interfaccia Milter, Spamd o Rspamd.
2. Proxy trasparente dei protocolli di posta (SMTP, POP3, IMAP). In questa modalità utilizza SpIDer Gate.

Postazioni macOS

Scansione antivirus

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

Monitoraggio di file

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

Monitoraggio del traffico web

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

Quarantena

Isolamento di oggetti dannosi e sospetti in una directory speciale.

Dispositivi mobili SO Android

Scansione antivirus

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

Monitoraggio di file

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

Filtro di chiamate ed SMS

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 applicazioni.

Aiuto nella risoluzione di problemi

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

Controllo dell'esecuzione di applicazioni

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

Assicurazione della comunicazione tra i componenti della rete antivirus

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

Server proxy Dr.Web

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

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

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

Compressione del traffico

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

Cifratura del traffico

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

Funzioni addizionali

NAP Validator

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

2.2. Requisiti di sistema

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

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

<table>
<tr><th>Numeri di porte</th><th>Protocolli</th><th>Connessioni</th><th>Scopo</th></tr>
<tr><td rowspan="3">2193</td><td>TCP</td><td>• in ingresso, in uscita per il Server e il Server proxy
• in uscita per Agent</td><td rowspan="2">Per la comunicazione dei componenti antivirus con il Server e per le connessioni tra i server.

Tra gli altri scopi, viene utilizzata dal Server proxy per stabilire una connessione con i client.</td></tr>
<tr><td>UDP</td><td>in ingresso, in uscita</td></tr>
<tr><td>Per il funzionamento dello Scanner di rete.</td></tr>
<tr><td rowspan="2">139, 445</td><td>TCP</td><td>• in uscita per il Server
• in ingresso per l'Agent</td><td rowspan="2">Per l'installazione remota di Agent Dr.Web</td></tr>
<tr><td>UDP</td><td>in ingresso, in uscita</td></tr>
<tr><td>9080</td><td>HTTP</td><td rowspan="3">• in ingresso per il Server
• in uscita per il computer su cui viene aperto il Pannello di controllo</td><td rowspan="2">Per il funzionamento del Pannello di controllo della sicurezza Dr.Web.</td></tr>
<tr><td>9081</td><td>HTTPS</td></tr>
<tr><td>10101</td><td>TCP</td><td>Per il funzionamento dell'utility di diagnostica remota del Server.</td></tr>
<tr><td>80</td><td>HTTP</td><td rowspan="2">in uscita</td><td rowspan="2">Per ricevere aggiornamenti da SAM.</td></tr>
<tr><td>443</td><td>HTTPS</td></tr>
</table>

Server Dr.Web

Componente	Requisiti
Processore	CPU con il supporto del set di istruzioni SSE2 e con la frequenza di clock di 1,3 GHz e superiori.

Componente	Requisiti
Memoria operativa	• Requisiti minimi: 1 GB. • Requisiti consigliati: 2 GB o più.
Spazio su disco rigido	• Almeno 50 GB per il software Server e uno spazio aggiuntivo per la memorizzazione dei file temporanei, per esempio, pacchetti di installazione Agent individuali (circa 17 MB ognuno) nella sottodirectory `var\installers-cache` della directory di installazione Server Dr.Web. • Fino a 5 GB per il database. • A seconda del percorso di installazione del Server, sul disco di sistema in SO Windows o in `/var/tmp` nei sistemi operativi della famiglia UNIX (o in un'altra directory per i file temporanei, se è stata ridefinita): ▫ per l'installazione del Server, sono necessari almeno 4,3 GB per l'avvio dell'installer e per l'estrazione dei file temporanei; ▫ per il funzionamento del Server, è necessario uno spazio libero sul disco di sistema per la memorizzazione dei file temporanei e di lavoro, a seconda delle dimensioni del database e delle impostazioni del repository.
Sistema operativo	• Windows (la lista completa dei sistemi operativi supportati è riportata nel documento **Allegati**, in Allegato A). • Linux, nel caso di presenza della libreria `glibc` 2.13 o versioni successive; incluso ALT Linux 5.0 o versioni successive, Astra Linux Special Edition 1.3 o versioni successive. • FreeBSD 10.3 o versioni successive.
Supporto di ambienti virtuali e cloud	È supportato il funzionamento sui sistemi operativi che soddisfano i requisiti elencati sopra, negli ambienti virtuali e cloud, tra cui: • VMware; • Hyper-V; • Xen; • KVM.
Altro	In aggiunta sotto SO FreeBSD è necessaria la disponibilità della libreria `compat-10x`. Per l'utilizzo del database Oracle è necessaria la disponibilità della libreria `Linux kernel AIO access library` (`libaio`).

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

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

Server proxy Dr.Web

Componente	Requisito
Processore	CPU con il supporto del set di istruzioni SSE2 e con la frequenza di clock di 1,3 GHz e superiori.
Memoria operativa	Almeno 1 GB.
Spazio su disco rigido	Almeno 1 GB.
Sistema operativo	• Windows (la lista completa dei sistemi operativi supportati è riportata nel documento **Allegati**, in Allegato A). • Linux, nel caso di presenza della libreria `glibc` 2.13 o versioni successive; incluso ALT Linux 5.0 o versioni successive, Astra Linux Special Edition 1.3 o versioni successive. • FreeBSD 10.3 o versioni successive.

Pannello di controllo della sicurezza Dr.Web

a) Browser web:

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

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**.
- Per il corretto utilizzo del Pannello di controllo attraverso il browser Windows Internet Explorer tramite il protocollo sicuro `https` è necessario installare tutti gli ultimi aggiornamenti del browser.
- L'utilizzo del Pannello di controllo attraverso il browser Windows Internet Explorer in modalità compatibilità non è supportato.

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

Pannello di controllo mobile Dr.Web

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

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

NAP Validator

Per il server:

- SO Windows Server 2008.

Per gli agent:

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

Agent Dr.Web e il pacchetto antivirus

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

- SO Windows:

Componente	Requisito
Processore	CPU con la frequenza di clock di 1 GHz e superiori.
Memoria operativa libera	Almeno 512 MB.
Spazio libero su disco rigido	Almeno 1 GB per i file eseguibili e uno spazio aggiuntivo per i log di funzionamento e per i file temporanei.
Altro	1. Per il corretto funzionamento della guida contestuale di **Agent Dr.Web per Windows** è necessaria la presenza di Windows Internet Explorer 6.0 o versioni successive. 2. Per il plugin Dr.Web per Microsoft Outlook deve essere installato il client Microsoft Outlook di Microsoft Office: • Outlook 2000; • Outlook 2002; • Outlook 2003; • Outlook 2007; • Outlook 2010 SP2; • Outlook 2013; • Outlook 2016; • Outlook 2019.

- SO della famiglia Linux:

Componente	Requisito
Processore	Processori con l'architettura e il set di istruzioni • Intel/AMD: 32 bit (IA-32, x86) e 64 bit (x86-64, x64, amd64); • ARM64.
Memoria operativa libera	Almeno 512 MB (consigliato 1 GB o più).
Spazio libero su disco rigido	Almeno 500 MB di spazio libero sul volume su cui sono situate le directory di Antivirus.

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

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

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

Sulle postazioni di una rete antivirus gestita tramite Dr.Web Enterprise Security Suite non deve essere utilizzato nessun altro software antivirus (incluso il software di altre versioni dei programmi antivirus Dr.Web).

2.3. Contenuto del pacchetto

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

1. In caso di SO della famiglia UNIX:
   - `drweb-<versione_pacchetto>-<build>-esuite-server-<versione_SO>.tar.gz.run`

     Pacchetto di Server Dr.Web*
   - `drweb-reloader-<sistema_operativo>-<numero_di_bit>`

     Versione console di Loader di repository Dr.Web.
2. In caso di SO Windows:
   - `drweb-<versione_pacchetto>-<build>-esuite-server-<versione_SO>.exe`

     Pacchetto di Server Dr.Web*
   - `drweb-<versione_pacchetto>-<build>-esuite-agent-full-windows.exe`

     Installer completo di Agent Dr.Web.
   - `drweb-reloader-windows-<numero_di_bit>.exe`

     Versione console di Loader di repository Dr.Web.
   - `drweb-reloader-gui-windows-<numero_di_bit>.exe`

     Versione grafica di Loader di repository Dr.Web.

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

- software di Server Dr.Web per il SO corrispondente,
- dati di sicurezza di Server Dr.Web,
- software di Pannello di controllo della sicurezza Dr.Web,
- software di Agent Dr.Web e dei pacchetti antivirus per le postazioni con SO Windows,

- modulo di aggiornamento di Agent Dr.Web per Windows,
- Antispam di Dr.Web per Windows,
- database dei virus, database dei filtri incorporati dei componenti antivirus e di Antispam di Dr.Web per Windows,
- documentazione,
- notizie di Doctor Web.

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

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

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

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

Capitolo 3: Concessione delle licenze

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

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

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

File della chiave di licenza

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

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

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

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

- Il file della chiave di licenza fa parte del set antivirus Dr.Web Enterprise Security Suite acquistato, se è stato incluso nel pacchetto software all'assemblaggio. Tuttavia, di regola, vengono forniti solamente i numeri di serie.
- Il file della chiave di licenza viene inviato agli utenti via email dopo la registrazione del numero di serie sul sito web dell'azienda Doctor Web sull'indirizzo https://products.drweb.com/register/v4/, se nessun altro indirizzo è indicato nella scheda di registrazione allegata al prodotto. Andare al sito indicato, compilare il modulo con informazioni sull'acquirente e inserire nel campo indicato il numero di serie di registrazione (si trova nella scheda di registrazione). Un archivio con i file della chiave verrà inviato sull'indirizzo email indicato dall'utente. È inoltre possibile scaricare i file della chiave direttamente dal sito indicato.
- Il file della chiave di licenza può essere fornito su un supporto separato.

Si consiglia di conservare il file della chiave di licenza fino alla scadenza della sua validità e di utilizzarlo per la reinstallazione o per il ripristino dei componenti del programma. In caso di perdita del file della chiave di licenza, si può rifare la procedura di registrazione sul sito indicato e ottenere

nuovamente un file della chiave di licenza. A questo scopo occorre indicare lo stesso numero di serie di registrazione e le stesse informazioni sull'acquirente che sono state indicate per la prima registrazione; soltanto l'indirizzo email può essere diverso. In questo caso il file della chiave di licenza verrà inviato sul nuovo indirizzo email.

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

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

L'utilizzo dei file della chiave di licenza nel processo di installazione del programma è descritto in p. Installazione di Server Dr.Web.

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

Capitolo 4: Introduzione all'uso

4.1. Creazione della rete antivirus

Brevi istruzioni per l'installazione di una rete antivirus:

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

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

   

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

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

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

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

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

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

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

Gli Agent Dr.Web per le postazioni SO Android, SO Linux, macOS possono inoltre essere installati dai pacchetti dei prodotti standalone e successivamente connessi al Server Dr.Web centralizzato. Le impostazioni degli Agent sono descritte nei relativi **Manuali utente**.

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

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

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

4. Se necessario, installare e configurare il Server proxy. La descrizione viene riportata in p. Installazione del Server proxy.

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

   

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

   Il Pannello di controllo è disponibile sull'indirizzo:

   `http://<Indirizzo_Server>:9080`

   o

   `https://<Indirizzo_Server>:9081`

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

   Nella finestra di dialogo di richiesta di autenticazione inserire le credenziali dell'amministratore. Le credenziali dell'amministratore con i permessi completi di default:

   - Nome utente — **admin**.
   - La password:
     - in caso di SO Windows — la password che è stata impostata quando veniva installato il Server.
     - in caso di SO della famiglia UNIX — la password che è stata creata automaticamente durante l'installazione di Server (vedi inoltre p. Installazione di Server Dr.Web per SO della famiglia UNIX).

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

6. Effettuare la configurazione iniziale di Server (le impostazioni di Server vengono descritte dettagliatamente in **Manuale dell'amministratore**, in Capitolo 9: Configurazione di Server Dr.Web):

a. Nella sezione Gestione licenze aggiungere uno o più chiavi di licenza e distribuirle ai gruppi corrispondenti, in particolare, al gruppo **Everyone**. Il passaggio è obbligatorio se durante l'installazione di Server la chiave di licenza non è stata impostata.

b. Nella sezione Configurazione generale del repository impostare quali componenti della rete antivirus verranno aggiornati da SAM Dr.Web. Se la rete antivirus includerà postazioni protette con SO Android, SO Linux, macOS, è necessario caricare i **Prodotti aziendali Dr.Web**.

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

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

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

c. Sulla pagina **Amministrazione** → **Server Dr.Web** sono riportate informazioni sulla versione di Server. Se è disponibile una nuova versione, aggiornare Server, come descritto in **Manuale dell'amministratore**, p. Aggiornamento di Server Dr.Web e ripristino da copia di backup.

d. Se necessario, configurare Connessioni di rete per modificare le impostazioni di rete di default utilizzate per l'interazione di tutti i componenti della rete antivirus.

e. Se necessario, configurare la lista degli amministratori del Server. Inoltre, è disponibile l'autenticazione esterna degli amministratori. Per maggiori informazioni vedi **Manuale dell'amministratore**, Capitolo 6: Amministratori della rete antivirus.

f. Prima di iniziare ad utilizzare il software antivirus, è consigliabile modificare l'impostazione della directory per il backup dei dati critici del Server (v. **Manuale dell'amministratore**, p. Configurazione del calendario di Server Dr.Web). È preferibile collocare questa directory su un altro disco locale per ridurre la probabilità di una perdita simultanea dei file del software Server e della copia di backup.

