



Dr.WEB®

Enterprise Security Suite

Defend what you create

Manuale dell'amministratore

© 2004-2015 Doctor Web. Tutti i diritti riservati

Materiali, riportati in questo documento, sono di proprietà di Doctor Web e si possono utilizzare esclusivamente per uso personale dell'acquirente del prodotto. Nessuna parte di tale può essere copiata, riprodotta su una risorsa di rete o trasmessa per canali di comunicazione o via mass media o utilizzata in altro modo oltre uso personale, se non facendo riferimento alla fonte.

MARCHI

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

LIMITAZIONE DI RESPONSABILITÀ

Doctor Web e i suoi fornitori sono in ogni caso esenti di qualsiasi responsabilità per errori e/o omissioni, presenti nel presente documento, e per danni (diretti o indiretti, incluso un profitto perso) causati da essi all'acquirente del prodotto.

Dr.Web Enterprise Security Suite
Versione 10.0
Manuale dell'amministratore
02.09.2015

Doctor Web, Sede centrale in Russia
125124
Russia, Mosca,
via 3 Yamskogo Polya, tenuta 2, edificio 12A

Sito web: www.drweb.com
Telefono: +7 (495) 789-45-87

Le informazioni sulle sedi rappresentative si trovano sul sito ufficiale dell'azienda.

Doctor Web

Doctor Web è uno sviluppatore russo di sistemi di sicurezza informatica.

Doctor Web offre valide soluzioni di protezione antivirus e antispam per enti pubblici, aziende e utenti privati.

I programmi antivirali della famiglia Dr.Web vengono sviluppati a partire dal 1992, sempre raggiungono i migliori risultati nel rilevamento di malware e corrispondono agli standard internazionali di sicurezza.

I certificati e premi conferiti ai prodotti Dr.Web provano il loro avanzato grado di affidabilità. Gli utenti di Dr.Web si trovano in diverse parti del mondo.

Ringraziamo i nostri utenti per la fiducia che hanno nelle soluzioni della famiglia Dr.Web!



Sommario

Capitolo 1: Antivirus Dr.Web Enterprise Security Suite	8
1.1. Introduzione	8
1.2. Segni convenzionali e abbreviazioni	9
1.3. Sul prodotto	10
1.4. Requisiti di sistema	16
1.5. Set di fornitura	20
1.6. Concessione delle licenze	21
Capitolo 2: Componenti della rete antivirus e la loro interfaccia	23
2.1. Server Dr.Web	23
2.1.1. Gestione del Server Dr.Web sotto SO Windows®	24
2.1.2. Gestione del Server Dr.Web sotto SO della famiglia UNIX®	26
2.2. Agent Dr.Web	29
2.3. Pannello di controllo della sicurezza Dr.Web	30
2.3.1. Amministrazione	33
2.3.2. Rete antivirus	34
2.3.3. Relazioni	39
2.3.4. Impostazioni	40
2.3.5. Guida	43
2.4. Componenti del Pannello di controllo della sicurezza Dr.Web	44
2.4.1. Scanner di rete	44
2.4.2. Gestione licenze	47
2.5. Schema interazione dei componenti della rete antivirus	54
Capitolo 3: Introduzione all'uso. Generalità	58
3.1. Creazione di una rete antivirus semplice	58
3.2. Configurazione delle connessioni di rete	59
3.2.1. Connessioni dirette	60
3.2.2. Servizio di rilevamento di Server Dr.Web	61
3.2.3. Utilizzo del protocollo SRV	61
Capitolo 4: Amministratori della rete antivirus	63
4.1. Autenticazione di amministratori	63
4.1.1. Autenticazione di amministratori del Server database	64
4.1.2. Autenticazione con utilizzo di Active Directory	64
4.1.3. Autenticazione con utilizzo di LDAP	65



4.1.4. Autenticazione con utilizzo di RADIUS	66
4.1.5. Autenticazione con utilizzo di PAM	67
4.2. Amministratori e gruppi di amministratori	68
4.3. Gestione degli account amministratori e dei gruppi di amministratori	70
4.3.1. Creazione ed eliminazione di account amministratori e di gruppi	70
4.3.2. Modifica di account amministratori e di gruppi	72
Capitolo 5: Gestione integrata delle postazioni	75
5.1. Gruppi di sistema e custom	75
5.2. Gestione dei gruppi	78
5.2.1. Creazione ed eliminazione di gruppi	78
5.2.2. Modifica dei gruppi	78
5.3. Sistemazione delle postazioni in gruppi custom	80
5.3.1. Sistemazione manuale delle postazioni in gruppi	80
5.3.2. Configurazione dell'appartenenza automatica a un gruppo	81
5.4. Utilizzo dei gruppi per configurare postazioni	82
5.4.1. Ereditarietà della configurazione da parte della postazione	83
5.4.2. Copiatura delle impostazioni in altri gruppi/postazioni	85
5.5. Comparazione delle postazioni e dei gruppi	85
Capitolo 6: Gestione delle postazioni	86
6.1. Gestione degli account di postazioni	86
6.1.1. Criteri di approvazione delle postazioni	86
6.1.2. Rimozione e recupero della postazione	87
6.1.3. Unione delle postazioni	88
6.2. Impostazioni generali della postazione	89
6.2.1. Proprietà della postazione	89
6.2.2. Componenti installati del pacchetto antivirus	92
6.2.3. Hardware e software sulle postazioni SO Windows®	93
6.3. Configurazione delle impostazioni della postazione	94
6.3.1. Permessi dell'utente della postazione	94
6.3.2. Calendario dei task della postazione	96
6.3.3. Componenti da installare del pacchetto antivirus	100
6.4. Configurazione dei componenti antivirus	101
6.4.1. Componenti	102
6.4.2. Configurazione di Agent Dr.Web per Windows®	104
6.4.3. Configurazione di SpIDer Mail per Windows®. Filtro delle applicazioni	110
6.5. Scansione antivirus delle postazioni	111



6.5.1. Visualizzazione ed interruzione dell'esecuzione dei componenti	112
6.5.2. Interruzione dell'esecuzione dei componenti per tipo	113
6.5.3. Avvio della scansione della postazione	113
6.5.4. Configurazione dello Scanner	114
6.6. Visualizzazione delle statistiche della postazione	120
6.6.1. Statistiche	120
6.6.2. Grafici	123
6.6.3. Quarantena	125
6.7. Invio dei file d'installazione	126
6.8. Invio di messaggi alle postazioni SO Windows®	128
Capitolo 7: Configurazione del Server Dr.Web	131
7.1. Log	131
7.1.1. Log di funzionamento di Server Dr.Web	131
7.2. Configurazione del Server Dr.Web	132
7.2.1. Generali	133
7.2.2. DNS	137
7.2.3. Statistiche	137
7.2.4. Sicurezza	139
7.2.5. Cache	140
7.2.6. Database	140
7.2.7. Proxy	142
7.2.8. Trasporto	142
7.2.9. Moduli	143
7.2.10. Cluster	143
7.2.11. Posizione	144
7.2.12. Download	144
7.2.13. Aggiornamenti per gruppi	145
7.2.14. Licenze	146
7.3. Accesso remoto al Server Dr.Web	146
7.4. Configurazione del calendario di Server Dr.Web	147
7.5. Configurazione del web server	154
7.5.1. Generali	154
7.5.2. Avanzate	155
7.5.3. Trasporto	156
7.5.4. Sicurezza	156
7.6. Procedure personalizzate	157



7.7. Configurazione degli avvisi	158
7.7.1. Configurazione degli avvisi	158
7.7.2. Avvisi nella console web	162
7.7.3. Avvisi non inviati	163
7.8. Gestione del repository di Server Dr.Web	163
7.8.1. Stato del repository	165
7.8.2. Aggiornamenti differiti	165
7.8.3. Configurazione generale del repository	166
7.8.4. Configurazione dettagliata del repository	168
7.8.5. Contenuti del repository	171
7.9. Possibilità aggiuntive	173
7.9.1. Gestione del database	173
7.9.2. Statistiche di Server Dr.Web	175
7.9.3. Copie di backup	176
7.10. Caratteristiche di una rete con diversi Server Dr.Web	177
7.10.1. Struttura di una rete con diversi Server Dr.Web	177
7.10.2. Configurazione delle relazioni tra i Server Dr.Web	179
7.10.3. Utilizzo di una rete antivirus con diversi Server Dr.Web	183
7.10.4. Utilizzo di un database unico da parte di diversi Server Dr.Web	185
Capitolo 8: Aggiornamento dei componenti di Dr.Web Enterprise Security Suite	186
8.1. Aggiornamento di Server Dr.Web e ripristino da copia di backup	186
8.2. Aggiornamento manuale dei componenti di Dr.Web Enterprise Security Suite	188
8.3. Aggiornamenti programmati	188
8.4. Aggiornamento del repository di Server Dr.Web, non connesso a Internet	189
8.4.1. Copiatura del repository di un altro Server Dr.Web	189
8.4.2. Caricamento del repository da SAM	190
8.5. Limitazione degli aggiornamenti delle postazioni	194
8.6. Aggiornamento di Agent Dr.Web mobile	195
Capitolo 9: Configurazione dei componenti aggiuntivi	197
9.1. Server proxy	197
9.2. NAP Validator	200
Indice analitico	203



Capitolo 1: Antivirus Dr.Web Enterprise Security Suite

1.1. Introduzione

La documentazione dell'amministratore della rete antivirus **Dr.Web® Enterprise Security Suite** contiene le informazioni che descrivono principi generali e dettagli della realizzazione della protezione antivirus completa dei computer della società tramite **Dr.Web® Enterprise Security Suite** (di seguito brevemente denominato **Dr.Web ESS**).

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

1. **Guida all'installazione** (file **drweb-esuite-10-install-manual-it.pdf**)
2. **Manuale dell'amministratore** (file **drweb-esuite-10-admin-manual-it.pdf**)

Il manuale dell'amministratore è indirizzato *all'amministratore della rete antivirus* – dipendente della società responsabile della gestione della protezione antivirus dei computer (workstation e server) di questa rete.

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

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



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

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

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





1.2. Segni convenzionali e abbreviazioni

Segni convenzionali

Nel presente Manuale vengono utilizzati i segni riportati nella [tabella 1-1](#).

Tabella 1-1. Leggenda

Segno	Commento
 Notarsi che	Osservazione o indicazione importante.
 Attenzione	Avviso di eventuali situazioni di errore, nonché dei momenti importanti, a cui particolarmente prestare attenzione.
Dr.Web ESS	Denominazioni dei prodotti e dei componenti Dr.Web .
<i>Rete antivirus</i>	Termine nella posizione di definizione o in quella di riferimento a definizione.
<indirizzo_IP>	Campi per la sostituzione delle denominazioni funzionali con i valori effettivi.
Annulla	Nomi dei pulsanti dello schermo, delle finestre, delle voci del menu e degli altri elementi dell'interfaccia di programma.
CTRL	Nomi dei tasti della tastiera.
C:\Windows\	Nomi dei file e delle cartelle, frammenti di codice del programma.
Allegato A	Riferimenti incrociati a capitoli del documento o collegamenti ipertestuali a risorse esterne.

Abbreviazioni

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

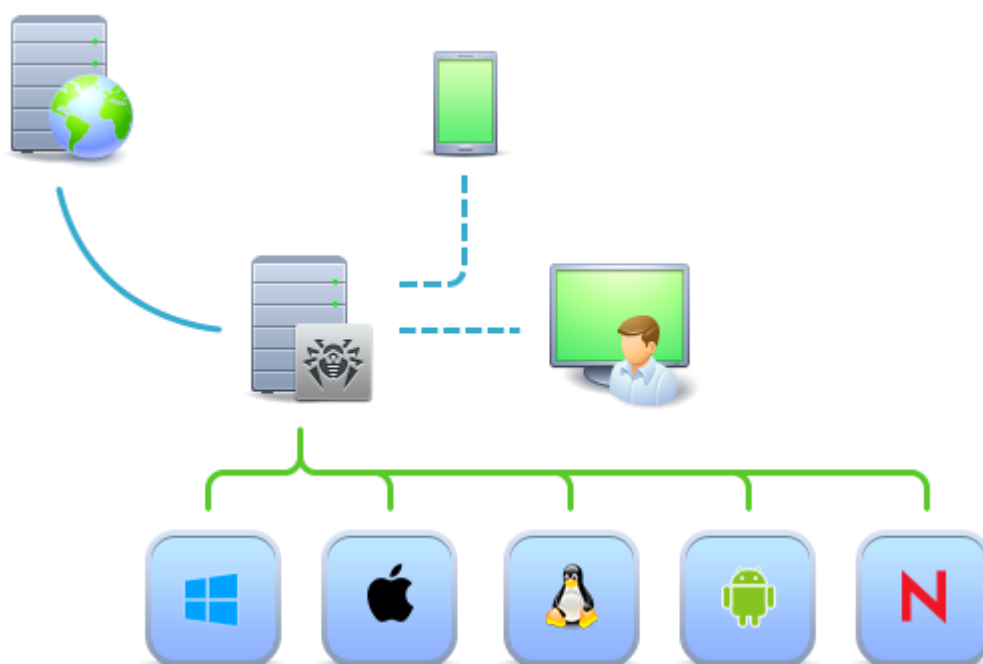
- ◆ ACL – lista di controllo degli accessi (Access Control List),
- ◆ CDN – rete di distribuzione di contenuti (Content Delivery Network),
- ◆ DFS – file system distribuito (Distributed File System),
- ◆ DNS – sistema dei nomi a dominio (Domain Name System),
- ◆ FQDN – nome di dominio completo (Fully Qualified Domain Name),
- ◆ **Dr.Web ESS – Dr.Web Enterprise Security Suite**,
- ◆ GUI – interfaccia utente grafica (Graphical User Interface), versione del programma con la GUI – una versione che utilizza gli strumenti della GUI,
- ◆ NAP – Network Access Protection,
- ◆ MTU – dimensione massima di un pacchetto dati (Maximum Transmission Unit),
- ◆ TTL – tempo di vita pacchetto (Time To Live),
- ◆ UDS – socket di dominio UNIX (UNIX Domain Socket),
- ◆ DB, DBMS – database, database management system,
- ◆ **SAM Dr.Web** – Sistema di aggiornamento mondiale di **Dr.Web**,
- ◆ LAN – rete locale,
- ◆ SO – sistema operativo,
- ◆ EBNF – forma estesa di Backus-Naur (Extended Backus-Naur form).

1.3. Sul prodotto

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

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

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.



Struttura logica della rete antivirus



Server di protezione centralizzata

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

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

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

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

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 installati sulle postazioni protette.

È possibile utilizzare i seguenti tipi di database:

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

- SQLite2 (InitDB),
- SQLite3.

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

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

Si può utilizzare qualsiasi database che corrisponda alle esigenze. La scelta deve essere basata sulle esigenze a cui deve rispondere il database, quali: possibilità di essere utilizzato da una rete antivirus della dimensione adatta, le caratteristiche di manutenzione del software database, le possibilità di amministrazione fornite dal database, nonché i requisiti e gli standard approvati ed utilizzati dall'azienda.

Pannello di controllo di protezione centralizzata

Il Pannello di controllo di protezione centralizzata viene installato automaticamente insieme al **Server** e fornisce un'interfaccia web utilizzata per gestire su remoto il **Server** e la rete antivirus modificando le impostazioni del **Server**, nonché le impostazioni dei computer protetti, conservate sul **Server** e sui computer protetti.

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

- Windows® Internet Explorer®,
- Mozilla® Firefox®,



- Google Chrome®.

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

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

- Comoda installazione dell'**Antivirus** su postazioni protette, è possibile: installare il software su remoto sulle postazioni SO Windows prima aver esaminato la rete per cercare computer; creare pacchetti con identificatori univoci e parametri di connessione al **Server** per semplificare il processo di installazione dell'**Antivirus** da parte dell'amministratore o per consentire agli utenti di installare l'**Antivirus** su postazioni in modo autonomo .
- Gestione semplificata delle postazioni di rete antivirus per il tramite del metodo di gruppi (per maggiori informazioni consultare la sezione [Capitolo 5: Gruppi. Gestione integrata delle postazioni](#)).
- 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 di pacchetti antivirus; assegnare i permessi di configurare e di gestire pacchetti antivirus dei computer protetti agli utenti di questi computer (per maggiori informazioni consultare la sezione [Capitolo 6: Gestione delle postazioni](#)).
- Gestione centralizzata della scansione antivirus di postazioni, in particolare, è possibile: avviare la scansione antivirus su remoto sia secondo un calendario prestabilito che su diretta richiesta dell'amministratore dal **Pannello di controllo**; configurare in modo centralizzato le impostazioni di scansione antivirus, trasmesse su postazioni per eseguire in seguito una scansione locale con queste impostazioni (per maggiori informazioni consultare la sezione [Scansione antivirus delle postazioni](#)).
- Possibilità di ricevere le informazioni statistiche sullo stato delle postazioni protette, le statistiche sui virus, le informazioni sullo stato del software antivirus installato, sullo stato dei componenti antivirus in esecuzione, nonché l'elenco dell'hardware e del software della postazione protetta (per maggiori informazioni consultare la sezione [Visualizzazione delle statistiche della postazione](#)).
- Sistema flessibile dell'amministrazione del **Server** e della rete antivirus grazie alla possibilità di delimitare i poteri di diversi amministratori, nonché la possibilità di connettere amministratori attraverso sistemi di autenticazione esterni, quali Active Directory, LDAP, RADIUS, PAM (per maggiori informazioni consultare la sezione [Capitolo 4: Amministratori della rete antivirus](#)).
- Possibilità di gestire le licenze della protezione antivirus di postazioni utilizzando un complesso sistema di assegnazione di licenze alle postazioni e ai gruppi di postazioni, nonché la possibilità di trasferire licenze tra alcuni **Server** se la configurazione della rete antivirus include diversi server (per maggiori informazioni consultare la sezione [Gestione licenze](#)).
- Un vasto set di impostazioni da utilizzare per configurare il **Server** e i suoi componenti separati, è possibile: impostare un calendario di manutenzione del **Server**; connettere procedure personalizzate; configurare in modo flessibile l'aggiornamento di tutti i componenti di rete antivirus da **SAM** e la successiva distribuzione degli aggiornamenti verso le postazioni; configurare sistemi che avvisano l'amministratore di eventi accaduti nella rete antivirus tramite diversi metodi di consegna dei messaggi; configurare le relazioni tra i server per configurare una rete antivirus con diversi server (per maggiori informazioni consultare la sezione [Capitolo 7: Configurazione di Server Dr.Web](#)).