7. Configurare il software antivirus per postazioni (la configurazione dei gruppi e delle postazioni viene descritta dettagliatamente in **Manuale dell'amministratore**, in Capitolo 7 e Capitolo 8):

   a. Se necessario, creare gruppi di postazioni personalizzati.

   b. Configurare il gruppo **Everyone** e i gruppi personalizzati creati. In particolare, configurare la sezione dei componenti da installare.

8. Installare il software Agent Dr.Web sulle postazioni.

   Nella sezione File di installazione controllare l'elenco dei file disponibili per l'installazione di Agent. Selezionare la variante di installazione adatta, basandosi sul sistema operativo della

postazione, sulla possibilità di installazione su remoto, sulla variante di configurazione delle impostazioni di Server nel corso dell'installazione di Agent ecc. Per esempio:

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

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

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

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

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

4.2. Configurazione delle connessioni di rete

Informazioni generali

Al Server Dr.Web si connettono i seguenti client:

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

Una connessione viene sempre stabilita da parte del client.

Sono 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 diversamente impostato), i client utilizzano 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 configuralo manualmente in modo opportuno.

4.2.1. 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`.

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

Per il funzionamento corretto di tutto il sistema Dr.Web Enterprise Security Suite, è sufficiente che il Server "sia in ascolto" su 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 /server` <*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 cercando Server Dr.Web e tenta di installare l'Agent dal primo Server trovato 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.

4.2.2. 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 (analogamente alle connessioni dirette): `udp/231.0.0.1:2193`.

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

4.2.3. 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. https://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`.

4.3. Connessione sicura

4.3.1. Cifratura e compressione del traffico dati

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

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

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

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

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

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

Criterio di coordinazione delle impostazioni

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

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

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

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

Impostazioni del client	Impostazioni del Server		
	Sì	**Possibile**	**No**
Sì	+	+	Errore
Possibile	+	+	–
No	Errore	–	–

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

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

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

Connessione attraverso Server proxy Dr.Web

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

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

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

- Se il Server e il client supportano la cifratura TLS, utilizzata nella versione 12.0, allora basta che siano soddisfatte le condizioni descritte sopra per stabilire una connessione operativa.
- Se uno dei componenti non supporta la cifratura TLS: sul Server e/o sul client è installata la versione 10 e precedenti con la cifratura GOST, viene eseguita una verifica addizionale secondo la tabella 4-2.

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

Impostazioni della connessione con il client	Impostazioni della connessione con il Server			
	Nulla	**Compressione**	**Cifratura**	**Tutto**
Nulla	Modalità normale	Modalità normale	Errore	Errore
Compressione	Modalità normale	Modalità normale	Errore	Errore
Cifratura	Errore	Errore	Modalità trasparente	Errore
Tutto	Errore	Errore	Errore	Modalità trasparente

Segni convenzionali

Impostazioni delle connessioni con il Server e con il client	
Nulla	Non è supportata né la compressione né la cifratura.
Compressione	È supportata solo la compressione.
Cifratura	È supportata solo la cifratura.
Tutto	Sono supportate sia la compressione che la cifratura.
Risultato della connessione	
Modalità normale	La connessione stabilita implica il funzionamento in modalità normale — con l'elaborazione dei comandi e la memorizzazione nella cache.
Modalità trasparente	La connessione stabilita implica il funzionamento in modalità trasparente — senza l'elaborazione dei comandi e la memorizzazione nella cache. Viene selezionata la versione minima del protocollo di cifratura: se uno dei componenti (Server o Agent) è della versione 11 e l'altro è della versione 10, viene impostata la cifratura utilizzata nella versione 10.
Errore	La connessione del Server proxy con il Server e con il client verrà interrotta.

Pertanto, se il Server e l'Agent sono di diverse versioni: uno della versione 11, e l'altro della versione 10 e precedenti, alle connessioni stabilite attraverso il Server proxy si applicano le seguenti limitazioni:

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

Impostazioni di cifratura e di compressione sul Server Dr.Web

Per definire le impostazioni di compressione e di cifratura del Server

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

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

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

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

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

1. Aprire il Pannello di controllo per il Server che è il server di gestione per il Server proxy.
2. Selezionare la voce **Rete antivirus** nel menu principale del Pannello di controllo, nella finestra che si è aperta nella lista gerarchica fare clic sul nome del Server proxy di cui si vuole modificare le impostazioni o sul nome del suo gruppo primario se le impostazioni del Server proxy sono ereditate.
3. Nel menu di gestione che si è aperto selezionare la voce **Server proxy Dr.Web**. Si aprirà la sezione delle impostazioni.
4. Passare alla scheda **Ascolto**.
5. Nella sezione **Parametri di connessione con i client** nella lista a cascata **Crittografia** e **Compressione** selezionare la modalità di cifratura e di compressione del traffico per i canali tra il Server proxy e i relativi client: Agent ed installer di Agent.
6. Nella sezione **Parametri di connessione con i Server Dr.Web** viene impostata una lista di Server su cui verrà reindirizzato il traffico. Selezionare nella lista il Server richiesto e premere il pulsante sulla barra degli strumenti di questa sezione per modificare i parametri di connessione con il Server Dr.Web selezionato. Nella finestra che si è aperta, nelle liste a cascata **Crittografia** e **Compressione** selezionare la modalità di cifratura e di compressione del traffico per il canale tra il Server proxy e il Server selezionato.
7. Per salvare le impostazioni definite, premere il pulsante **Salva**.

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

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

Il file di configurazione `drwcsd-proxy.conf` è descritto nel documento **Allegati**, nella sezione Allegato G4.

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

- Eseguire il seguente comando:

In caso di SO Linux:

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

In caso di SO FreeBSD:

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

Impostazioni di cifratura e di compressione sulle postazioni

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

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

Agent Dr.Web per Windows

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

- In caso di installazione in remoto dal Pannello di controllo la modalità di cifratura e compressione viene definita direttamente nelle impostazioni della sezione **Installazione via rete**.
- In caso di installazione locale l'installer grafico non fornisce la possibilità di modificare la modalità di cifratura e di compressione, tuttavia, queste impostazioni possono essere definite tramite le opzioni della riga di comando all'avvio dell'installer (vedi documento **Allegati**, p. H1. Installer di rete).

Dopo l'installazione di Agent la possibilità di modificare le impostazioni di cifratura e compressione localmente sulla postazione non viene fornita. Di default è impostata la modalità **Possibile** (se durante l'installazione non è stato impostato un altro valore), cioè l'utilizzo della cifratura e della

compressione dipende dalle impostazioni sul lato Server. Tuttavia, le impostazioni sul lato Agent possono essere modificate attraverso il Pannello di controllo (vedi sopra).

Antivirus Dr.Web per Android

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

Antivirus Dr.Web per Linux

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

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

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

Antivirus Dr.Web per macOS

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

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

4.3.2. Strumenti per la connessione sicura

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

1. **Chiave di cifratura privata di Server** `drwcsd.pri`**.**

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

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

   La chiave privata viene utilizzata nei seguenti casi:

   a) Creazione delle chiavi pubbliche e dei certificati.

La chiave di cifratura pubblica e il certificato vengono creati automaticamente dalla chiave privata durante l'installazione di Server. In tale caso è possibile sia creare una nuova chiave privata che utilizzarne una esistente (per esempio, quella dall'installazione precedente di Server). Inoltre, le chiavi di cifratura e i certificati possono essere creati in qualsiasi momento tramite l'utility di server `drwsign` (vedi documento **Allegati**, p. H7.1. Utility di generazione delle chiavi e dei certificati digitali).

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

b) Autenticazione di Server.

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

Il Server effettua la firma digitale di un messaggio tramite la chiave privata e invia il messaggio al client. Il client verifica la firma del messaggio ricevuto tramite il certificato.

c) Decifratura dei dati.

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

2. **Chiave di cifratura pubblica di Server** `drwcsd.pub`**.**

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

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

3. **Certificato di Server** `drwcsd-certificate.pem`**.**

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

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

Il certificato viene utilizzato nei seguenti casi:

a) Autenticazione di Server.

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

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

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

b) *Cifratura dei dati*.

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

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

d) *Autenticazione di Server proxy*.

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

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

4. **Chiave privata di web server.**

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

5. **Certificato di web server.**

È disponibile per tutti i componenti della rete antivirus.

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

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

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

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

4.3.3. Connessione dei client al Server Dr.Web

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

Al Server Dr.Web possono connettersi i seguenti client:

- **Agent Dr.Web.**

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

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

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

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

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

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

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

  Dopo l'installazione di Agent, i dati del certificato vengono iscritti al registro, e il file di certificato stesso in seguito non viene utilizzato.

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

- **Server Dr.Web adiacenti.**

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

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

- **Server proxy Dr.Web.**

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

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

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

Non è consigliato installare un Agent fornito con il Server versione 11 connettendolo a un Server versione 10 e viceversa.

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

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

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

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

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

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

   Per maggiori informazioni vedi le sezioni della Installazione di Server Dr.Web per SO Windows e Utilizzo del protocollo SRV.

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

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

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

   Per maggiori informazioni vedi la sezione del **Manuale dell'amministratore** Configurazione del calendario del Server Dr.Web.

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

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

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

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

   Per maggiori informazioni vedi la sezione del **Manuale dell'amministratore** Autenticazione di amministratori.

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

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

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

   b) Configurare i criteri di Active Directory corrispondenti per l'installazione automatica del pacchetto sulle postazioni nel dominio.

   Per maggiori informazioni vedi la sezione della Installazione di Agent Dr.Web con utilizzo di Active Directory.

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

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

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

   Per maggiori informazioni vedi la sezione del **Manuale dell'amministratore** Scanner di rete.

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

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

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

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

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

5.1. Installazione di Server Dr.Web

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

L'avanzamento del processo di installazione di Server Dr.Web dipende dalla versione 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.

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

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

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

5.1.1. Installazione di Server Dr.Web per SO Windows

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

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

Il file del pacchetto e gli altri file richiesti durante l'installazione del programma devono essere situati su dischi locali del computer su cui viene installato il software Server. 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 (vedi **Manuale dell'amministratore**, p. Aggiornamento del repository di Server Dr.Web manualmente).

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 per l'utilizzo di DBMS. Parametri dei driver di DBMS).

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

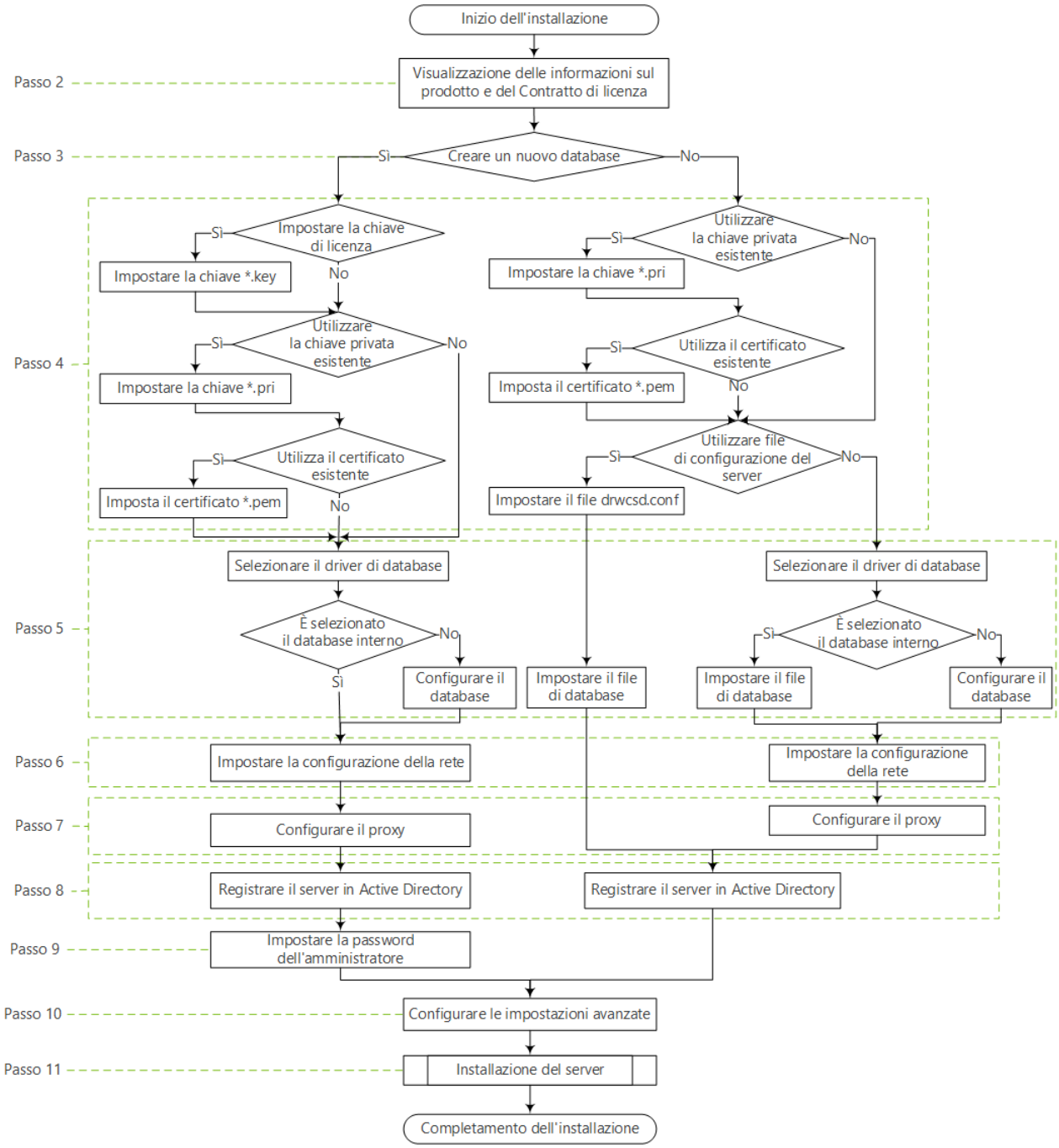

Immagine 5-1. Schema a blocchi del processo di installazione di Server Dr.Web (Premere un blocco dello schema per passare alla descrizione)

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

1. Avviare il file del pacchetto.

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

2. Si apre una finestra con 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 (vedi passaggio **5**).
4. Nella finestra successiva configurare le impostazioni del database.
   a) Se nel passaggio **3** è stata 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 dall'installazione precedente di Server.
  - Alla prima installazione del Server togliere il flag **Utilizza la chiave di cifratura privata esistente**. Le nuove chiavi di cifratura e il certificato verranno generati automaticamente durante il 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. Verranno creati automaticamente un file con la chiave pubblica (il contenuto della chiave pubblica corrisponderanno al contenuto della chiave pubblica precedente) e un certificato (ogni volta quando un certificato viene generato da una stessa chiave privata, è un nuovo certificato).
  - Se si installa il Server per una rete antivirus esistente e si utilizza una chiave di cifratura privata esistente, spuntare il flag **Utilizza certificato esistente** per impostare il file di certificato precedentemente utilizzato. Questo consentirà agli Agent già installati di connettersi al nuovo Server in quanto i client connessi al Server sono associati a un certificato specifico (ogni volta quando un certificato viene generato da una stessa chiave privata, è un nuovo certificato). Nel caso contrario, dopo l'installazione sarà necessario copiare il nuovo certificato su tutte le postazioni su cui gli Agent Dr.Web erano precedentemente installati.
  - Se si verifica un errore durante l'estrazione della chiave pubblica, impostare il percorso del file con la relativa chiave pubblica manualmente nel campo che si è aperto **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 passaggio **3** è stata 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 dall'installazione precedente di Server.
  - Alla prima installazione del Server togliere il flag **Utilizza la chiave di cifratura privata esistente**. Le nuove chiavi di cifratura e il certificato verranno generati automaticamente durante il 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. Verranno creati automaticamente un file con la chiave pubblica (il contenuto della chiave pubblica corrisponderanno al contenuto della chiave pubblica precedente) e un certificato (ogni volta quando un certificato viene generato da una stessa chiave privata, è un nuovo certificato).
  - Se si installa il Server per una rete antivirus esistente e si utilizza una chiave di cifratura privata esistente, spuntare il flag **Utilizza certificato esistente** per impostare il file di certificato precedentemente utilizzato. Questo consentirà agli Agent già installati di connettersi al nuovo Server in quanto i client connessi al Server sono associati a un certificato specifico (ogni volta quando un certificato viene generato da una stessa chiave privata, è un nuovo certificato). Nel caso contrario, dopo l'installazione sarà necessario copiare il nuovo certificato su tutte le postazioni su cui gli Agent Dr.Web erano precedentemente installati.
  - Se si verifica un errore durante l'estrazione della chiave pubblica, impostare il percorso del file con la relativa chiave pubblica manualmente nel campo che si è aperto **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 passaggio **3** e dalla disponibilità del file di configurazione di Server, impostato nel passaggio **4**:
   - Se nel passaggio **3** è stata selezionata l'opzione **Crea un nuovo database** o per l'opzione **Usa il database esistente** nel passaggio **4** non è stato impostato il percorso del file di configurazione di Server, selezionare il driver da utilizzare. In particolare:

- **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 addizionali.
- 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 dettagli negli allegati (v. documento **Allegati**, p. Allegato B. Impostazioni necessarie per l'utilizzo di DBMS. Parametri dei driver di DBMS).

- Se nel passaggio **3** è stata selezionata l'opzione **Usa il database esistente** e nel passaggio **4** è stato impostato il percorso del file di configurazione di Server, impostare il percorso del file di database che verrà utilizzato secondo il file di configurazione di Server impostato.

6. Se nel passaggio **3** è stata selezionata l'opzione **Crea un nuovo database** o per l'opzione **Usa il database esistente** nel passaggio **4** non è stato 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 è possibile gestire il Server solo dal Pannello di controllo aperto sullo stesso computer, nonché può connettersi al Server solo 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 l'accesso al Server è possibile su tutte le interfacce.

Di default viene utilizzata la porta `2193`.

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 passaggio **3** è stata selezionata l'opzione **Crea un nuovo database** o per l'opzione **Usa il database esistente** nel passaggio **4** non è stato impostato il percorso del file di configurazione di Server, si aprirà la finestra di **Server proxy** per configurare le impostazioni di 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 passaggio **3** è stata 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 **Directory di installazione di Server Dr.Web** viene impostata la directory in cui viene installato il Server. Per modificare la directory predefinita, premere il pulsante **Sfoglia** e selezionare la directory desiderata.
  - Nel campo **Directory per il backup di Server Dr.Web** viene impostata la directory in cui verranno salvati i backup dei dati critici del Server secondo il calendario dei task del Server. Per cambiare la directory predefinita, premere il pulsante **Sfoglia** e selezionare la directory desiderata.
- 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 addizionali, 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 configurare e di gestione base del Server:

- La directory **Gestione del server** contiene i comandi di avvio, riavvio e arresto del Server, nonché i comandi di configurazione del log e altri comandi del Server descritti in modo più dettagliato nel documento **Allegati**, p. H3. Server Dr.Web.

- La voce **Interfaccia web** — per aprire il Pannello di controllo e connettersi al Server installato su 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.

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

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

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

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

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

   

   Per eseguire il pacchetto di installazione, è possibile utilizzare le opzioni della riga di comando. I parametri del comando di esecuzione sono riportati nel documento **Allegati**, p. H6. Installer di Server Dr.Web per SO della famiglia UNIX.

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

2. In seguito viene riportato il testo del contratto di licenza. Per continuare l'installazione, si deve accettare il contratto di licenza.
3. Quando il programma chiede 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.
6. Durante l'installazione viene generata una password casuale per l'amministratore principale. Dopo il completamento dell'installazione questa password viene restituita attraverso la console nei risultati dell'installazione del Server.

   

   La password amministratore creata viene salvata nel database del Server. Se necessario, è possibile recuperare questa password tramite gli strumenti di gestione del database, se è utilizzato un database esterno, o tramite l'utility `drwidbsh` per il database interno

(per maggiori informazioni v. documento **Allegati**, p. Ripristino della password dell'amministratore di Dr.Web Enterprise Security Suite).

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

Utilizzare i comandi:

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

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

Nel caso di installazione di Server nell'ambiente del sistema operativo Astra Linux versione 1.6 in modalità ambiente software chiuso, potrebbe non essere possibile avviare il programma di installazione a causa dell'assenza della chiave di cifratura pubblica di Server Dr.Web nella lista delle chiavi affidabili. In questo caso è necessario effettuare la configurazione preliminare della modalità ambiente software chiuso, dopodiché avviare di nuovo il programma di installazione.

Per pre-configurare la modalità ambiente software chiuso

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

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

4. Riavvia il sistema.

5.2. Installazione di Agent Dr.Web

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

Se sulla postazione è già installato l'Antivirus, prima di iniziare la nuova installazione, è necessario rimuovere l'Antivirus installato.

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

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

1. Localmente.

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

2. 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 12.0 avviene secondo il seguente schema:

- Se l'installer o il pacchetto di installazione di Agent viene avviato in modalità GUI su una postazione con un prodotto standalone installato versione 7.0/8.0/9.0/9.1/10.0/11.0/11.5, verrà avviato l'installer del prodotto installato. Quindi all'utente verrà chiesto di immettere un codice di conferma delle azioni e rimuovere il prodotto. Dopo il riavvio del sistema operativo verrà avviata la versione GUI dell'installer che è stato avviato inizialmente per l'installazione dell'Agent per Dr.Web Enterprise Security Suite versione 12.0.
- Se l'installer di Agent viene avviato in modalità background su una postazione con un prodotto standalone installato versione 7.0/8.0/9.0/9.1/10.0/11.0/11.5, nessun'azione verrà eseguita. In caso di installazione remota, l'installer restituirà al Pannello di controllo un messaggio sulla presenza 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 12.0 in qualsiasi dei modi possibili.
- Se l'installer di Agent viene avviato con installazione sia locale che remota su una postazione con il prodotto standalone installato versione 12.0, il prodotto installato passerà da modalità standalone a modalità di protezione centralizzata. Dopo la connessione e l'autenticazione sul Server possono essere ricevuti aggiornamenti, nuove impostazioni e liste dei componenti da installare, a seconda dei quali può essere richiesto un riavvio del computer.

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

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

5.2.1. File di installazione

Pacchetti di installazione

Pacchetto di installazione individuale

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

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

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

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

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

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

Pacchetto di installazione di gruppo

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

Il pacchetto d'installazione di gruppo comprende l'installer di Agent, le impostazioni di connessione al Server, nonché l'identificatore e la password del gruppo custom in cui verrà inclusa la postazione dopo l'installazione di Agent. Però le impostazioni di autenticazione della postazione sul Server e i componenti antivirus non fanno parte del pacchetto d'installazione di gruppo.

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

Installer

L'Installer di Agent è diverso dal pacchetto di installazione in quanto non include le impostazioni di connessione al Server e di autenticazione della postazione sul 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 direttamente 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 `webmin/install` (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 modificare questa risorsa a propria discrezione.

- *L'installer completo* `drweb-12.0.0-<build>-esuite-agent-full-windows.exe` installa contemporaneamente Agent e il pacchetto antivirus.

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

Gli Installer per l'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 scaricare nel repository i **Prodotti aziendali Dr.Web** dai server SAM ulteriormente dopo l'installazione di Server Dr.Web.

Informazioni dettagliate su come gestire il repository di Server sono riportate in **Manuale dell'amministratore**, sezione Gestione del repository 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.

   Gli installer per le postazioni protette sotto tutti i sistemi operativi supportati da Dr.Web Enterprise Security Suite si trovano nelle directory con i nomi corrispondenti al nome del sistema operativo.
2. Certificato di Server `drwcsd-certificate.pem`.

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 l'indirizzo IP o il 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).

5.2.2. Installazione locale di Agent Dr.Web

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

Prima della prima installazione degli Agent Dr.Web, è necessario aggiornare il repository 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, macOS

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

- Pacchetto di installazione individuale creato nel Pannello di controllo.
- Pacchetto d'installazione di gruppo creato nel Pannello di controllo.
- Installer di Agent Dr.Web.

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

a) In caso di creazione del pacchetto di installazione individuale, viene messo a disposizione un installer di Agent Dr.Web, nonché i parametri di connessione al Server e i parametri di autenticazione della postazione sul Server.

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 strumenti:

- Pacchetto di installazione individuale creato nel Pannello di controllo `drweb_ess_<SO>_<postazione>.exe`.
- Pacchetto di installazione di gruppo creato nel Pannello di controllo `drweb_ess_<SO>_<gruppo>.exe`.
- Installer completo di Agent Dr.Web `drweb-12.0.0-<build>-esuite-agent-full-windows.exe`.
- Installer di rete di Agent Dr.Web `drwinst.exe`.

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

a) Quando il software viene installato dal pacchetto di installazione individuale, le impostazioni di connessione al Server e quelle di autenticazione della postazione sul Server sono incluse nel pacchetto di installazione. L'installazione tramite il pacchetto di installazione individuale 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 da un pacchetto d'installazione di gruppo, le impostazioni di connessione al Server, nonché l'identificatore e la password del gruppo custom in cui verrà inclusa la postazione dopo l'installazione di Agent, fanno parte del pacchetto d'installazione. Però le impostazioni di autenticazione della postazione sul Server e i componenti antivirus non fanno parte del pacchetto d'installazione di gruppo. Dopo l'installazione di Agent viene eseguita la connessione di Agent al Server durante la quale viene determinata la disponibilità di postazioni libere nel gruppo custom di cui il pacchetto d'installazione di gruppo è stato utilizzato. Se sono

disponibili postazioni libere, le impostazioni di autenticazione della postazione sul Server vengono fornite automaticamente.

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.

d) 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.

Caratteristiche comparative dei file di installazione

File di installazione		Installazione di Agent	Installazione del pacchetto antivirus	Parametri di connessione al Server	Parametri di autenticazione sul server
Pacchetto di installazione	Individuale	+	–	+	+
	Di gruppo	+	–	+	–
Installer	Di rete	+	–	–	–
	Completo	+	+	–	–

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

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

Inoltre, è possibile eseguire tutti i tipi di file di installazione di Agent dalla riga di comando con utilizzo delle opzioni riportate nel documento **Allegati**, p. H1. Installer di rete.

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

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

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

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

3. Installare Agent Dr.Web sulla postazione.

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

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

   Se sulla postazione è già installato il software antivirus, l'installer cercherà di eliminarlo prima di cominciare l'installazione. Se il tentativo non è riuscito, l'utente dovrà per conto proprio eliminare il software antivirus utilizzato sulla postazione.

4. Per le postazioni macOS configurare i parametri di connessione al Server Dr.Web localmente.

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

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 un account utente, prestare attenzione al nome di Server impostato nelle

seguenti sezioni del Pannello di controllo:

1. **Amministrazione** → **Configurazione del web server** → campo **Indirizzo di Server Dr.Web**. Il valore di questo parametro viene utilizzato per generare il link di un pacchetto di 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 **Indirizzo di Server Dr.Web**. Il valore di questo parametro viene trascritto nei pacchetti di installazione di Agent e determina a quale Server si connetterà l'Agent ad installazione.