Le informazioni dettagliate sulle possibilità dell'installazione della protezione antivirus su postazioni sono riportate nella **Guida all'installazione**.

Parte del **Pannello di controllo della sicurezza Dr.Web** è il **Web server** che viene installato automaticamente insieme al **Server**. L'obiettivo principale del **Web server** è di assicurare il lavoro con le pagine del **Pannello di controllo** e con le connessioni di rete client.



Pannello di controllo mobile di protezione centralizzata

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

Il **Pannello di controllo mobile** viene connesso al **Server** sulla base delle credenziali dell'amministratore di rete antivirus, è anche possibile una connessione attraverso protocollo cifrato. Il **Pannello di controllo mobile** supporta le funzionalità di base del **Pannello di controllo**. L'amministratore di rete antivirus può gestire le postazioni protette direttamente da un dispositivo mobile, nonché può visualizzare le statistiche del funzionamento dei componenti antivirus su postazioni protette e ricevere gli avvisi progettati per il **Pannello di controllo mobile**.

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

Protezione delle postazioni della rete

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

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

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

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

Il modulo di gestione aggiorna a cadenze regolari i componenti antivirus e i database dei virus dal **Server**, nonché invia al **Server** le informazioni su eventi di virus accaduti sul computer protetto.

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

A seconda del sistema operativo della postazione, vengono fornite le seguenti funzioni di protezione:

Postazioni SO Microsoft® Windows®

Scansione antivirus

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

Monitoraggio di file

Scansione continua del file system in tempo reale. Controllo di ogni processo avviato e dei file che vengono creati su dischi rigidi e vengono aperti su supporti rimovibili.

Monitoraggio di email

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

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

Monitoraggio del web

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



Office control

Controllo dell'accesso alle 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 occasionali o contro l'infezione di virus, e vieta ai dipendenti l'accesso alle informazioni indesiderate.

Firewall

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

Quarantena

Isolamento di oggetti dannosi e sospettosi in apposita cartella.

Auto-protezione

Protezione dei file e delle cartelle **Dr.Web Enterprise Security Suite** contro la rimozione o la modifica non autorizzata o accidentale da parte dell'utente e contro la rimozione o la modifica da parte del malware. Quando l'auto-protezione è attivata, l'accesso ai file e alle cartelle **Dr.Web Enterprise Security Suite** è consentito solamente ai processi **Dr.Web**.

Protezione preventiva

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

Postazioni SO famiglia UNIX®

Scansione antivirus

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

Monitoraggio di file

Scansione continua del file system in tempo reale. Controllo di ogni processo avviato e dei file che vengono creati su dischi rigidi e vengono aperti su supporti rimovibili.

Monitoraggio del web

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

Quarantena

Isolamento di oggetti dannosi e sospettosi in apposita cartella.

Postazioni Mac OS® X

Scansione antivirus

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

Monitoraggio di file

Scansione continua del file system in tempo reale. Controllo di ogni processo avviato e dei file che vengono creati su dischi rigidi e vengono aperti su supporti rimovibili.

Quarantena

Isolamento di oggetti dannosi e sospettosi in apposita cartella.

Dispositivi mobili SO Android

Scansione antivirus

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



Monitoraggio di file

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

Filtraggio di chiamate e di messaggi

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

Antifurto

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

Limitazione dell'accesso a risorse Internet

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

Firewall

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

Aiuto nella risoluzione di problemi

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

Controllo dell'esecuzione di applicazioni

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

Server SO Novell® NetWare®

Scansione antivirus

Scansione del computer on demand e secondo il calendario.

Monitoraggio di file

Scansione continua del file system in tempo reale. Controllo di ogni processo avviato e dei file che vengono creati su dischi rigidi e vengono aperti su supporti rimovibili.

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 di assicurare la comunicazione del **Server** e delle postazioni protette nel caso non sia possibile organizzare l'accesso diretto, per esempio, se il **Server** e le postazioni protette si trovano in reti diverse senza l'instradamento dei pacchetti tra di esse. Tramite la funzione di memorizzazione in cache, è anche possibile ridurre il traffico di rete e il tempo di ottenimento degli aggiornamenti da parte delle postazioni protette.

Compressione del traffico

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

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.



Possibilità aggiuntive

NAP Validator

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

Loader di repository

Il Loader di repository Dr.Web, fornito come utility aggiuntiva, permette di scaricare i prodotti **Dr.Web Enterprise Security Suite** dal **Sistema di aggiornamento mondiale**. Si può utilizzarlo per scaricare aggiornamenti dei prodotti **Dr.Web Enterprise Security Suite** per mettere gli aggiornamenti su un **Server** non connesso a Internet.

1.4. Requisiti di sistema

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

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



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


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

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



Fare attenzione: nelle versioni **4.XX** del **Server** la porta 2371 veniva utilizzata per la comunicazione dei componenti antivirus con il **Server**. Nella versione **10.0** questa porta non è più supportata.

Per il funzionamento del Server Dr.Web occorre:

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

Per il funzionamento del Server proxy Dr.Web occorre:

Componente	Requisito
Processore	Intel® Pentium® III frequenza di 667 MHz e superiori.
Memoria operativa	almeno 1 GB.
Spazio su disco rigido	almeno 1 GB.
Sistema operativo	<ul style="list-style-type: none">• Microsoft Windows;• Linux;• FreeBSD;



Componente	Requisito
	<ul style="list-style-type: none">• Solaris. La lista completa degli SO supportati è riportata nel documento Allegati , in Allegato A .
Altro	Per l'installazione del Server proxy sotto SO della famiglia UNIX è necessaria la disponibilità delle librerie: 1.5b versione 3 e superiori.

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

- ◆ Browser Windows Internet Explorer 8 e superiori, browser Mozilla Firefox 25 e superiori o browser Google Chrome 30 e superiori.



Si possono inoltre utilizzare i browser Opera® 10 e superiori, Safari® 4 e superiori. Tuttavia, la possibilità di utilizzare il software sotto questi browser non è garantita.

Non è garantita la completa operatività del **Pannello di controllo** avviato sotto il browser Windows Internet Explorer 8 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 utilizzare il **Server** attraverso il **Pannello di controllo** nel browser Windows Internet Explorer.

In questo caso si deve utilizzare un altro browser.

Per il corretto funzionamento del **Pannello di controllo** sotto il 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 viene aperto il **Pannello di controllo**.

Per aprire il **Pannello di controllo** in modo corretto tramite il menu **Start** nel browser Windows Internet Explorer in SO Windows 8 e Windows Server 2012 con l'interfaccia delle piastrelle dinamiche, è necessario configurare le seguenti impostazioni del browser: **Opzioni Internet** → **Programmi** → **Apertura di Internet Explorer** spuntare il flag **Sempre in Internet Explorer in visualizzazione classica**.

- ◆ L'Estensione del **Pannello di controllo della sicurezza Dr.Web** per l'utilizzo delle complete funzionalità del **Pannello di controllo**. L'estensione viene fornita insieme al pacchetto **Server** e viene installata a richiesta del browser nel processo di utilizzo degli elementi del **Pannello di controllo** che necessitano del caricamento dell'estensione (per lo **Scanner di rete** per l'installazione remota di componenti antivirus).



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

In caso di utilizzo del browser Safari, l'estensione del **Pannello di controllo della sicurezza Dr.Web** è disponibile soltanto per le versioni che girano sotto SO Windows.

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

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

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

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

◆ iOS:

Componente	Requisito
Sistema operativo	iOS® 7 e superiori
Dispositivo	Apple® iPhone® Apple® iPad®

◆ SO Android:

Componente	Requisito
Sistema operativo	Android 4.0 e superiori

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

- ◆ SO Windows Server 2008.

Per gli agent:

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

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

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

- SO Microsoft Windows:

Componente	Requisito
Processore	CPU con la frequenza di clock di 1 GHz e superiori.
Memoria operativa libera	Almeno 512 MB.
Spazio libero su disco rigido	Almeno 1 GB per i file eseguibili + spazio aggiuntivo per i log di funzionamento e per i file temporanei.
Altro	<ol style="list-style-type: none">1. Per il corretto funzionamento della guida sensibile al contesto di Agent Dr.Web per Windows è necessaria la disponibilità di Windows® Internet Explorer® 6.0 e superiori.2. Per il plugin Dr.Web per Outlook deve essere installato il client Microsoft Outlook di Microsoft Office:<ul style="list-style-type: none">◆ Outlook 2000 (Outlook 9),◆ Outlook 2002 (Outlook 10 oppure Outlook XP),◆ Office Outlook 2003 (Outlook 11),◆ Office Outlook 2007 (Outlook 12),◆ Office Outlook 2010 (Outlook 14),◆ Office Outlook 2013 (Outlook 15).



- SO della famiglia Linux:

Componente	Requisito
Processore	a 32 bit (IA-32, x86) ed a 64 bit (x86-64, x64, amd64) piattaforma Intel.
Memoria operativa libera	Almeno 512 MB.
Spazio libero su disco rigido	Almeno 400 MB di spazio libero sul volume su cui sono situate le cartelle dell' Antivirus .