   Se il valore di questo parametro non è impostato in nessuno posto, nel corso della creazione del pacchetto di 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** nel menu principale del Pannello di controllo.
2. Nella barra degli strumenti premere il pulsante **Aggiungi oggetto della rete** → **Crea postazione**. Nella parte destra della finestra del Pannello di controllo si apre la barra di creazione di un account postazione.
3. Nel campo **Numero** indicare il numero di account che si vuole creare.
4. Nel campo **Identificatore** viene generato automaticamente l'identificatore univoco della postazione che viene creata. Se necessario, è possibile modificarlo.
5. Nel campo **Nome** impostare il nome di postazione che verrà visualizzato nella lista gerarchica della rete antivirus. In seguito, dopo che la postazione si è connessa al Server, questo nome può essere sostituito automaticamente al nome impostato localmente sulla postazione.
6. Nei campi **Password** e **Confermare la password** è possibile impostare una password di accesso della postazione al Server. Se la password non è indicata, verrà generata automaticamente.

   Quando vengono creati più di un account, i campi **Identificatore**, **Nome** e **Password** (**Confermare la password**) verranno impostati automaticamente e non possono essere modificati durante la creazione di postazioni.
7. Nel campo **Descrizione** inserire informazioni supplementari sulla postazione. Questo parametro non è obbligatorio.
8. Nella sezione **Gruppi** vengono impostati i gruppi di cui farà parte la postazione che viene creata.

- Nella lista **Appartenenza** si può configurare una lista di gruppi custom di cui farà parte la postazione.
  Di default, la postazione fa parte del gruppo **Everyone**. Se ci sono gruppi personalizzati, si può includerci la postazione che viene creata, senza limitazioni al 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**.

- Nella lista **Criteri** è possibile impostare un criterio da cui verranno prese le impostazioni della postazione che viene creata.
  Di default, nessun criterio è assegnato. Per assegnare un criterio, spuntare il flag di fronte al criterio richiesto. La postazione erediterà impostazioni dalla versione corrente di questo criterio. Non è possibile assegnare più di un criterio a una postazione.

9. Nella sezione **Server proxy** vengono configurate le impostazioni del Server proxy Dr.Web associato a questa postazione.
   Se si vuole installare il Server proxy sulla postazione che viene creata, spuntare il flag **Crea un Server proxy associato** ed impostare i parametri del Server proxy. I parametri sono analoghi ai parametri di creazione del Server proxy.

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

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

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

I link 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.

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

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

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

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

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

1. Nel menu dell'applicazione Antivirus Dr.Web premere la voce **Preferenze** e selezionare la sezione **Modalità**.
2. Spuntare il flag **Attiva la modalità di protezione centralizzata**.
3. Le impostazioni di connessione al Server, quale l'indirizzo IP e i parametri di autenticazione sul Server, vengono definite automaticamente dal file di configurazione `install.cfg` locato all'interno del pacchetto di installazione individuale.

   Per utilizzare il file:

   a) Nella Gestione licenze premere sul link **Altri tipi di attivazione**.

   b) Trascinare il file di configurazione nella finestra che si è aperta o fare clic sull'area circondata da linea punteggiata per aprire una finestra per selezionare il file.

   Dopo l'installazione del file, i campi di input delle impostazioni di connessione al Server verranno compilati automaticamente.

5.2.2.2. Installazione di Agent Dr.Web attraverso un pacchetto d'installazione di gruppo

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

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

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

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

   Se sulla postazione è già installato il software antivirus, l'installer cercherà di eliminarlo prima di cominciare l'installazione. Se il tentativo non è riuscito, l'utente dovrà per conto proprio eliminare il software antivirus utilizzato sulla postazione.

7. Dopo l'installazione di Agent, l'Agent viene connesso al Server indicato nel pacchetto d'installazione di gruppo. Nel corso della prima connessione al Server viene determinata la disponibilità di postazioni libere nel gruppo custom di cui il pacchetto d'installazione di gruppo è stato utilizzato per l'installazione di Agent. Il numero di postazioni libere viene determinato sulla base del numero degli account in questo gruppo, di cui l'ammissione non è ancora scaduta. Con ogni connessione del pacchetto d'installazione di gruppo, il numero di postazioni libere viene ricalcolato per fornire le informazioni attuali.

a) Se sono disponibili postazioni libere, le impostazioni di autenticazione della postazione per la connessione al Server vengono fornite automaticamente. Questa procedura viene eseguita in modo trasparente per l'amministratore e non richiede un intervento aggiuntivo.

b) Se non ci sono postazioni libere in questo gruppo, l'installazione viene interrotta con un relativo messaggio all'utente.

5.2.2.3. Installazione di Agent Dr.Web attraverso installer

L'Installer di Agent è diverso dal pacchetto di installazione in quanto non include le impostazioni di connessione al Server e di autenticazione della postazione sul 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 scaricare nel repository i **Prodotti aziendali Dr.Web** dai server SAM ulteriormente dopo l'installazione di Server Dr.Web.

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

Installazione locale su postazioni Android, Linux, macOS

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

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

Se il software viene installato attraverso l'installer senza il file di configurazione, è necessario indicare manualmente sulla postazione l'indirizzo del Server 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 un pacchetto di installazione che include un file di configurazione con le impostazioni di connessione e di autenticazione. Si consiglia di utilizzare il pacchetto di installazione invece dell'installer.

Installazione locale su postazioni SO Windows

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

- *l'installer di rete* `drwinst.exe` installa solo Agent. Dopo la connessione a Server, Agent scarica e installa i componenti corrispondenti del pacchetto antivirus.
- *l'installer completo* `drweb-12.0.0-<build>-esuite-agent-full-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 un pacchetto di installazione. Se non è necessario installare attraverso un pacchetto completo o l'installer di rete, si consiglia di utilizzare il pacchetto di installazione invece dell'installer.

Sono possibili le seguenti varianti di connessione al Server:

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.
Non viene impostato	Agent cerca Server nella rete utilizzando il *Servizio di rilevamento Server*. 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 solo in SO Windows.

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

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

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

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

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

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

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

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

   - 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 dell'opzione `/regagent yes` consente di registrare Agent nel corso dell'installazione nella lista di aggiunzione e di rimozione dei programmi.

La lista completa dei parametri dell'Installer di rete è riportata nel documento **Allegati**, p. H1. 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 di installazione di Agent (nell'installazione di Server questa è la sottodirectory `webmin/install` della directory di installazione di Server, in seguito può essere spostata) o scaricare dalla pagina di installazione del Pannello di controllo il file eseguibile dell'installer `drwinst.exe` e il certificato `drwcsd-certificate.pem`. Eseguire il file `drwinst.exe`.

Si apre la finestra dell'installazione guidata di Agent Dr.Web. Le azioni successive di installazione di Agent 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 sulle postazioni è descritta nel manuale **Agent Dr.Web per Windows. Manuale dell'utente**.

5.2.3. Installazione remota di Agent Dr.Web per SO Windows

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

L'installazione remota è possibile 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 degli Agent Dr.Web è possibile solo su postazioni con i SO della famiglia Windows (vedi documento **Allegati**, p. Allegato A. Lista completa delle versioni supportate dei SO), ad eccezione delle edizioni Starter e Home.
>
> Per installare l'Agent Dr.Web in remoto su postazioni, è necessario disporre dei privilegi di amministratore delle 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 (vedi la tabella sotto per la posizione dell'impostazione in diverse versioni del SO Windows).

Se le postazioni della rete 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.

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

> Le impostazioni indicate possono abbassare la sicurezza dei computer della rete. Si consiglia vivamente di conoscere lo scopo delle impostazioni indicate prima di apportare modifiche al sistema, altrimenti, di rinunciare all'installazione remota e installare l'Agent in maniera manuale.
>
> Dopo aver configurato la postazione della rete, si consiglia di ripristinare tutte le impostazioni modificate ai valori che erano impostati prima della modifica per non violare i criteri di sicurezza di base del sistema operativo.

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

SO	Impostazione	
		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: **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**.

<table>
<tr><th>SO</th><th colspan="2">Impostazione</th></tr>
<tr><td rowspan="2"></td><td></td><td>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.</td></tr>
<tr><td colspan="2">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.</td></tr>
<tr><td rowspan="5">Windows 7

Windows Server 2008 R2</td><td rowspan="2">Attivare Condivisione file e stampanti</td><td>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.</td></tr>
<tr><td>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.</td></tr>
<tr><td rowspan="2">Impostare autenticazione a livello di rete nei criteri locali</td><td>Stile nuovo:

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.</td></tr>
<tr><td>Stile classico:</td></tr>
</table>

SO	Impostazione	
		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 8 Windows 8.1 Windows Server 2012 Windows Server 2012 R2 Windows 10	Attivare Condivisione file e stampanti	Stile nuovo: **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**.
		Stile classico: **Impostazioni → Pannello di controllo → Centro connessioni di rete e condivisione → Modifica impostazioni di condivisione avanzate → Condivisione file e stampanti → Attivare Condivisione file e stampanti**.
	Impostare autenticazione a livello di rete nei criteri locali	Stile nuovo: **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 protezione per gli account locali → Classico: gli utenti locali effettuano l'autenticazione di se stessi**.
		Stile classico: **Impostazioni → Pannello di controllo → Amministrazione → Criteri di protezione locali → Impostazioni di protezione → Criteri di protezione locali → Impostazioni di protezione →**

SO	Impostazione	
		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.	

Se per l'account sulla postazione della rete è 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**.

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

Sono possibili i seguenti modi di installazione remota 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 Dr.Web, utilizzando Scanner di rete

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

Tabella 5-1. Possibili tipi di icone

Icona	Descrizione
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	
	Postazione attiva con il software antivirus installato.
	Postazione attiva con lo stato del software antivirus non confermato: sul computer non è installato il software antivirus o la presenza del software non è stata verificata.

Si possono inoltre espandere gli elementi della directory corrispondenti alle postazioni con l'icona per visualizzare una lista dei componenti installati.

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

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

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

9. 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.

10. Di default nel campo **Server Dr.Web** è visualizzato l'indirizzo IP o il nome DNS del Server Dr.Web a cui è connesso il Pannello di controllo. Se necessario, indicare in questo campo l'indirizzo del Server da cui verrà installato il software antivirus. Quando vengono impostati più 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 (modalità *Multicast*).

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

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

11. Dalla lista a cascata **Lingua** selezionare la lingua di interfaccia per Antivirus Dr.Web che verrà installato sulle postazioni.
12. Nel campo **Numero di installazioni simultanee** impostare il numero massimo di postazioni su cui può essere eseguita l'installazione remota che viene lanciata.
13. Nel campo **Time-out dell'installazione (s)** impostare il tempo massimo in secondi di attesa del completamento dell'installazione di Agent. Valori ammissibili: 1-600. Di default, è impostato il

valore di 180 secondi. In caso di capacità bassa del canale di comunicazione tra il Server e l'Agent, si consiglia di aumentare il valore di questo parametro.

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

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

    Nel corso dell'installazione dell'Agent prima viene utilizzato il primo account nella lista. Se l'installazione sotto questo account non è riuscita, viene utilizzato l'account successivo e così via.
18. Dopo aver inserito tutti i parametri necessari, premere **Installa**.

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

Per avviare l'installazione, viene utilizzato l'installer di rete del Server corrente, che si trova nella directory `webmin\install\windows` della directory di installazione di Server, e inoltre il certificato SSL `drwcsd-certificate.pem` locato nella directory `etc` della directory di installazione di Server.

19. 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.
20. Riavviare il computer a richiesta di 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 installare Agent Dr.Web via 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 passaggi successivi di installazione sono uguali ai passaggi **8-21** della procedura sopra.

Installazione per account con gli ID specificati

Se viene creato un nuovo account di postazione:

1. Creare un nuovo account o diversi nuovi account di postazioni (v. p. Creazione di nuovo account).
2. Subito dopo la creazione del nuovo account, nella parte destra della finestra principale si apre un pannello con l'intestazione **Creazione della postazione**. Premere il pulsante **Installa**.
3. Si apre la finestra di Scanner di rete.
4. I passaggi successivi di installazione sono uguali ai passaggi **2-21** della procedura sopra.
5. Dopo la fine dell'installazione, controllare se nella lista gerarchica sono cambiare le icone delle postazioni corrispondenti.

Se viene utilizzato un account di postazione già esistente:

1. Nella lista gerarchica della rete antivirus selezionare una nuova postazione o un gruppo di postazioni su cui non sono ancora stati installati gli Agent, oppure selezionare il gruppo **New** (per installare su tutti i nuovi account disponibili).
2. Nella barra degli strumenti premere il pulsante **Installa Agent Dr.Web**.
3. Si apre la finestra di Scanner di rete.
4. I passaggi successivi di installazione sono uguali ai passaggi **2-21** della procedura sopra.
5. Dopo la fine dell'installazione, controllare se nella lista gerarchica sono cambiare 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.

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

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

L'installazione di Agent 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. Selezionare la voce **Amministrazione** nel menu principale, dopodiché nel menu di gestione selezionare la sezione **Configurazione generale del repository**.
2. Andare alla scheda **Pacchetti di installazione Dr.Web** → **Prodotti aziendali Dr.Web**.
3. Spuntare il flag di fronte a **Agent Dr.Web per Active Directory**. Premere **Salva**.
4. Aggiornare il repository attraverso la sezione **Stato del repository** nel menu di gestione.
5. Dopo il caricamento da SAM l'installer di Agent Dr.Web per le reti con **Active Directory** sarà disponibile nella pagina di installazione all'indirizzo:

   `https://`<*Indirizzo_Server*>`:`<*numero_porta*>`/install/activedirectory`

   dove <*indirizzo_server*> è l'indirizzo IP o il nome DNS del computer su cui è installato il Server Dr.Web; <*numero_porta*> è il numero di porta `9081` (o `9080` per http).
6. Scaricare l'installer di Agent Dr.Web per le reti con **Active Directory** dalla pagina di installazione.
7. 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 di installazione di Agent Dr.Web per le reti con **Active Directory** di solito ha il seguente formato:

`drweb-12.00.0-<build>-esuite-agent-activedirectory.msi`

Parametri

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

- `ESSERVERADDRESS=<nome_DNS>` — l'indirizzo del Server Dr.Web a cui si connetterà l'Agent. Per i formati possibili vedi documento **Allegati**, p. Allegato E.
- `ESSERVERPATH=<nome_completo_file>` — il percorso completo del certificato del Server Dr.Web e il nome del file (di default, è il file `drwcsd-certificate.pem` nella sottodirectory `webmin/install` della directory di installazione del Server Dr.Web).
- `TARGETDIR` — la directory di rete per l'immagine di Agent (pacchetto di installazione di Agent modificato), la quale 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 indicato nel formato di indirizzi di rete, anche se è disponibile localmente; la directory deve essere obbligatoriamente accessibile dalle postazioni di destinazione.