- Mac OS X: i requisiti della configurazione coincidono con i requisiti del sistema operativo;
- OS Android: i requisiti della configurazione coincidono con i requisiti del sistema operativo;
- OS Novell NetWare: i requisiti della configurazione coincidono con i requisiti del sistema operativo.



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



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

1.5. Set di fornitura

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

1. In caso di UNIX – come file in formato `run` per installare i seguenti componenti sulle versioni corrispondenti di SO:
 - ◆ Pacchetto principale di **Server Dr.Web**,
 - ◆ Pacchetto supplementare (extra) di **Server Dr.Web**,
 - ◆ **Server proxy**.
2. In caso di Microsoft Windows – come file eseguibili dell'installazione guidata per installare i seguenti componenti:
 - ◆ Pacchetto principale di **Server Dr.Web**,
 - ◆ Pacchetto supplementare (extra) di **Server Dr.Web**,
 - ◆ **Server proxy**,
 - ◆ **Agent Dr.Web** per Active Directory,
 - ◆ Utility per modificare lo schema Active Directory,
 - ◆ Utility per modificare gli attributi degli oggetti Active Directory,
 - ◆ **NAP Validator**.

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

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

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

2. **Pacchetto supplementare (extra)** – include i pacchetti di tutti i prodotti per l'impresa forniti che possono essere installati sulle postazioni con tutti gli SO supportati.



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



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

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

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

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

1.6. Concessione delle licenze

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



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

I contenuti e il prezzo di una licenza di utilizzo della soluzione antivirus **Dr.Web Enterprise Security Suite** dipendono dal numero di postazioni protette nella rete (compresi i server che fanno parte della 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.

Le caratteristiche della concessione delle licenze, nonché l'utilizzo dei file della chiave per una rete antivirus già installata sono descritti in dettaglio in p. [Gestione licenze](#).

Il file della chiave di licenza può fare parte del set antivirus **Dr.Web Enterprise Security Suite** acquistato. Tuttavia, di solito vengono forniti solamente i numeri di serie.

Il file della chiave di licenza viene inviato a utenti via email, di solito, dopo la registrazione del numero di serie sul sito web (l'indirizzo del sito della registrazione è <http://products.drweb.com/register/>, se un altro indirizzo non è indicato nella scheda di registrazione fornita insieme al prodotto). Andare al sito indicato, compilare il modulo con le informazioni su acquirente e inserire nel campo indicato il numero di serie di registrazione (è reperibile nella scheda di registrazione). Un archivio con i file della chiave verrà inviato sull'indirizzo email indicato dall'utente. Inoltre, si può scaricarlo direttamente dal sito indicato.

I file della chiave vengono forniti all'utente in un archivio .zip contenente uno o più file della chiave per le postazioni protette.

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

- ◆ via email (di solito dopo la registrazione sul sito web, v. sopra);
- ◆ insieme al pacchetto del prodotto se i file di licenza sono stati inclusi nel pacchetto alla creazione;
- ◆ su un supporto separato come un file.

Si consiglia di conservare il file della chiave di licenza fino alla scadenza del periodo 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 riottenere il file della chiave di licenza. Per farlo, occorre indicare lo stesso numero di serie di registrazione e le stesse informazioni su acquirente che sono stati indicati al momento della prima registrazione; soltanto l'indirizzo email può essere diverso. In questo caso il file della chiave di licenza verrà inviato al nuovo indirizzo email.

Per provare **l'Antivirus**, si possono utilizzare i file della chiave demo. Tali file della chiave assicurano le funzionalità complete dei principali componenti antivirus, però hanno un periodo di validità limitato. Per ottenere i file della chiave demo, è necessario compilare il 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 verrà inviato sull'indirizzo email indicato dall'utente.

L'utilizzo dei file della chiave nel processo di installazione del programma è descritto in **Guida all'installazione**, p. [Installazione di Server Dr.Web](#).



Capitolo 2: Componenti della rete antivirus e la loro interfaccia

2.1. Server Dr.Web

La rete antivirus deve includere almeno un **Server Dr.Web**.



Per aumentare l'affidabilità e la produttività della rete antivirus, nonché per bilanciare il carico, **Dr.Web Enterprise Security Suite** consente di creare una rete antivirus con diversi **Server**. In tale caso, il software server viene installato su più computer contemporaneamente.

Il **Server Dr.Web** è un servizio residente nella memoria operativa. Il software **Server Dr.Web** è stato sviluppato per diversi SO (per elenco completo degli SO supportati v. il documento **Allegati, Allegato A**).

Funzioni principali

Il Server Dr.Web svolge le seguenti funzioni:

- ◆ avviare l'installazione dei pacchetti antivirus sul computer scelto o su un gruppo di computer,
- ◆ domandare il numero della versione del pacchetto antivirus, nonché i dati di creazione e i numeri delle versioni dei database dei virus ad ogni computer protetto,
- ◆ aggiornare contenuti della cartella di installazione centralizzata e della cartella di aggiornamenti,
- ◆ aggiornare i database dei virus e i file eseguibili dei pacchetti antivirus, nonché i file eseguibili dei componenti di rete antivirus sui computer protetti.

Raccolta delle informazioni sullo stato di rete antivirus

Il **Server Dr.Web** permette di raccogliere e di registrare nel log le informazioni circa il funzionamento dei pacchetti antivirus, trasmesse su di esso dal software sui computer protetti (dagli **Agent Dr.Web**, per maggiori informazioni v. sotto). Le informazioni vengono registrate nel log generale di eventi realizzato nel formato di database. In una rete di piccola dimensione (non più di 200-300 computer), il database interno può essere utilizzato per la registrazione dati nel log generale di eventi. Per reti grandi, è prevista la possibilità di utilizzare database esterni.



Il database incorporato può essere utilizzato se al **Server** sono connesse non più di 200-300 postazioni. Se lo permettono la configurazione dell'hardware del computer su cui è installato il **Server Dr.Web** e il carico di altri processi eseguiti su questo computer, è possibile connettere fino a 1000 postazioni.

Altrimenti, si deve utilizzare un database esterno.

Se viene utilizzato un database esterno e se al **Server** sono connesse più di 10000 postazioni, sono consigliabili i seguenti requisiti minimi:

- ◆ processore con velocità 3GHz,
- ◆ memoria operativa a partire dai 4 GB per il **Server Dr.Web**, a partire dai 8 GB per il server del database,
- ◆ SO della famiglia UNIX.

Devono essere raccolte e registrate nel log generale di eventi le seguenti informazioni:

- ◆ versione dei pacchetti antivirus su computer protetti,



- ◆ ora e data di installazione e di aggiornamento del software di postazione antivirus, nonché la versione del software,
- ◆ ora e data di aggiornamento dei database dei virus, nonché le sue versioni,
- ◆ versione dell'SO installato su computer protetti, tipo di processore, posizione delle cartelle di sistema dell'SO ecc.,
- ◆ configurazione e modalità di funzionamento dei pacchetti antivirus (utilizzo dei metodi euristici, lista dei tipi di file scansionati, azioni in caso di rilevamento di virus informatici ecc.),
- ◆ eventi dei virus: nome del virus informatico rilevato, data di rilevamento, azioni eseguite, il risultato di trattamento ecc.

Il **Server Dr.Web** avvisa l'amministratore della rete antivirus se si sono verificati degli eventi relativi al funzionamento della rete antivirus attraverso email o gli strumenti broadcast standard dei sistemi operativi Windows. La configurazione degli eventi che provocano l'invio degli avvisi e degli altri parametri di avviso è descritta in p. [Configurazione degli avvisi](#).

Server web

Il **Web server** fa parte del **Pannello di controllo della sicurezza Dr.Web** e svolge le seguenti funzioni principali:

- ◆ autenticare gli amministratori e concedere loro autorizzazioni nel **Pannello di controllo**;
- ◆ automatizzare il funzionamento delle pagine del **Pannello di controllo**;
- ◆ supportare pagine generate dinamicamente del **Pannello di controllo** ;
- ◆ supportare le connessioni sicure HTTPS con i client.

2.1.1. Gestione del Server Dr.Web sotto SO Windows®

Interfaccia e gestione del Server Dr.Web

Il **Server Dr.Web** non ha interfaccia incorporata. 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 cartella **Dr.Web Server** contenente i seguenti elementi di configurazione e di gestione base del **Server**:

- ◆ La cartella **Gestione del server** – contiene i comandi di avvio, di riavvio e di arresto del **Server**, nonché i comandi di configurazione del logging e gli altri comandi del **Server** descritti in dettaglio nel documento **Allegati**, p. [H3. Server Dr.Web](#).
- ◆ La voce **Interfaccia web** si usa per aprire il **Pannello di controllo** e per connettersi al **Server** installato sul questo computer (sull'indirizzo <http://localhost:9080>).
- ◆ La voce **Documentazione** si usa per aprire la documentazione dell'amministratore in formato HTML.