Prima dell'installazione amministrativa, non è necessario mettere i file di installazione manualmente nella directory di destinazione per l'immagine di Agent (vedi 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 di destinazione automaticamente nel corso dell'installazione amministrativa. Se questi file sono presenti nella directory di destinazione 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 di destinazione diversa per ciascun Server.

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

Esempi

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

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

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

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

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

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

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

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

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

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

   L'installer di Agent 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 (vedi documento **Allegati**, p. Allegato E). Indicare il percorso del certificato di Server Dr.Web (`drwcsd-certificate.pem`). Premere il pulsante **Avanti**.

4. Nella finestra successiva, indicare la directory di rete in cui verrà scritto l'immagine di Agent. Il percorso della directory deve essere scritto nel formato di indirizzi di rete, anche se la directory è disponibile localmente; la directory deve essere obbligatoriamente accessibile dalle postazioni di destinazione. Premere il pulsante **Installa**.
5. Dopo la fine dell'installazione viene automaticamente richiamata la finestra di configurazione attraverso cui si può ordinare l'installazione dei pacchetti sui computer della rete.

Configurazione dell'installazione del pacchetto su postazioni selezionate

1. Nel **Pannello di controllo** (o nel menu **Start** in caso di SO Windows 2003/2008/2012/2012R2 Server, nel menu **Start** → **Programmi** in caso di SO Windows 2000 Server), selezionare **Amministrazione** → **Active Directory — utenti e computer** (in modalità grafica di installazione di Agent 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 fare questo, dal menu contestuale del dominio selezionare **Nuovo** → **Unità**. Nella finestra che si è aperta, immettere il nome della nuova unità e premere **OK**. Includere nell'unità creata i computer su cui si vuole installare Agent.
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.

5.3. Installazione di NAP Validator

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

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

Per installare NAP Validator

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

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

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

5.4. Installazione del Server proxy Dr.Web

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.

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

- In modo automatico durante l'installazione di Agent Dr.Web per Windows

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

- In modo automatico su una postazione con installato Agent Dr.Web per Windows

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

- Manualmente tramite l'installer grafico

  L'installazione viene effettuata dall'amministratore manualmente su qualsiasi postazione adatta della rete. È possibile che su tale postazione non sia installato nessun altro componente della rete antivirus.

L'installazione di Server proxy nei sistemi operativi della famiglia UNIX viene effettuata solo manualmente tramite l'installer.

5.4.1. Creazione dell'account del Server proxy Dr.Web

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

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

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

   

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

2. Selezionare la voce **Rete antivirus** nel menu principale del Pannello di controllo.
3. Le azioni necessarie per la creazione di un Server proxy dipenderanno da quello se si vuole installare il Server proxy su una postazione esistente con Agent Dr.Web o installare il Server proxy separatamente:

N	Azioni	Installare con Agent	Installare separatamente
a)	1. Nell'albero della rete antivirus selezionare una postazione su cui si vuole installare un Server proxy associato. 2. Nella barra delle proprietà della postazione selezionata passare alla sezione **Server proxy**.	+	–
b)	1. Nell'albero della rete antivirus selezionare una postazione su cui si vuole installare un Server proxy associato. 2. Nella barra degli strumenti selezionare l'opzione **Aggiungi oggetto della rete** → **Crea Server proxy**.	+	+
c)	1. Assicurarsi che nell'albero della rete antivirus non sia selezionata una postazione. 2. Nella barra degli strumenti selezionare l'opzione **Aggiungi oggetto della rete** → **Crea Server proxy**.	+	+

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

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

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

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

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

L'identificatore e la password di Server proxy vengono utilizzati in un unico esemplare. Su tutti i Server a cui si connette il Server proxy devono essere creati account di Server proxy con le informazioni di autenticazione uguali (vedi Connessione del Server proxy Dr.Web al Server Dr.Web).

Dopo la creazione dell'account di Server proxy non sarà possibile modificare l'identificatore.

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

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

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

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

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

   Un Server proxy può rientrare in solo un gruppo.

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

9. Premere il pulsante **Salva**.

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

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

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

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

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

1. Definire le impostazioni del Server proxy nel Pannello di controllo, come descritto in **Manuale dell'amministratore** nella sezione Configurazione del Server proxy in remoto. Le impostazioni devono essere definite per il gruppo in cui si prevede di creare il Server proxy. In questo caso esso erediterà le impostazioni definite al momento della creazione. È anche possibile definire queste impostazioni (sia per il gruppo in caso di ereditarietà che individualmente per il Server proxy stesso) dopo la creazione del Server proxy, ma prima della connessione del Server proxy all'account che viene creato.

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

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

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

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

5.4.3. Installazione del Server proxy Dr.Web tramite l'installer

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

Installazione del Server proxy in SO Windows

1. Creare un account di Server proxy tramite il Pannello di controllo, come descritto nella sezione Creazione dell'account del Server proxy Dr.Web.
2. Copiare sulla postazione su cui si prevede di effettuare l'installazione il certificato del Server a cui si connetterà il Server proxy (vedi Connessione del Server proxy Dr.Web al Server Dr.Web) e l'installer di Server proxy fornito insieme al pacchetto Server.

3. Avviare l'installer di Server proxy. Si apre la finestra **InstallShield Wizard** con informazioni sul prodotto che viene installato. Premere il pulsante **Avanti**.
4. Nella finestra dei parametri di Server proxy nella scheda **Generali** impostare i seguenti parametri principali:
   - Se necessario, nel campo **Percorso dei dati del programma** modificare il percorso per il collocamento dei file utilizzati da Server proxy: il log di funzionamento, i file di configurazione, la cache. Di default viene utilizzato il percorso `%PROGRAMDATA%/Doctor Web/drwcs`. Per selezionare un percorso diverso, premere il pulsante **Sfoglia**.
   - Nel campo **Indirizzo per l'ascolto** 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 **Porta** impostare il numero di porta su cui il Server proxy "è in ascolto". Di default è la porta `2193`.
   - Spuntare il flag **Attiva rilevamento** per attivare la modalità di simulazione del Server. Questa modalità consente ai client di rilevare il Server proxy come un Server Dr.Web nel processo della sua ricerca attraverso le richieste broadcast.
   - Spuntare il flag **Attiva multicasting** affinché il Server proxy risponda alle richieste broadcast indirizzate al Server.
     - Nel campo **Gruppo multicast** 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 i client che cercano i Server Dr.Web attivi. Se il campo viene lasciato vuoto, il Server proxy non farà parte di nessuno dei gruppi multicast. Di default il gruppo multicast di cui il Server fa parte è `231.0.0.1`.
   - Nella sezione **Parametri di connessione con i client**:
     - Dalla lista a cascata **Crittografia** selezionare la modalità di cifratura traffico per i canali tra il Server proxy e i client: Agent ed installer di Agent.
     - Dalla lista a cascata **Compressione** selezionare la modalità di compressione del traffico per i canali tra il Server proxy e i client: Agent ed installer di Agent. Dalla lista a cascata **Livello** selezionare un livello di compressione (da 1 a 9).
5. Nella scheda **Cache** impostare i seguenti parametri di memorizzazione nella cache del Server proxy:

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

   - Nel campo **Periodo di rimozione delle revisioni (min)** impostare la periodicità di rimozione delle vecchie revisioni dalla cache nel caso in cui il loro numero ha superato il numero massimo consentito di revisioni conservate. Il valore viene impostato in minuti. Di default è di 60 minuti.

- Nel campo **Numero di revisioni conservate** impostare il numero massimo di revisioni di ciascun prodotto che rimarranno nella cache dopo una pulizia. Di default vengono conservate le ultime 3 revisioni, le revisioni più vecchie vengono rimosse.

- Nel campo **Periodo di scaricamento da memoria dei file non utilizzati (min)** impostare l'intervallo di tempo in minuti tra gli scaricamenti di file non utilizzati dalla memoria operativa. Di default è di 10 minuti.
- Dalla lista a cascata **Modalità di verifica dell'integrità** selezionare la modalità di verifica dell'integrità dei dati memorizzati nella cache:
  - **All'avvio** — al momento dell'avvio del Server proxy (può richiedere molto tempo).
  - **Durante l'inattività** — durante il tempo di inattività del Server proxy.

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

6. Si apre la finestra di configurazione del reindirizzamento delle connessioni:
   - Nel campo **Indirizzo di reindirizzamento** impostare l'indirizzo del Server Dr.Web su cui verranno reindirizzate le connessioni stabilite dal Server proxy. Come la prima voce della lista deve essere indicato il Server a cui il Server proxy dovrà connettersi per ricevere la configurazione. Il certificato di questo Server è stato copiato sulla postazione nel passaggio 2.

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

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

   Per aggiungere un altro Server alla lista di reindirizzamento traffico, fare clic sul pulsante  e definire le impostazioni come nella lista sopra.

   Per cancellare un Server dalla lista di reindirizzamento traffico, fare clic sul pulsante  di fronte al Server che si vuole cancellare.

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

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

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

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

   La connessione sarà al primo Server specificato nel passaggio 6 per il reindirizzamento traffico.

- Nel campo **Certificato Server** impostare il file di certificato copiato sulla postazione nel passaggio 2. Per selezionare il file, premere il pulsante **Sfoglia**.
- Nei campi **Identificatore** e **Password** impostare le credenziali dell'account creato sul Server nel passaggio 1.

8. Si apre una finestra che avvisa che il Server proxy è pronto per l'installazione.

   Se è necessario modificare i parametri di installazione aggiuntivi, in particolare, la directory di installazione di Server proxy, premere **Parametri aggiuntivi**.

   Per iniziare l'installazione del Server proxy, premere il pulsante **Installa**.

9. Dopo il completamento del processo di installazione premere il pulsante **Esci**.
10. Dopo l'installazione il Server proxy si connetterà al Server indicato come il primo nel passaggio 6 per ottenere un file di configurazione completo. Se le impostazioni non sono state definite sul Server, il file di configurazione non verrà scaricato. La configurazione impostata dall'installer verrà utilizzata fino a quando non verrà impostata una configurazione sul Server connesso.

Installazione di Server proxy sotto i sistemi operativi della famiglia UNIX

1. Avviare l'installer di Server proxy tramite il seguente comando:

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

2. Per continuare l'installazione, accettare il contratto di licenza.
3. Indicare il percorso del certificato di Server. Il certificato può anche essere aggiunto dopo l'installazione di Server proxy (vedi Connessione del Server proxy Dr.Web al Server Dr.Web).
4. Se necessario, possono essere utilizzati i file di configurazione da un'installazione precedente di Server proxy:
   - Per utilizzare una copia di backup memorizzata di default nella directory `/var/tmp/drwcsd-proxy`, premere INVIO.
   - Per utilizzare una copia di backup da un'altra directory, inserire manualmente il percorso della copia di backup.
   - È inoltre possibile installare il Server proxy con le impostazioni predefinite, senza utilizzare una copia di backup della configurazione da un'installazione precedente. Per fare ciò, premere 0.
5. Dopo l'installazione di Server proxy, se necessario, è possibile modificare manualmente i file di configurazione corrispondenti (vedi Connessione del Server proxy Dr.Web al Server Dr.Web).

Avvio e arresto

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

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

Nel corso dell'installazione del software sotto il sistema operativo **Linux** verrà creato uno script `init` per l'avvio e l'arresto del Server proxy `/etc/init.d/dwcp_proxy`.

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

Impostazioni di connessione

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

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

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

  - Il certificato del Server è richiesto per la connessione al Server per la finalità di gestione delle impostazioni in remoto, e inoltre per il supporto della cifratura del traffico tra il Server e il Server proxy.
  - Il certificato del Server proxy, che viene firmato dal certificato e dalla chiave privata del Server (la procedura viene effettuata automaticamente sul Server dopo la connessione e non richiede l'intervento dell'amministratore), è richiesto per la connessione degli Agent e per il supporto della cifratura del traffico tramite gli Agent e il Server proxy.

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

```
[<certificato_1>]


[<certificato_2>]


[<certificato_3>]

...
```

- **Indirizzo del Server.**

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

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

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

  

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

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

```
[<ID_del_Server_proxy>]

[<Password_del_Server_proxy>]
```

Connessione del Server proxy al Server Dr.Web

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

Connessione automatica durante l'installazione in SO Windows:

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

  Dopo l'installazione del Server proxy i file per la connessione al Server si trovano di default nella directory: `C:\Program Files\DrWeb Server\etc`.

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

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

5. Nel file di configurazione `drwcsd-proxy.auth` definire le impostazioni di connessione al Server per l'account creato nel passaggio 2 secondo il formato descritto sopra.