La directory di installazione di Server Dr.Web ha la seguente struttura:

- ◆ `bin` – file eseguibili di **Server Dr.Web**.
- ◆ `etc` – file di configurazione principali dei componenti di rete antivirus.
- ◆ `Installer` – programma che permette di installare l'**Antivirus** sul computer protetto e chiave di cifratura pubblica (`drwcsd.pub`).
- ◆ `update-db` – script necessari per aggiornare la struttura dei database del **Server**.
- ◆ `var` – la cartella contiene le sottocartelle:
 - `es-dl-cache` – pacchetti d'installazione personali degli utenti conservati entro due settimane dopo la creazione;
 - `backup` – backup dei database e degli altri dati critici;



- `extensions` – script di procedure personalizzate, ideati per automatizzare l'esecuzione di determinati task;
 - `repository` – cartella di repository in cui vengono messi gli aggiornamenti attuali dei database dei virus, dei file di pacchetti antivirus e dei componenti di rete antivirus. La cartella include sottocartelle per singoli componenti del software dentro cui si trovano sottocartelle per singoli SO. La cartella deve essere scrivibile per l'utente sotto il cui account viene avviato il **Server** (di regola, è l'utente **LocalSystem**);
 - `templates` – moduli dei resoconti.
- ◆ `webmin` – elementi del **Pannello di controllo della sicurezza Dr.Web**: documentazione, icone, moduli.



I contenuti della cartella di aggiornamenti `\var\repository` vengono scaricati dal server di aggiornamenti tramite il protocollo HTTP/HTTPS automaticamente, secondo il calendario impostato per il **Server**; inoltre l'amministratore della rete antivirus può mettere manualmente gli aggiornamenti in queste cartelle.

File di configurazione principali

File	Descrizione	Directory predefinita
<code>agent.key</code> (il nome può essere diverso)	chiave di licenza di Agent	etc
<code>certificate.pem</code>	certificato per SSL	
<code>download.conf</code>	impostazioni di rete per la generazione dei pacchetti d'installazione di Agent	
<code>drwcsd.conf</code> (il nome può essere diverso)	file di configurazione del Server	
<code>drwcsd.conf.distr</code>	template del file di configurazione di Server con i parametri di default	
<code>drwcsd.pri</code>	chiave di cifratura privata	
<code>enterprise.key</code> (il nome può variare)	chiave di licenza di Server . Viene mantenuta soltanto se era presente dopo l'aggiornamento dalle versioni precedenti. Quando viene installato il nuovo Server 10.0 , è assente.	
<code>frontdoor.conf</code>	file di configurazione per l'utility di diagnostica remota di Server	
<code>http-alerter-certs.pem</code>	certificati per la verifica dell'host apple-notify.drweb.com in caso di invio delle notifiche push	
<code>private-key.pem</code>	chiave privata RSA	
<code>webmin.conf</code>	file di configurazione del Pannello di controllo	
<code>auth-ads.xml</code>	file di configurazione per l'autenticazione esterna degli amministratori attraverso Active Directory	
<code>auth-ldap.xml</code>	file di configurazione per l'autenticazione esterna degli amministratori attraverso LDAP	
<code>auth-radius.xml</code>	file di configurazione per l'autenticazione esterna degli amministratori attraverso RADIUS	
<code>database.sqlite</code>	database incorporato	<code>var</code>
<code>drwcsd.pub</code>	chiave di cifratura pubblica	• <code>Installer</code>




File	Descrizione	Directory predefinita
		<ul style="list-style-type: none">webmin install

Avvio e arresto del Server Dr.Web

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

Inoltre, si può avviare, riavviare o arrestare il **Server Dr.Web** in uno dei seguenti modi:

- ◆ Caso generale:
 - Tramite il comando corrispondente locato nel menu **Start** → **Programmi** → **Server Dr.Web**.
 - Tramite gli strumenti di gestione dei servizi nella sezione **Amministrazione** del **Pannello di controllo** del SO Windows.
- ◆ Arresto e riavvio tramite il **Pannello di controllo**:
 - Nella sezione **Amministrazione**: riavvio con l'ausilio del pulsante , arresto con l'ausilio del pulsante .
- ◆ Tramite i comandi console eseguiti dalla sottocartella `bin` della cartella di installazione del **Server** (v. anche il documento **Allegati**, p. [H3. Server Dr.Web](#)):
 - `drwcsd start` – avvio del **Server**.
 - `drwcsd restart` – riavvio completo del servizio **Server**.
 - `drwcsd stop` – terminazione regolare del **Server**.



Notare: affinché il **Server** legga le variabili di ambiente, è necessario riavviare il servizio tramite gli strumenti di gestione dei servizi o tramite il comando console.

2.1.2. Gestione del Server Dr.Web sotto SO della famiglia UNIX®

Interfaccia e gestione del Server Dr.Web

Il **Server Dr.Web** non ha interfaccia incorporata. Generalmente, il **Server Dr.Web** viene gestito tramite il **Pannello di controllo** che funge da interfaccia esterna del **Server**.

La directory di installazione di Server Dr.Web ha la seguente struttura:

`/opt/drwcs/` per l'OS Linux, per l'OS Solaris e `/usr/local/drwcs` per l'OS FreeBSD:

- `bin` – file eseguibili di **Server Dr.Web**.
- `doc` – file di contratti di licenza.
- `ds-modules`
- `fonts` – tipi di carattere per l'interfaccia del **Pannello di controllo**.
- `Installer` – installer di rete e chiave di cifratura pubblica per installare l'**Antivirus** su computer protetti.
- `lib` – set di librerie per il funzionamento del **Server**.
- `update-db` – script necessari per aggiornare la struttura dei database del **Server**.
- `webmin` – tutti gli elementi del **Pannello di controllo della sicurezza Dr.Web**.



`/var/opt/drwcs/` per l'SO Linux, per l'SO Solaris e `/var/drwcs` per l'SO FreeBSD:

- `backup` – backup dei database e degli altri dati critici.
- `bases` – database dei virus decompressi per la compatibilità all'indietro con le versioni precedenti degli **Agent Dr.Web**.
- `coredump` – crash dump del **Server**.
- `database.sqlite` – database incorporato del **Server**.
- `etc` – file delle impostazioni principali dei componenti della rete antivirus.
- `extensions` – script personalizzati ideati per automatizzare l'esecuzione di determinati task.
- `installers-cache` – cache degli installer dell'**Agent**. Viene utilizzato per memorizzare pacchetti di installazione dell'**Agent** durante la creazione delle postazioni nel **Pannello di controllo**.
- `log` – file di log del **Server**.
- `object` – cache degli oggetti del **Pannello di controllo**.
- `reports` – cartella temporanea utilizzata per generare e memorizzare resoconti.
- `repository` – cartella di aggiornamenti in cui vengono messi gli aggiornamenti attuali dei database dei virus, dei file di pacchetti antivirus e dei componenti di rete antivirus. La cartella include sottocartelle per singoli componenti del software dentro cui si trovano sottocartelle per singoli SO. La cartella deve essere scrivibile per l'utente sotto il cui account viene avviato il **Server** (di regola, è l'utente **drwcs**).
- `run` – PID del processo del **Server**.
- `sessions` – sessioni del **Pannello di controllo**.
- `upload` – directory di caricamento dei file temporanei che vengono impostati tramite il **Pannello di controllo** (chiavi ecc.).

`/etc/opt/drweb.com/` per l'SO Linux (solo in caso di installazione tramite pacchetti generici `*.tar.gz.run`) e `/usr/local/etc/opt/` per l'SO FreeBSD:

- `software/drweb-esuite.remove` – script di rimozione del **Server**.
- + eventuali file e cartelli addizionali.

`/usr/local/etc/rc.d/` per l'SO FreeBSD:

- `drwcsd.sh` – script di avvio e di terminazione del **Server**.

`/var/tmp/drwcs` – backup dopo la rimozione del **Server**.

File di configurazione principali

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





File	Descrizione	Directory predefinita
enterprise.key (il nome può variare)	chiave di licenza di Server . Viene mantenuta soltanto se era presente dopo l'aggiornamento dalle versioni precedenti. Quando viene installato il nuovo Server 10.0 , è assente.	
frontdoor.conf	file di configurazione per l'utility di diagnostica remota di Server	
http-alerter-certs.pem	certificati per la verifica dell'host apple-notify.drweb.com in caso di invio delle notifiche push	
private-key.pem	chiave privata RSA	
webmin.conf	file di configurazione del Pannello di controllo	
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	
database.sqlite	database incorporato	<ul style="list-style-type: none">• per SO Linux e SO Solaris: /var/opt/drwcs• in caso del SO FreeBSD: /var/drwcs
drwcsd.pub	chiave di cifratura pubblica	<ul style="list-style-type: none">• per SO Linux e SO Solaris: /opt/drwcs/Installer /opt/drwcs/webmin/ install• in caso del SO FreeBSD: /usr/local/drwcs/Installer /usr/local/drwcs/webmin/ install

Avvio e arresto del Server Dr.Web

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

Inoltre, si può avviare, riavviare o arrestare il **Server Dr.Web** in uno dei seguenti modi:

◆ Arresto e riavvio tramite il **Pannello di controllo**:

- Nella sezione **Amministrazione**: riavvio con l'aiuto del pulsante , arresto con l'aiuto del pulsante  (non è disponibile nella versione per l'SO Solaris).

◆ Tramite il relativo comando console (v. anche il documento Allegati, p. [H3. Server Dr.Web](#)):

○ Avvio:

- per l'SO FreeBSD:
/usr/local/etc/rc.d/drwcsd.sh start
- per l'SO Linux e per l'SO Solaris:
/etc/init.d/drwcsd start

○ Riavvio:

- per l'SO FreeBSD:
/usr/local/etc/rc.d/drwcsd.sh restart



- per l'SO Linux e per l'SO Solaris:
/etc/init.d/drwcsd restart
- Arresto:
 - per l'SO FreeBSD:
/usr/local/etc/rc.d/drwcsd.sh stop
 - Per l'SO Linux e per l'SO Solaris:
/etc/init.d/drwcsd stop



Notare: affinché il **Server** legga le variabili di ambiente, è necessario riavviare il servizio tramite il comando console.

2.2. Agent Dr.Web



La descrizione dettagliata di **Agent** e dei principi di funzionamento è disponibile nel manuale **Agent Dr.Web® per Windows. Manuale dell'utente**.

Principio di funzionamento

Le postazioni vengono protetti contro i virus dai pacchetti antivirus **Dr.Web** per i rispettivi SO.

Funzionando come parte di **Antivirus Dr.Web** di **Enterprise Security Suite** questi pacchetti vengono controllati dall'**Agent Dr.Web** installato sul computer protetto e residente permanentemente nella memoria. Se viene mantenuta la connessione con il **Server Dr.Web**, l'amministratore può configurare l'**Antivirus** sulle postazioni in modo centralizzato tramite il **Pannello di controllo**, assegnare un calendario delle scansioni antivirus, visualizzare le statistiche ed altre informazioni su funzionamento dei componenti antivirus, avviare ed arrestare una scansione antivirus ecc.

Il **Server Dr.Web** scarica gli aggiornamenti e li trasmette agli **Agent** connessi. Così con l'ausilio di **Agent Dr.Web** viene realizzata, supportata e regolata automaticamente l'ottimale strategia per la protezione antivirus a prescindere dal livello di qualifica degli utenti delle postazioni.

Tuttavia, nel caso di sconnessione provvisoria di una postazione da rete antivirus, l'**Agent Dr.Web** utilizza la copia locale delle configurazioni, la protezione antivirus su postazione mantiene la sua funzionalità (durante il periodo che non supera il periodo di validità di licenza di utente), ma l'aggiornamento dei database dei virus e del software non viene eseguito.

L'aggiornamento degli **Agent** mobile è descritto nel paragrafo [Aggiornamento degli Agent mobile Dr.Web](#).

Funzioni principali

L'Agent Dr.Web svolge le seguenti funzioni:

- ◆ l'installazione, l'aggiornamento e la configurazione del pacchetto antivirus **Dr.Web**, l'avvio della scansione, nonché l'esecuzione di altri task creati dal **Server Dr.Web**;
- ◆ permette di richiamare i componenti del pacchetto antivirus **Dr.Web** attraverso l'apposita interfaccia;
- ◆ trasmette i risultati dell'esecuzione dei task al **Server Dr.Web**;
- ◆ trasmette al **Server Dr.Web** degli avvisi su eventi, precedentemente specificati, nel funzionamento del pacchetto antivirus.

Ogni **Agent Dr.Web** è connesso a un **Server Dr.Web** e fa parte di uno o più gruppi registrati su questo **Server** (per maggiori informazioni vedere p. [Gruppi di sistema e custom](#)). Le informazioni vengono trasmesse tra l'**Agent** e il **Server** indicato attraverso il protocollo utilizzato in rete locale



(TCP/IP versione 4 o 6).



Di seguito il computer protetto con l'**Agent** installato, in conformità con le sue funzioni nella rete antivirus, verrà nominato *postazione* di rete antivirus. Si deve ricordare che a seconda delle sue funzioni svolte nella rete locale tale computer può essere sia una postazione che un server di rete locale.

2.3. Pannello di controllo della sicurezza Dr.Web

Per la gestione della rete antivirus in generale (compresa la modifica dei suoi contenuti e della sua struttura) e di tutti i suoi componenti, nonché per la configurazione di **Server Dr.Web**, si utilizza il **Pannello di controllo della sicurezza Dr.Web**.



Affinché il **Pannello di controllo** possa funzionare in maniera corretta nel web browser Windows Internet Explorer, è necessario aggiungere l'indirizzo del **Pannello di controllo** all'area attendibile nelle impostazioni del browser: **Tools (Servizio)** → **Internet Options (Opzioni Internet)** → **Security (Sicurezza)** → **Trusted Sites (Siti attendibili)**.

Affinché il **Pannello di controllo** possa funzionare in maniera corretta nel web browser Chrome, è necessario attivare i cookies nella configurazione del browser.

Connessione al Server Dr.Web

Su qualunque computer che abbia una connessione di rete con il **Server Dr.Web**, 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**.



I numeri di porta sono diversi per le connessioni http e per le connessioni protette https: rispettivamente 9080 e 9081.

Nella finestra di dialogo di richiesta di autenticazione inserire il nome e la password dell'amministratore (il nome amministratore predefinito con i permessi completi è **admin**, la password è la password che è stata impostata durante l'installazione del **Server**).

In caso di caricamento su https (connessione sicura SSL), il browser richiede una conferma del certificato utilizzato dal **Server**. La richiesta della conferma potrebbe essere accompagnata dalle informazioni che il certificato sia inattendibile o invalido. Il browser visualizza queste informazioni perché il certificato è sconosciuto. Per caricare il **Pannello di controllo** è necessario accettare il certificato proposto. Altrimenti, il caricamento non sarà possibile.



In alcune versioni dei browser, per esempio, in **Firefox 3** e superiori, in caso di connessione via https, viene restituito un errore, e il **Pannello di controllo** non viene caricato. In questo caso sulla pagina di errore si deve selezionare la voce **Aggiungi sito alla lista esclusioni** (sotto il messaggio di errore). Dopo questo, l'accesso al **Pannello di controllo** sarà consentito.



Interfaccia del Pannello di controllo della sicurezza Dr.Web

La finestra del **Pannello di controllo** (v. immagine [2-1](#)) è suddivisa in *intestazione del menu principale* e in *area operativa*.

Area operativa

Tramite l'area operativa si può accedere alle funzionalità principali del **Pannello di controllo**. È costituita da due o tre pannelli, a seconda delle azioni che vengono eseguite. Le funzionalità dei pannelli sono nidificate da sinistra a destra:

- ◆ *menu di gestione* è sempre situato nella parte sinistra della finestra,
- ◆ a seconda della voce selezionata nel menu di gestione, vengono visualizzati uno o due pannelli supplementari. Nell'ultimo caso, nella parte destra vengono mostrate le proprietà o le impostazioni degli elementi visualizzati nel pannello centrale.

La lingua dell'interfaccia viene impostata separatamente per ciascun account amministratore (v. p. [Gestione degli account amministratori](#)).

Menu principale

Nel menu principale del **Pannello di controllo** sono disponibili le seguenti voci:

- ◆ sezione [Amministrazione](#),
- ◆ sezione [Rete antivirus](#),
- ◆ sezione [Relazioni](#),
- ◆ [barra di ricerca](#),
- ◆ account amministratore utilizzato per accedere al **Pannello di controllo**,
- ◆ eventi,
- ◆ sezione [Impostazioni](#),
- ◆ sezione [Guida](#),
- ◆ pulsante **Esci** per terminare la corrente sessione di lavoro con il **Pannello di controllo**.



Se nel **Pannello di controllo** è attiva [l'autenticazione automatica](#), dopo che si è fatto clic sul pulsante **Esci**, le informazioni circa il nome e la password dell'amministratore vengono eliminate.

Quando si entrerà successivamente nel **Pannello di controllo**, si dovrà ripetere la procedura standard di autenticazione, indicando il nome e la password. In questo caso, se è attiva [l'autenticazione automatica](#), il nome e la password indicati vengono salvati in questo browser, e l'autenticazione nel **Pannello di controllo** verrà eseguita automaticamente (senza inserire il nome e la password) fino a quando non si farà clic di nuovo sul pulsante **Esci**.