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

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

   È necessario impostare i seguenti permessi per i file:

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

drwcsd-proxy.auth 0600 drwcs:drwcs
```

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

6.1. Rimozione di Server Dr.Web

6.1.1. Rimozione di Server Dr.Web per SO Windows

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

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

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**.

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

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

Per rimuovere Server Dr.Web versione 10 e successive

SO Server	Azione
FreeBSD	Eseguire lo script: `/usr/local/etc/drweb.com/software/drweb-esuite.remove`
Linux	Eseguire lo script: `/etc/opt/drweb.com/software/drweb-esuite.remove`

Quando il Server viene rimosso nei SO **FreeBSD** e **Linux**, i processi server verranno terminati automaticamente, il database, i file delle chiavi e i file di configurazione verranno copiati nella directory predefinita — `/var/tmp/drwcs` (l'elenco dei file per il backup è riportato nella sezione Aggiornamento di Server Dr.Web per SO della famiglia UNIX).

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

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

6.2. Rimozione di Agent Dr.Web

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

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

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

6.2.1. Rimozione di Agent Dr.Web per SO Windows

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

L'installazione e la rimozione del software Agent su remoto sono possibili solo in una 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 della postazione antivirus su remoto (solo in caso di SO della famiglia Windows)

1. Selezionare la voce **Rete antivirus** nel menu principale del Pannello di controllo.
2. Nella finestra che si è aperta, nella directory della rete antivirus selezionare il gruppo richiesto o postazioni antivirus separate.
3. Nella barra degli strumenti della directory di rete antivirus premere **Generali** → **Disinstalla Agent Dr.Web**.
4. 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.

Nel caso di rimozione di Agent su remoto (la rimozione sulla postazione viene eseguita in background) verrà eseguito un riavvio forzato della postazione con un intervallo di cinque minuti. Non è possibile modificare l'intervallo o annullare il riavvio. Gli utenti della postazione vengono notificati del prossimo riavvio in una notifica a comparsa.

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

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 Dr.Web nella lista dei programmi installati**.

Se Agent è stato installato in modalità background dell'installer, la rimozione di software antivirus tramite i mezzi standard sarà disponibile solo se nell'installazione è stata utilizzata l'opzione `/regagent 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 client 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 o versioni successive e SO Windows Server 2008 o versioni successive:
    `%ALLUSERSPROFILE%\Doctor Web\Setup\`

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

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

- **Pacchetto di installazione individuale drweb_ess_<*SO*>_<*postazione*>.exe.**

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

- **Installer completo drweb-12.0.0-<*build*>-esuite-agent-full-windows.exe**

  Per rimuovere il software Agent e il pacchetto antivirus tramite l'installer completo, avviare il file di installazione `drweb-12.0.0-<build>-esuite-agent-full-windows.exe` della versione del prodotto che è installata.

- **Installer di rete drwinst.exe**

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

  Per esempio:

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

All'avvio del pacchetto di installazione `drweb_ess_<SO>_<postazione>.exe`, dell'installer completo `drweb-12.0.0-<build>-esuite-agent-full-windows.exe`

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

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

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

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

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

6.3. Rimozione del Server proxy Dr.Web

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

1. Localmente.

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

2. In remoto.

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

6.3.1. Rimozione del Server proxy Dr.Web in locale

In caso di SO Windows

Alla rimozione del Server proxy viene rimosso il file di configurazione `drwcsd-proxy.conf` (`drwcsd-proxy.xml` in caso della versione 10 e precedenti). Se necessario, salvare il file di configurazione manualmente prima di rimuovere il Server proxy.

Il software Server proxy viene rimosso tramite i mezzi standard di SO Windows attraverso la sezione **Pannello di controllo** → **Installazione ed eliminazione programmi** (**Programmi e funzionalità** in caso di SO Windows 2008 o versioni successive).

In caso di SO della famiglia UNIX

Quando viene rimosso il Server proxy, una copia di backup dei file di configurazione viene automaticamente salvata nella directory `/var/tmp/drwcsd-proxy`.

SO del Server proxy	Azione
FreeBSD	Eseguire lo script: `/usr/local/etc/drweb.com/software/drweb-esuite-proxy.remove`
Linux	Eseguire lo script: `/etc/opt/drweb.com/software/drweb-proxy.remove`

6.3.2. Rimozione del Server proxy Dr.Web in remoto

La rimozione del Server proxy in remoto è disponibile nel caso in cui il Server proxy è connesso al Server (vedi Connessione del Server proxy Dr.Web al Server Dr.Web).

Se l'account Server proxy viene rimosso nel Pannello di controllo, il Server proxy stesso viene rimosso dalla postazione.

Per rimuovere il Server proxy

1. Selezionare la voce **Rete antivirus** nel menu principale del Pannello di controllo.
2. Nella finestra che si è aperta, nella lista gerarchica fare clic sul nome di uno o più Server proxy che si vuole rimuovere.

3. Nella barra degli strumenti premere **Generali** → **Rimuovi gli oggetti selezionati**.
4. Si apre la finestra di conferma della rimozione dell'oggetto. Fare clic su **OK**.

Per rimuovere il Server proxy che è installato sulla postazione associata

1. Selezionare la voce **Rete antivirus** nel menu principale del Pannello di controllo.
2. Aprire la sezione delle proprietà della postazione su cui è installato il Server proxy in uno dei seguenti modi:
   a) Premere il nome della postazione nella lista gerarchica della rete antivirus. Nella parte destra della finestra del Pannello di controllo si apre automaticamente una sezione con le proprietà della postazione.
   b) Selezionare la voce **Proprietà** del menu di gestione. Si apre la finestra con le proprietà della postazione.
3. Nella finestra delle proprietà della postazione passare alla sezione **Server proxy**.
4. Premere **Rimuovi Server proxy**.
5. Fare clic su **Salva**. Il Server proxy verrà disinstallato dalla postazione. L'account del Server proxy verrà rimosso dal Server.

Capitolo 7: Aggiornamento dei componenti di Dr.Web Enterprise Security Suite

L'aggiornamento di Server dalle versioni 11.X alla versione 12.0 è disponibile 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.

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

- Prima dell'inizio dell'aggiornamento si consiglia vivamente di controllare la correttezza delle impostazioni del protocollo TCP/IP per la possibilità di accesso a internet. In particolare, il servizio DNS deve essere attivato e contenere le impostazioni corrette.
- Prima di aggiornare Server Dr.Web, si consiglia di aggiornare tutti i componenti della rete antivirus Dr.Web Enterprise Security Suite, inclusi Agent Dr.Web, all'ultima versione disponibile su SAM.
- Nel caso di configurazione della rete con diversi server, si deve tenere presente che tra i Server versione 12 e i Server versione 6 non è possibile la trasmissione degli aggiornamenti tra i server, e la comunicazione tra i server viene utilizzata solo per la trasmissione delle statistiche. Per assicurare la trasmissione degli aggiornamenti tra i server, è necessario aggiornare tutti i Server. Se c'è la necessità di mantenere nella rete antivirus i Server delle versioni precedenti per la connessione degli Agent installati sotto i sistemi operativi non supportati dalla versione 12 (vedere p. Aggiornamento di Agent Dr.Web), i Server versione 6 e i Server versione 12 devono ricevere gli aggiornamenti in modo indipendente.
- L'aggiornamento del cluster di Server Dr.Web dalle versioni 6 e 10 alla versione 12 deve essere eseguito separatamente, cioè i nodi devono essere sconnessi dal cluster uno per uno, associati al database interno e aggiornati, dopo di che devono essere nuovamente collegati uno per uno al cluster comune.
- Quando si aggiornano i componenti alla versione 12.0 in una rete antivirus in cui viene utilizzato il Server proxy Dr.Web, è necessario aggiornare anche il Server proxy alla versione 12.0. Altrimenti, la connessione degli Agent forniti con la versione 12.0 al Server versione 12.0 non sarà possibile. Si consiglia di effettuare l'aggiornamento nel seguente ordine: Server Dr.Web → Server proxy Dr.Web → Agent Dr.Web.
- Se il Server viene aggiornato dalla versione 6 alla versione 12, le impostazioni di funzionamento del Server attraverso il server proxy non vengono salvate. Dopo aver installato la versione 12, è necessario configurare manualmente la connessione attraverso il server proxy (vedere **Manuale dell'amministratore**, p. Proxy).
- All'aggiornamento di Server nessuna impostazione del repository viene trasferita nella nuova versione (le impostazioni vengono resettate ai valori di default), tuttavia, viene eseguito un back delle impostazioni. Se necessario, configurare le impostazioni del repository manualmente dopo l'aggiornamento di Server.

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

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

7.1. Aggiornamento di Server Dr.Web per SO Windows

L'aggiornamento del Server dalle versioni 6, 10 e 11 alla versione 12 e all'interno della versione 12 viene effettuato automaticamente tramite l'installer.

L'aggiornamento di Server dalle versioni 11.X alla versione 12.0 è inoltre disponibile 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.

Quando viene aggiornato il Server Dr.Web sotto il sistema operativo Windows dalla versione 10 e precedenti, le impostazioni delle seguenti sezioni del Pannello di controllo non verranno trasferite nella versione 12:

- **Configurazione del Server Dr.Web** → **Rete** → **Download** (il file `download.conf`),
- **Accesso remoto al Server Dr.Web** (il file `frontdoor.conf`),
- **Configurazione del web server** (il file `webmin.conf`).

Le impostazioni in queste sezioni verranno resettate ai valori di default. Se si vogliono utilizzare le impostazioni della versione precedente, configurarle manualmente dopo l'aggiornamento di Server nelle sezioni corrispondenti del Pannello di controllo sulla base dei dati da copie di backup dei file di configurazione.

Prima dell'inizio dell'aggiornamento del Server prestare attenzione alla sezione Aggiornamento di Agent Dr.Web.

L'aggiornamento di Server all'interno della versione 12 può inoltre 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 12 contengono un file di pacchetto. Alcuni di essi possono essere installati solo tramite il Pannello di controllo.

Salvataggio dei file di configurazione

Quando il Server viene aggiornato alla versione 12 per mezzo dell'installer, i file di configurazione vengono salvati nella directory impostata per il backup:

- Se viene aggiornato dalla versione 6: nella directory *<disco_di_installazione>*:\DrWeb Backup.
- Se viene aggiornato dalle versioni 10, 11 e all'interno della versione 12: nella directory che viene definita nell'impostazione **Salva backup dei dati critici di Server Dr.Web** durante l'aggiornamento (di default è *<disco_di_installazione>*:\DrWeb Backup).

Quando viene aggiornato un Server versione 6, vengono salvati i seguenti file di configurazione:

File	Descrizione
agent.key (il nome può essere diverso)	chiave di licenza di Agent
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
drwcsd.conf (il nome può essere diverso)	file di configurazione del Server
dbinternal.dbs	database incorporato
drwcsd.pri	chiave di cifratura privata
drwcsd.pub	chiave di cifratura pubblica
enterprise.key (il nome può essere diverso)	chiave di licenza di Server
webmin.conf	file di configurazione del Pannello di controllo

Quando viene aggiornato un Server versione 10, vengono salvati i seguenti file di configurazione:

File	Descrizione
agent.key (il nome può essere diverso)	chiave di licenza di Agent

File	Descrizione
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
enterprise.key (il nome può essere diverso)	chiave di licenza di Server. Viene mantenuta soltanto se era presente dopo l'aggiornamento dalle versioni precedenti. Se viene installato il nuovo Server 12.0, è assente
drwcsd.conf (il nome può essere diverso)	file di configurazione del Server
drwcsd.conf.distr	modello di file di configurazione di Server con i parametri di default
drwcsd.pri	chiave di cifratura privata
drwcsd.pub	chiave di cifratura pubblica
download.conf	impostazioni di rete per la generazione dei pacchetti di installazione di Agent
frontdoor.conf	file di configurazione per l'utility di diagnostica remota di Server
webmin.conf	file di configurazione del Pannello di controllo
openssl.cnf	certificato del Server per HTTPS

Quando viene aggiornato il Server dalla versione 11 e all'interno della versione 12, vengono salvati i seguenti file di configurazione:

File	Descrizione
agent.key (il nome può essere diverso)	chiave di licenza di Agent
auth-ads.conf	file di configurazione per l'autenticazione esterna degli amministratori attraverso Active Directory
auth-radius.conf	file di configurazione per l'autenticazione esterna degli amministratori attraverso RADIUS
auth-ldap.conf	file di configurazione per l'autenticazione esterna degli amministratori attraverso LDAP

File	Descrizione
`auth-ldap-rfc4515.conf`	file di configurazione dell'autenticazione esterna degli amministratori attraverso LDAP in base a uno schema semplificato
`auth-ldap-rfc4515-check-group.conf`	modello di file di configurazione dell'autenticazione esterna degli amministratori attraverso LDAP in base a uno schema semplificato con la verifica dell'appartenenza al gruppo di Active Directory
`auth-ldap-rfc4515-check-group-novar.conf`	modello di file di configurazione dell'autenticazione esterna degli amministratori attraverso LDAP in base a uno schema semplificato con la verifica dell'appartenenza al gruppo di Active Directory con l'uso delle variabili
`auth-ldap-rfc4515-simple-login.conf`	modello di file di configurazione dell'autenticazione esterna degli amministratori attraverso LDAP in base a uno schema semplificato