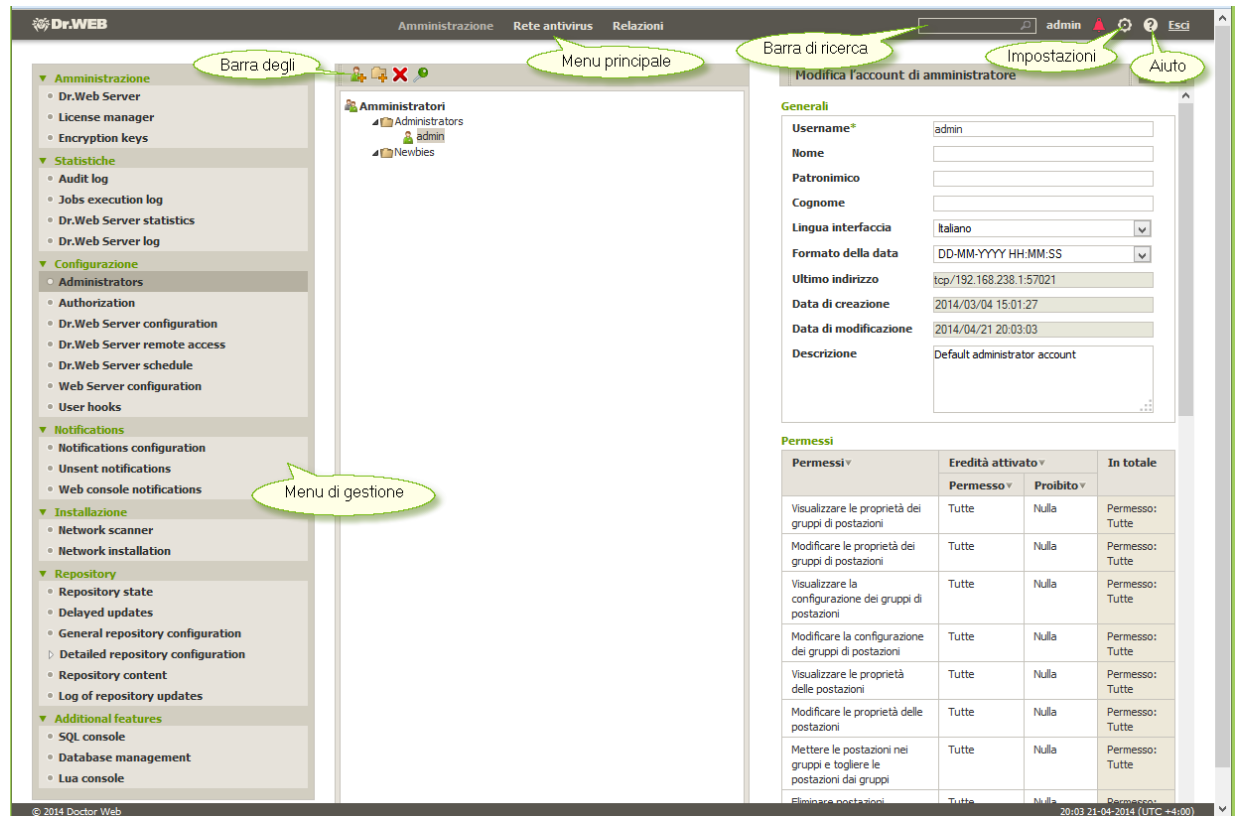


Immagine 2-1. Finestra del Pannello di controllo della sicurezza Dr.Web. Fare clic su una voce del menu principale per andare alla descrizione

Barra di ricerca

Per semplificare la ricerca di un elemento richiesto, si utilizza la *barra di ricerca* locata nella colonna di destra del menu principale del **Pannello di controllo**. La barra permette di eseguire la ricerca sia dei gruppi che di singole postazioni sulla base dei parametri indicati.

Per cercare postazioni o gruppi di postazioni:

1. Nella lista a cascata della barra di ricerca, scegliere il criterio di ricerca:
 - ◆ **Postazione** - per cercare postazioni per nome,
 - ◆ **Gruppo** - per cercare gruppi per nome,
 - ◆ **ID** - per cercare gruppi e postazioni per identificatore unico,
 - ◆ **Descrizione** - per cercare gruppi e postazioni per descrizione,
 - ◆ **Indirizzo IP** - per cercare postazioni per indirizzo IP,
 - ◆ **Hardware** - per cercare postazioni per nome dell'hardware della postazione,
 - ◆ **Programma** - per cercare postazioni per nome del software installato su postazione.
2. Inserire una stringa sulla base della quale verrà eseguita la ricerca. Si può utilizzare:
 - ◆ una stringa concreta per la completa corrispondenza con il parametro di ricerca,
 - ◆ una maschera della stringa di ricerca: sono consentiti i caratteri * e ?.
3. Premere il tasto INVIO per far partire la ricerca.
4. Nella lista gerarchica saranno visualizzati tutti gli elementi trovati secondo i parametri di ricerca, e:
 - ◆ se si è cercata una postazione, sarà visualizzata l'appartenenza della postazione a tutti i gruppi di cui fa parte,
 - ◆ se nessun elemento è stato trovato nel corso della ricerca, sarà visualizzata una lista gerarchica vuota con il messaggio **Nessun risultato della ricerca**.





2.3.1. Amministrazione

Dal menu principale del **Pannello di controllo** selezionare la voce **Amministrazione**. Per visualizzare e modificare le informazioni nella finestra che si è aperta, utilizzare il menu di gestione situato sul lato sinistro della finestra.

Il menu di gestione contiene le seguenti voci:

1. Amministrazione

- ◆ **Server Dr.Web** – apre un pannello tramite cui è possibile visualizzare le informazioni principali su **Server**, nonché riavviarlo tramite il pulsante  o arrestarlo tramite il pulsante  (non disponibile nella versione per SO Solaris) locati nella parte superiore destra del pannello. Inoltre, se sono disponibili aggiornamenti scaricati di **Server Dr.Web** da questa sezione è raggiungibile la sezione [Aggiornamenti di Server Dr.Web](#) con una lista delle versioni di **Server** per l'aggiornamento e il backup.
- ◆ [Gestione licenze](#) – consente di gestire i file della chiave di licenza.
- ◆ **Chiavi di crittografia** – consente di esportare (salvare localmente) le chiavi di crittografia pubblica e privata.

2. Logs

- ◆ **Log di verifica** – consente di visualizzare il log di eventi e di modifiche fatte tramite il **Pannello di controllo**.
- ◆ **Log di esecuzione dei task** – contiene l'elenco dei task impostati sul **Server** con l'annotazione di esecuzione e con commenti.
- ◆ [Log del Server Dr.Web](#) – contiene l'elenco dei log di eventi relativi al funzionamento del **Server**.
- ◆ **Log di aggiornamenti del repository** – contiene un elenco di aggiornamenti da **SAM**, che include le informazioni dettagliate su revisioni aggiornate dei prodotti.

3. Configurazione

- ◆ [Amministratori](#) – apre il pannello di gestione degli account amministratori di rete antivirus.
- ◆ [Autenticazione](#) – apre il pannello di gestione dell'autenticazione degli amministratori nel **Pannello di controllo**.
- ◆ [Configurazione del Server Dr.Web](#) – apre il pannello delle impostazioni principali del **Server**.
- ◆ [Accesso remoto al Server Dr.Web](#) – contiene le impostazioni per la connessione dell'utility di diagnostica remota del **Server**.
- ◆ [Scheduler del Server Dr.Web](#) – apre il pannello di configurazione del calendario dei task del **Server**.
- ◆ [Configurazione del web server](#) – apre il pannello delle impostazioni principali del **Web server**.
- ◆ [Procedure personalizzate](#).

4. Installazione

- ◆ [Scanner di rete](#) – permette di impostare una lista delle reti e di scansionare le reti alla ricerca del software antivirus installato per determinare lo stato di protezione dei computer, nonché di installare il software antivirus.
- ◆ **Installazione via rete** – permette di semplificare l'installazione del software **Agent** su concrete postazioni (v. **Guida all'installazione**, p. [Installazione di Agent Dr.Web tramite il Pannello di controllo della sicurezza Dr.Web](#)).

5. Avvisi

- ◆ [Notifiche nella console web](#) – permette di visualizzare e gestire gli avvisi all'amministratore ricevuti tramite il metodo **Web console**.
- ◆ [Notifiche non inviate](#) – permette di tracciare e gestire gli avvisi all'amministratore che non sono stati inviati secondo le impostazioni della sezione **Configurazione degli avvisi**.
- ◆ [Configurazione delle notifiche](#) – permette di configurare gli avvisi all'amministratore su eventi nella rete antivirus.



6. Repository

- ◆ [Stato del repository](#) – permette di controllare lo stato del repository: data dell'ultimo aggiornamento dei componenti nel repository e il loro stato.
- ◆ [Aggiornamenti differiti](#) – contiene una lista dei prodotti per cui gli aggiornamenti dei prodotti sono stati vietati temporaneamente nella sezione **Configurazione dettagliata del repository**.
- ◆ [Configurazione generale del repository](#) – apre la finestra di configurazione della connessione a **SAM** e dell'aggiornamento del repository per tutti i prodotti.
- ◆ [Configurazione dettagliata del repository](#) – consente di configurare le revisioni separatamente per ogni prodotto nel repository.
- ◆ [Contenuti del repository](#) – consente di visualizzare e gestire i contenuti correnti del repository a livello di directory e di file del repository.

7. Possibilità aggiuntive

- ◆ [Gestione del database](#) – consente di fare la manutenzione diretta del database con cui interagisce il **Server Dr.Web**.
- ◆ [Statistiche del Server Dr.Web](#) – contiene le statistiche del funzionamento di questo **Server**.
- ◆ **Console SQL** – dà la possibilità di eseguire query SQL al database utilizzato dal **Server Dr.Web**.
- ◆ **Console Lua** – dà la possibilità di eseguire script LUA, sia quelli digitati direttamente nella console che quelli caricati da file.
- ◆ **Utility** – apre una sezione per il caricamento delle utility supplementari per l'interazione con **Dr.Web Enterprise Security Suite**:
 - [Loader di repository Dr.Web](#) per il download dei prodotti **Dr.Web Enterprise Security Suite** da **Sistema di aggiornamento mondiale**. La versione grafica del **Loader di repository Dr.Web** è disponibile solo in SO Windows.
 - **Utility di diagnostica remota del Server Dr.Web** consente di connettersi al **Server Dr.Web** su remoto per effettuare la gestione base e visualizzare le statistiche di funzionamento. La versione grafica dell'utility è disponibile solo in SO Windows.
 - **Pannello di controllo mobile Dr.Web** per l'amministrazione di una rete antivirus costruita sulla base di **Dr.Web Enterprise Security Suite**. Può essere installato e avviato sui dispositivi mobili iOS e SO Android.