`auth-pam.conf`	file di configurazione per l'autenticazione esterna degli amministratori attraverso PAM
`enterprise.key` (il nome può essere diverso)	chiave di licenza di Server. Viene mantenuta soltanto se era presente dopo l'aggiornamento dalle versioni precedenti. Se viene installato il nuovo Server 12.0, è assente
`drwcsd-certificate.pem`	certificato Server
`download.conf`	impostazioni di rete per la generazione dei pacchetti di installazione di Agent
`drwcsd.conf` (il nome può essere diverso)	file di configurazione del Server
`drwcsd.conf.distr`	modello di file di configurazione di Server con i parametri di default
`drwcsd.pri`	chiave di cifratura privata
`dbexport.gz`	esportazione del database
`drwcsd.pub`	chiave di cifratura pubblica
`frontdoor.conf`	file di configurazione per l'utility di diagnostica remota di Server
`openssl.cnf`	certificato del Server per HTTPS
`webmin.conf`	file di configurazione del Pannello di controllo
`yalocator.apikey`	Chiave API per l'Estensione Yandex.Locator

Se si prevede di utilizzare i file di configurazione dal Server versione 6, notare:

1. La chiave di licenza di Server non viene più utilizzata (v. p. Concessione delle licenze).
2. Il database incorporato viene aggiornato e il file di configurazione di Server viene convertito per mezzo dell'installer. Questi file non possono essere sostituiti con le copie salvate automaticamente durante il passaggio dal Server versione 6.

Se necessario, salvare altri file importanti in un percorso diverso dalla directory di installazione del Server, per esempio, modelli di 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 `SQLite`.

Prima di aggiornare, assicurarsi che nel DBMS Microsoft SQL sia indicato l'ordinamento case-sensitive (suffisso `_CS`) e diacritico (suffisso `_AS`). In caso contrario, l'aggiornamento automatico non sarà possibile.

Prima di aggiornare, assicurarsi inoltre che il DBMS utilizzato sia supportato dal Server Dr.Web versione 12. In caso contrario, l'aggiornamento automatico non sarà possibile. La lista dei DBMS supportati è riportata nel documento **Allegati**, in Allegato B. Impostazioni per l'utilizzo di DBMS. Parametri dei driver di DBMS.

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

Per salvare il database

1. Arrestare 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, eseguire il file del pacchetto. I passaggi successivi dipendono dalla versione che viene aggiornata.

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

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

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

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

Se viene aggiornato dalla versione 6

1. 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**.
2. Si apre una finestra con le informazioni sul prodotto e con il testo del contratto di licenza. Dopo aver letto le condizioni del Contratto di licenza, per continuare l'aggiornamento, spuntare il flag **Accetto le condizioni del Contratto di licenza** e premere il pulsante **Avanti**.
3. Nei passaggi successivi il Server viene configurato in modo simile al processo di Installazione di Server Dr.Web in base ai file di configurazione dalla versione precedente. L'installer determina automaticamente la directory di installazione di Server, la posizione dei file di configurazione e del database incorporato dall'installazione precedente. Se necessario, è possibile modificare i percorsi dei file che sono stati trovati automaticamente dall'installer.
4. Per iniziare la rimozione del Server versione precedente e l'installazione del Server versione 12.0 premere il pulsante **Installa**.

   Durante la rimozione di Server i file di configurazione vengono salvati automaticamente nella directory <*disco_di_installazione*>:\DrWeb Backup.

Se viene aggiornato dalla versione 10.0

1. 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**.
2. Si apre una finestra con le informazioni sul prodotto e con il testo del contratto di licenza. Dopo aver letto le condizioni del Contratto di licenza, per continuare l'aggiornamento, spuntare il flag **Accetto le condizioni del Contratto di licenza** e premere il pulsante **Avanti**.
3. Nei passaggi successivi il Server viene configurato in modo simile al processo di Installazione di Server Dr.Web in base ai file di configurazione dalla versione precedente. L'installer determina automaticamente la directory di installazione di Server, la posizione dei file di configurazione e del database incorporato dall'installazione precedente. Se necessario, è possibile modificare i percorsi dei file che sono stati trovati automaticamente dall'installer.
4. Per iniziare la rimozione del Server versione precedente e l'installazione del Server versione 12.0 premere il pulsante **Installa**.
5. Durante l'aggiornamento si aprirà una finestra di configurazione del backup dei dati critici prima della rimozione del Server versione precedente. È consigliabile impostare il flag **Salva backup dei dati critici di Server Dr.Web**. Se necessario, è possibile modificare la directory per il backup impostata di default (<*disco_di_installazione*>:\DrWeb Backup).

Se viene aggiornato dalle versioni 10.0.1, 10.1, 11 e all'interno della versione 12

1. 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**.
2. Si aprirà una finestra di configurazione del backup dei dati critici prima della rimozione del Server versione precedente. È consigliabile impostare il flag **Salva backup dei dati critici di Server Dr.Web**. Se necessario, è possibile modificare la directory per il backup impostata di default (<*disco_di_installazione*>:\DrWeb Backup). Per iniziare il processo di rimozione della versione precedente di Server, premere **Rimuovi**.
3. Una volta completata la rimozione della versione precedente di Server, inizia l'installazione della versione nuova. Si apre una finestra con informazioni sul prodotto e con un link al testo del contratto di licenza. Dopo aver letto le condizioni del contratto di licenza, per continuare l'aggiornamento, spuntare il flag **Accetto le condizioni del Contratto di licenza** e premere il pulsante **Avanti**.
4. Nei passaggi successivi il Server viene configurato in modo simile al processo di Installazione di Server Dr.Web in base ai file di configurazione dalla versione precedente. L'installer determina automaticamente la directory di installazione di Server, la posizione dei file di configurazione e del database incorporato dall'installazione precedente. Se necessario, è possibile modificare i percorsi dei file che sono stati trovati automaticamente dall'installer.
5. Per iniziare il processo di installazione del Server versione 12.0, premere il pulsante **Installa**.

Finito l'aggiornamento dei Server della rete antivirus, è necessario:

1. 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).
2. Cancellare la cache del browser utilizzato per la connessione al Pannello di controllo.

7.2. Aggiornamento di Server Dr.Web per SO della famiglia UNIX

L'aggiornamento del Server alla versione 12.0 dipende dalla versione di partenza:

- L'aggiornamento dalla versione 6.0.4 alla versione 12.0 viene effettuato solo manualmente.
- Non in tutti i sistemi operativi della famiglia UNIX è possibile aggiornare dalle versioni 10.X alla versione 12.0 automaticamente tramite l'installer sopra la versione installata. Pertanto, nei sistemi operativi della famiglia UNIX in cui l'aggiornamento automatico sopra il pacchetto già installato non è possibile, è necessario effettuare l'aggiornamento manualmente.
- L'aggiornamento di Server dalle versioni 11.X e all'interno della versione 12.0 per i tipi di pacchetti uguali viene eseguito automaticamente tramite l'installer per tutti i sistemi operativi della famiglia UNIX. Se lo si desidera, è anche possibile effettuare l'aggiornamento manualmente.
- L'aggiornamento di Server dalle versioni 11.X alla versione 12.0 è inoltre disponibile 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.

Quando viene aggiornato il Server Dr.Web sotto i sistemi operativi della famiglia UNIX dalla versione 10 e precedenti, le impostazioni della sezione del Pannello di controllo **Configurazione del web server** (il file `webmin.conf`) non verranno trasferite nella versione 12.

Le impostazioni in questa sezione verranno resettate ai valori di default. Se si vogliono utilizzare le impostazioni della versione precedente, configurarle manualmente dopo l'aggiornamento di Server nella sezione corrispondente del Pannello di controllo sulla base dei dati da una copia di backup del file di configurazione.

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

Prima dell'inizio dell'aggiornamento del Server prestare attenzione alla sezione Aggiornamento di Agent Dr.Web.

L'aggiornamento di Server all'interno della versione 12 può inoltre 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 12 contengono un file di pacchetto. Alcuni di essi possono essere installati solo tramite il Pannello di controllo.

Salvataggio dei file di configurazione

Quando il Server viene rimosso e aggiornato automaticamente alla versione 12, i file di configurazione vengono salvati nella directory impostata per il backup di default: `/var/tmp/drwcs/`.

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

File	Descrizione
`agent.key` (il nome può essere diverso)	chiave di licenza di Agent
`certificate.pem`	certificato per SSL
`common.conf`	file di configurazione (per alcuni SO della famiglia UNIX)
`dbinternal.dbs`	database incorporato
`drwcsd.conf` (il nome può essere diverso)	file di configurazione del Server
`drwcsd.pri`	chiave di cifratura privata
`drwcsd.pub`	chiave di cifratura pubblica
`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

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

File	Descrizione
`agent.key` (il nome può essere diverso)	chiave di licenza di Agent

File	Descrizione
auth-ldap.xml	file di configurazione per l'autenticazione esterna degli amministratori attraverso LDAP
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
certificate.pem	certificato per SSL
common.conf	file di configurazione (per alcuni SO della famiglia UNIX)
dbexport.gz	esportazione del database (viene creato nel processo di rimozione del Server dal comando drwcs.sh xmlexportdb)
download.conf	impostazioni di rete per la generazione dei pacchetti di installazione di Agent
drwcsd.conf (il nome può essere diverso)	file di configurazione del Server
drwcsd.pri	chiave di cifratura privata
drwcsd.pub	chiave di cifratura pubblica
enterprise.key (il nome può essere diverso)	chiave di licenza di Server. Viene mantenuta soltanto se era presente dopo l'aggiornamento dalle versioni precedenti. Se viene installato il nuovo Server 12.0, è assente
frontdoor.conf	file di configurazione per l'utility di diagnostica remota di Server
local.conf	impostazioni del log di Server
private-key.pem	chiave privata RSA
webmin.conf	file di configurazione del Pannello di controllo
*.dbs *.sqlite	database incorporato

Quando viene rimosso un Server versioni 11 e 12, vengono salvati i seguenti file di configurazione:

File	Descrizione
agent.key (il nome può essere diverso)	chiave di licenza di Agent

File	Descrizione
auth-ldap.conf	file di configurazione per l'autenticazione esterna degli amministratori attraverso LDAP
auth-ldap-rfc4515.conf	file di configurazione dell'autenticazione esterna degli amministratori attraverso LDAP in base a uno schema semplificato
auth-pam.conf	file di configurazione per l'autenticazione esterna degli amministratori attraverso PAM
auth-radius.conf	file di configurazione per l'autenticazione esterna degli amministratori attraverso RADIUS
certificate.pem	certificato per SSL
common.conf	file di configurazione (per alcuni SO della famiglia UNIX)
dbexport.gz	esportazione del database (viene creato nel processo di rimozione del Server dal comando drwcs.sh xmlexportdb)
download.conf	impostazioni di rete per la generazione dei pacchetti di installazione di Agent
drwcsd-certificate.pem	certificato Server
drwcsd.conf (il nome può essere diverso)	file di configurazione del Server
drwcsd.pri	chiave di cifratura privata
drwcsd.pub	chiave di cifratura pubblica
enterprise.key (il nome può essere diverso)	chiave di licenza di Server. Viene mantenuta soltanto se era presente dopo l'aggiornamento dalle versioni precedenti. Se viene installato il nuovo Server 12.0, è assente
frontdoor.conf	file di configurazione per l'utility di diagnostica remota di Server
local.conf	impostazioni del log di Server
private-key.pem	chiave privata RSA
webmin.conf	file di configurazione del Pannello di controllo
yalocator.apikey	Chiave API per l'Estensione Yandex.Locator

Nel caso di aggiornamento automatico nella directory per il backup vengono salvati i seguenti file:

Per il Server versione 10:

File	Descrizione
`auth-ldap.xml`	file di configurazione per l'autenticazione esterna degli amministratori attraverso LDAP
`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
`db.backup.gz`	esportazione del database (viene creato nel processo di aggiornamento del Server dal comando `drwcs.sh exportdb`)

Per il Server versioni 11 e 12:

File	Descrizione
`auth-ldap.conf`	file di configurazione per l'autenticazione esterna degli amministratori attraverso LDAP
`auth-ldap-rfc4515.conf`	file di configurazione dell'autenticazione esterna degli amministratori attraverso LDAP in base a uno schema semplificato
`auth-pam.conf`	file di configurazione per l'autenticazione esterna degli amministratori attraverso PAM
`auth-radius.conf`	file di configurazione per l'autenticazione esterna degli amministratori attraverso RADIUS
`db.backup.gz`	esportazione del database (viene creato nel processo di aggiornamento del Server dal comando `drwcs.sh exportdb`)

Se si prevede di utilizzare i file di configurazione dal Server versione 6, notare:

1. La chiave di licenza di Server non viene più utilizzata (v. p. Concessione delle licenze).
2. Il database incorporato viene aggiornato e il file di configurazione di Server viene convertito per mezzo dell'installer. Questi file non possono essere sostituiti con le copie salvate automaticamente durante il passaggio dal Server versione 6.

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 exportdb /var/tmp/esbase.es
     ```
   - In caso di SO Linux:
     ```
     # /etc/init.d/drwcsd exportdb /var/tmp/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

Nel caso di aggiornamento del Server dalla versione 10 alla versione 12 (ad eccezione dei Server installati sotto SO **Linux** e installati dai pacchetti `*.rpm.run` e `*.deb.run`), invece della rimozione della versione vecchia del Server e dell'installazione della versione nuova, è possibile l'aggiornamento di pacchetto automatico. Per tale scopo, avviare l'installazione del relativo pacchetto Server.

L'aggiornamento di Server dalla versione 11 e all'interno della versione 12 per i tipi di pacchetti uguali viene eseguito automaticamente per tutti i sistemi operativi della famiglia UNIX.

In questo caso i file di configurazione verranno convertiti automaticamente e collocati nelle directory richieste. Inoltre, alcuni file di configurazione vengono salvati nella directory per il backup.

Aggiornamento manuale

Nel caso in cui non è possibile aggiornare il Server versione 6.0.4 o successive sopra un pacchetto già installato, è necessario rimuovere il software Server delle versioni precedenti salvando una copia di backup, e installare il software versione 12 sulla base della copia di backup salvata.

Per aggiornare Server Dr.Web

1. Arrestare il Server.
2. Se si vogliono utilizzare in seguito alcuni file (oltre ai file che verranno salvati in automatico nel processo di rimozione del Server nel passaggio **3**), creare i backup di questi file manualmente, per esempio, i modelli di report ecc.
3. Rimuovere il software Server (v. p. Rimozione di Server Dr.Web per SO della famiglia UNIX). Verrà automaticamente chiesto di salvare copie di backup dei file. A tale scopo, basta inserire il percorso per il salvataggio o accettare il percorso proposto di default.
4. Installare il Server Dr.Web versione 12.0 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 nel passaggio **3)**. Tutti i file di configurazione salvati e il database incorporato (nel caso di utilizzo del database incorporato) verranno convertiti automaticamente per l'uso dal Server versione 12.0. Senza la conversione automatica non è possibile utilizzare il database (nel caso di utilizzo del database incorporato) 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 dalla versione precedente del Server salvati (vedi passaggio 4) è necessario impostare come proprietario di file l'utente selezionato durante l'installazione della nuova versione del Server (di default è **drwcs**).

5. Avviare il Server.
6. Configurare l'aggiornamento del repository ed aggiornarlo completamente.

   

   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).

7.3. 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 di Agent Dr.Web per le postazioni SO Android,
3. Aggiornamento di Agent Dr.Web per le postazioni SO Linux e macOS.

7.3.1. Aggiornamento di Agent Dr.Web per le postazioni SO Windows

Aggiornamento degli Agent forniti con Dr.Web Enterprise Security Suite 10

L'aggiornamento degli Agent forniti con la versione Enterprise Security Suite 10 viene eseguito in modo automatico.

Dopo l'aggiornamento automatico viene visualizzato un avviso pop-up di necessità di riavvio; nel Pannello di controllo nello status della postazione viene segnata la necessità di riavvio dopo l'aggiornamento. Per completare l'aggiornamento, riavviare la postazione localmente o in remoto attraverso il Pannello di controllo.

Se la postazione si connette al Server attraverso Server proxy Dr.Web versione 10 o precedenti, prima dell'aggiornamento dell'Agent è necessario aggiornare il Server proxy alla versione 12 o rimuovere il Server proxy.

Aggiornamento automatico degli Agent forniti con Dr.Web Enterprise Security Suite 6

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

1. Gli Agent devono essere installati sui computer gestiti dai sistemi operativi della famiglia Windows supportati per l'installazione degli Agent per Dr.Web Enterprise Security Suite versione 12.0 (v. documento **Allegati**, p. Allegato A. Lista completa delle versioni supportate dei sistemi operativi).
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 visualizzato un avviso 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 visualizzato un avviso di necessità di riavvio. È necessario riavviare la postazione.

Aggiornamento manuale degli Agent forniti con Dr.Web Enterprise Security Suite 6

Se l'installazione di nuova versione di Agent durante un aggiornamento automatico non è riuscita per qualche ragione, non ci saranno altri tentatici 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 su postazioni con sistemi operativi non supportati per l'installazione di Agent per Dr.Web Enterprise Security Suite versione 12.0, non verrà eseguita nessuna azione 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 la disponibilità degli Agent sotto i SO non supportati è necessaria, si devono lasciare nella rete antivirus i Server delle versioni precedenti a cui sono connessi questi Agent. In tale caso, i Server versioni 6 e i Server versione 12.0 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.

7.3.2. Aggiornamento di Agent Dr.Web per le postazioni SO Android

L'aggiornamento di Agent Dr.Web per Android per l'uso con Dr.Web Enterprise Security Suite versione 12.0 deve essere eseguito manualmente sui dispositivi mobili.

Dr.Web Enterprise Security Suite versione 12.0 supporta solo l'uso di Agent Dr.Web per Android versione 12.2 e successive.

Per aggiornare localmente Agent Dr.Web per Android, utilizzare uno dei seguenti metodi:

1. Se è possibile scaricare separatamente tramite internet il pacchetto di installazione della versione standalone di Agent.

   Prima dell'inizio dell'aggiornamento del Server Dr.Web, aggiornare manualmente gli Agent Dr.Web per Android sui dispositivi mobili alla versione 12.2 o successive. La nuova versione può essere scaricata dal sito dell'azienda Doctor Web sull'indirizzo: https://download.drweb.com/android/. Il nuovo Agent si connetterà al Server della versione precedente, dopodiché il Server può essere aggiornato alla versione 12.0 secondo la procedura generale.
2. Se non è possibile scaricare separatamente tramite internet il pacchetto di installazione della versione standalone di Agent.

   Dopo l'aggiornamento del Server Dr.Web gli Agent Dr.Web per Android si connetteranno in automatico al Server aggiornato. Dopo un tentativo di aggiornamento la protezione sui dispositivi mobili verrà disattivata a causa dell'errore di versione incompatibile dei database. Aggiornare manualmente gli Agent direttamente sui dispositivi mobili. Il pacchetto di

installazione della nuova versione di Agent può essere scaricato nel Pannello di controllo nelle proprietà della postazione o sulla pagina di installazione.

3. Se non è possibile scaricare separatamente tramite internet il pacchetto di installazione della versione standalone di Agent e si vuole evitare la comparsa di un errore di aggiornamento sul dispositivo mobile.

   Prima di aggiornare il Server, disconnettere da esso gli Agent Dr.Web per Android. In questo caso i dispositivi mobili non potranno connettersi al nuovo Server per il download di aggiornamenti incompatibili. Aggiornare il Server alla versione 12.0 secondo la procedura generale. Scaricare il pacchetto di installazione della nuova versione di Agent nel Pannello di controllo nelle proprietà della postazione o sulla pagina di installazione. Aggiornare manualmente gli Agent sui dispositivi mobili. Connettere gli Agent aggiornati al nuovo Server.

7.3.3. Aggiornamento di Agent Dr.Web per le postazioni SO Linux e macOS

Gli Agent installati sulle postazioni con i sistemi operativi della famiglia Linux e con macOS si connetteranno al Server versione 12.0 se sono soddisfatte le seguenti condizioni:

1. Gli Agent devono essere installati sui computer gestiti dai sistemi operativi supportati per l'installazione degli Agent per Dr.Web Enterprise Security Suite versione 12.0 (v. documento **Allegati**, p. Allegato A. Lista completa delle versioni supportate dei sistemi operativi).
2. Sulle postazioni devono essere impostate le chiavi di cifratura e le impostazioni di rete del Server aggiornato.

Dopo la connessione delle postazioni al Server aggiornato:

1. Sulle postazioni vengono aggiornati solo i database dei virus. L'aggiornamento automatico del software antivirus stesso non viene eseguito.
2. Se sulle postazioni è installata l'ultima versione del software, nessuna ulteriore azione è necessaria.
3. Se il software sulle postazioni non è aggiornato, scaricare il pacchetto di installazione della nuova versione di Agent nel Pannello di controllo nelle proprietà della postazione o sulla pagina di installazione. Aggiornare il software delle postazioni manualmente, come descritto nei relativi **Manuali utente**.

7.4. Aggiornamento del Server proxy Dr.Web

7.4.1. Aggiornamento del Server proxy Dr.Web durante il funzionamento

L'aggiornamento del Server proxy può essere eseguito automaticamente durante il funzionamento.

Se il Server Dr.Web sotto SO della famiglia UNIX è stato precedentemente aggiornato dalla versione 11.0 o 11.0.1, l'aggiornamento automatico del Server proxy Dr.Web sarà impossibile. Per togliere questa restrizione, è necessario nella sezione **Amministrazione → Configurazione dettagliata del repository → Server proxy Dr.Web → Sincronizzazione** nel campo **Aggiorna soltanto i seguenti file** rimuovere manualmente il suffisso `^win.*`.

Nel caso di installazione iniziale del Server Dr.Web versione 11.0.2 le restrizioni sull'aggiornamento automatico del Server proxy non vengono imposte.

Il calendario di aggiornamento dipende dalle impostazioni di memorizzazione in cache proattiva del Server proxy:

1. Se il Server proxy non è incluso nella lista per la memorizzazione in cache proattiva (anche nel caso in cui la memorizzazione nella cache non viene utilizzata), gli aggiornamenti del Server proxy verranno scaricati e installati secondo il calendario di aggiornamento automatico.
2. Se il Server proxy è incluso nella lista per la memorizzazione in cache proattiva, gli aggiornamenti del Server proxy verranno scaricati secondo il calendario di memorizzazione in cache proattiva. Nel caso di ricezione di una nuova revisione del Server proxy, l'aggiornamento a questa revisione avverrà secondo il calendario di aggiornamento automatico.

L'aggiornamento automatico può essere configurato in uno dei seguenti modi:

- Attraverso le impostazioni di Server proxy nel Pannello di controllo del Server di gestione nella sezione **Aggiornamenti**. La descrizione dettagliata è riportata nel documento **Manuale dell'amministratore**, sezione Configurazione del Server proxy in remoto.
- Attraverso il file di configurazione di Server proxy `drwcsd-proxy.conf`. La descrizione dettagliata è riportata nel documento **Allegati**, p. Allegato G4.

7.4.2. Aggiornamento del Server proxy Dr.Web attraverso l'installer

I file di configurazione del Server proxy

Il file di configurazione del Server proxy versione 10 o precedenti:

File	Descrizione
`drwcsd-proxy.xml`	file di configurazione del Server proxy (vedere documento **Allegati**, p. Allegato G4)

I file di configurazione del Server proxy versione 11 o successive:

File	Descrizione
`drwcsd-proxy.conf`	file di configurazione del Server proxy (vedere documento **Allegati**, p. Allegato G4)
`drwcsd-proxy.auth`	dati di identificazione (l'ID e la password) per l'accesso ai Server Dr.Web
`drwcsd-proxy-trusted.list`	lista dei certificati affidabili dei Server Dr.Web
`drwcsd-proxy-signed.list`	lista dei certificati firmati del Server proxy
`drwcsd-proxy.pri`	chiave di cifratura privata del Server proxy

Aggiornamento del Server proxy sotto il sistema operativo Windows

L'aggiornamento viene effettuato automaticamente per mezzo dell'installer.

Per aggiornare il Server proxy dalla versione 10 o precedenti

1. Avviare il file del pacchetto del Server proxy.
2. Si apre una finestra che avvisa del software Server proxy versione precedente installato e offre di aggiornarlo alla versione nuova. Per iniziare la rimozione della versione precedente e l'installazione della versione nuova, premere il pulsante **Upgrade**.
3. Si apre una finestra con informazioni sul prodotto. Premere il pulsante **Next**.
4. Nei passaggi successivi il Server proxy viene configurato in modo simile al processo di Installazione di Server proxy Dr.Web in base al file di configurazione dalla versione precedente. L'installer determina automaticamente la directory di installazione di Server proxy e la posizione

del file di configurazione dall'installazione precedente. Se necessario, è possibile modificare le impostazioni prese dal file, che sono state trovate automaticamente dall'installer.

5. Per iniziare il processo di installazione del Server proxy versione 12.0, premere il pulsante **Install**.

Per aggiornare il Server proxy dalla versione 11 o successive

1. Avviare il file del pacchetto del Server proxy.
2. Si apre una finestra che avvisa del software Server proxy versione precedente installato e offre di aggiornarlo alla versione nuova. Per iniziare a configurare la procedura di aggiornamento, premere il pulsante **Upgrade**.
3. Si apre una finestra con informazioni sulla rimozione del Server proxy versione precedente. Per iniziare il processo di rimozione, premere **Uninstall**.
4. Una volta completata la rimozione della versione precedente del Server proxy, inizierà l'installazione della versione nuova. Si apre una finestra con informazioni sul prodotto. Premere il pulsante **Next**.
5. Nei passaggi successivi il Server proxy viene configurato in modo simile al processo di Installazione di Server proxy Dr.Web in base ai file di configurazione dalla versione precedente. L'installer determina automaticamente la directory di installazione di Server proxy e la posizione dei file di configurazione dall'installazione precedente. Se necessario, è possibile modificare le impostazioni prese dai file, che sono state trovate automaticamente dall'installer.
6. Per iniziare il processo di installazione del Server proxy versione 12.0, premere il pulsante **Install**.

Aggiornamento del Server proxy sotto i sistemi operativi della famiglia UNIX

Per aggiornare il Server proxy dalla versione 11.0 o precedenti

Quando viene aggiornato il Server proxy, vengono rimossi i file di configurazione. Se necessario, salvare i file di configurazione manualmente prima di iniziare l'aggiornamento.

1. Per avviare il processo di aggiornamento, eseguire il file del pacchetto del Server proxy: `./<file_del_pacchetto>.tar.gz.run`
2. Dopo il completamento dell'aggiornamento, se necessario, portare manualmente nei nuovi file di configurazione le impostazioni dai file di configurazione salvati prima dell'inizio dell'aggiornamento.

Per aggiornare il Server proxy dalla versione 11.0.1

1. Per avviare il processo di aggiornamento, eseguire il file del pacchetto del Server proxy: `./<file_del_pacchetto>.tar.gz.run`

2. Durante la rimozione della versione precedente verranno automaticamente salvati i file di configurazione del Server proxy.
3. Durante il processo di aggiornamento verrà offerto di utilizzare i file di configurazione da un'installazione precedente del Server proxy salvati tramite il backup:
   - Per utilizzare una copia di backup memorizzata di default nella directory `/var/tmp/drwcsd-proxy`, premere INVIO.
   - Per utilizzare una copia di backup da un'altra directory, inserire manualmente il percorso della copia di backup.
   - È inoltre possibile installare il Server proxy con le impostazioni predefinite, senza utilizzare una copia di backup della configurazione da un'installazione precedente. Per fare ciò, premere 0.

Indice analitico

Indice analitico

R

S

T