2.3.2. Rete antivirus

Nel menu principale del **Pannello di controllo** selezionare la voce **Rete antivirus**.

Menu di gestione

Per visualizzare e modificare le informazioni nella finestra che si è aperta, si utilizza il menu di gestione situato nella parte sinistra della finestra.

Il menu di gestione contiene le seguenti voci:

1. Generali

- ◆ [Grafici](#)
- ◆ [Componenti in esecuzione](#)
- ◆ [Componenti installati](#)
- ◆ [Quarantena](#)
- ◆ [Comparazione dell'hardware e del software](#) (in caso di selezione di un gruppo o di diverse postazioni)
- ◆ **Postazioni non attive**
- ◆ **Sessioni degli utenti**



- ◆ [Hardware e software](#) (in caso di selezione di una postazione)
 - ◆ [Proprietà](#)
 - ◆ [Regole di appartenenza al gruppo](#) (in caso di selezione di un gruppo definito dall'utente)
2. [Statistiche](#)
3. **Configurazione**
- ◆ [Permessi](#)
 - ◆ [Scheduler](#)
 - ◆ [Componenti da installare](#)
 - ◆ [Limitazioni degli aggiornamenti](#)
 - ◆ Lista dei componenti antivirus adatti per il sistema operativo della postazione selezionata o riportati per liste dei sistemi operativi in caso di selezione di un gruppo.



Le impostazioni dei componenti e le raccomandazioni per la configurazione sono riportate nel **Manuale dell'utente** per il relativo sistema operativo.

Lista gerarchica della rete antivirus

Nella parte centrale della finestra si trova la lista gerarchica della rete antivirus. La lista gerarchica visualizza la struttura ad albero degli elementi della rete antivirus. I nodi di questa struttura sono i [gruppi](#) e le [postazioni](#) che ne fanno parte.

Si possono eseguire le seguenti azioni con gli elementi della lista:

- ◆ fare clic con il tasto sinistro del mouse sul nome di un gruppo o di una postazione per visualizzare il menu di gestione del rispettivo elemento (nella parte sinistra della finestra) o le informazioni riepilogative su postazione nella barra delle proprietà (nella parte destra della finestra);
- ◆ fare clic con il tasto sinistro del mouse sull'icona di un gruppo per mostrare o nascondere i contenuti del gruppo.
- ◆ fare clic con il tasto sinistro del mouse sull'icona di una postazione per andare alla sezione delle proprietà di questa postazione.



Per selezionare più postazioni o gruppi dalla lista gerarchica, utilizzare il mouse tenendo premuti i tasti CTRL o SHIFT.

L'aspetto dell'icona di un elemento della lista dipende dal tipo o dallo stato di questo elemento (v. [tabella 2-1](#)).



Tabella 2-1. Icone degli elementi della lista gerarchica

Icona	Descrizione
Gruppi. Icone principali	
	Gruppi visualizzati sempre nella lista gerarchica.
	I gruppi non verranno visualizzati nella lista gerarchica se: <ul style="list-style-type: none">• ai gruppi è stata applicata l'azione Imposta la visibilità del gruppo → Nascondi se vuoto e in un dato momento i gruppi non includono postazioni,• ai gruppi è stata applicata l'azione Imposta la visibilità del gruppo → Nascondi e in un dato momento nella sezione Impostazioni della vista albero è deselezionato il flag Mostra gruppi nascosti.
Postazioni. Icone principali	
	Postazione disponibile con il software antivirus installato.
	Postazione non disponibile.
	Software antivirus su postazione è disinstallato.
	Stato della postazione in caso dell'installazione remota di Agent attraverso la rete. La postazione è in tale stato dal momento di un'installazione riuscita di Agent su questa postazione fino al momento della prima connessione della postazione al Server .
Icone aggiuntive	
	L'icona delle impostazioni individuali viene visualizzata sopra le icone principali delle postazioni e dei gruppi per cui le impostazioni individuali sono state definite (in caso dei gruppi anche quando il gruppo include postazioni con le impostazioni individuali). Per visualizzare l'icona, selezionare la voce Impostazioni della vista albero nella barra degli strumenti e spuntare il flag Mostra l'icona di impostazioni personalizzate . Per esempio, se le impostazioni individuali sono definite su una postazione con il software antivirus installato, che al momento è online, la sua icona avrà il seguente aspetto:
	L'icona dell'errore di aggiornamento viene visualizzata accanto alle icone principali delle postazioni sulle quali alcuni errori si sono verificati durante l'aggiornamento del software antivirus. Per visualizzare l'icona, selezionare la voce Impostazioni della vista albero nella barra degli strumenti e spuntare il flag Mostrare l'icona di errore aggiornamento . Per esempio, se è occorso un errore di aggiornamento del software antivirus su una postazione che al momento è online, la sua icona avrà il seguente aspetto:
	L'icona delle regole dell'appartenenza ai gruppi viene visualizzata accanto alle icone principali delle postazioni per le quali sono state stabilite le regole della sistemazione automatica delle postazioni. Per visualizzare l'icona, selezionare la voce Impostazioni della vista albero nella barra degli strumenti e spuntare il flag Mostrare l'icona di regole appartenenza al gruppo . Per esempio, se per un gruppo visualizzato sempre nella lista gerarchica, sono state impostate le regole dell'appartenenza, la sua icona avrà il seguente aspetto:

Gli elementi della lista gerarchica della rete antivirus vengono gestiti attraverso la barra degli strumenti.

























Barra degli strumenti

La barra degli strumenti della lista gerarchica contiene i seguenti elementi:


★ **Generali.** Consente di gestire parametri generali della lista gerarchica. Selezionare la voce opportuna dalla lista a cascata:


Modifica. Apre la barra delle proprietà della postazione o del gruppo nella parte destra della finestra del **Pannello di controllo**.




-  **Rimuovi gli oggetti selezionati.** Consente di rimuovere oggetti della lista gerarchica. Per farlo, selezionare uno o più oggetti dalla lista e fare clic su **Rimuovi gli oggetti selezionati**.
-  **Rimuovi le regole di appartenenza.** Consente di rimuovere le regole della sistemazione automatica delle postazioni in gruppi.
-  **Imposta questo gruppo come primario.** Consente di impostare come primario un gruppo scelto nella lista gerarchica per tutte le postazioni che ne fanno parte.
-  **Imposta il gruppo primario per le postazioni.** Consente di impostare gruppo primario per le postazioni selezionate nella lista gerarchica. Se un gruppo è selezionato nella lista gerarchica, a tutte le postazioni che ne fanno parte, verrà assegnato il gruppo primario scelto.
-  **Unisci le postazioni.** Consente di unire le postazioni sotto un singolo account nella lista gerarchica. Si può utilizzare questa funzione quando la stessa postazione è stata registrata sotto diversi account.
-  **Rimuovi le impostazioni personalizzate.** Consente di rimuovere le impostazioni personalizzate dell'oggetto selezionato dalla lista. In tale caso, l'oggetto eredita le impostazioni del gruppo primario. Se un gruppo è selezionato nella lista gerarchica, anche le impostazioni di tutte le postazioni che ne fanno parte vengono rimosse.
-  **Invia il messaggio alle postazioni.** Consente di inviare un messaggio con qualsiasi contenuto agli utenti.
-  **Resetta la password.** Consente di cancellare la password utente di accesso alle impostazioni dei componenti antivirus sulle postazioni selezionate. L'opzione è disponibile soltanto per le postazioni SO Windows.
-  **Riavvia la postazione.** Consente di lanciare su remoto il processo di riavvio di una postazione.
-  **Disinstalla Agent Dr.Web.** Rimuove l'**Agent** e il software antivirus dalla postazione o da un gruppo di postazioni selezionate.
-  **Installa Agent Dr.Web.** Apre lo **Scanner di rete** per installare l'**Agent** sulle postazioni selezionate. Questa voce è attiva soltanto se vengono selezionate postazioni nuove approvate o postazioni su cui l'**Agent** è stato disinstallato in precedenza.
-  **Recupera le postazioni rimosse.** Consente di recuperare le postazioni rimosse in precedenza. Questa voce è attiva soltanto se postazioni vengono selezionate dal sottogruppo **Deleted** del gruppo **Status**.
-  **Invia file di installazione.** Consente di inviare i file di installazione per le postazioni selezionate dalla lista agli indirizzi di posta elettronica definiti nelle impostazioni di questa sezione.
-  **Aggiungi una postazione o un gruppo.** Consente di creare un nuovo elemento della rete antivirus. Per farlo, selezionare la voce opportuna dalla lista a cascata:
-  **Crea una postazione.** Consente di creare una nuova postazione (v. **Guida all'installazione**, p. **Creazione di un nuovo account**).
 -  **Crea un gruppo.** Consente di creare un nuovo gruppo di postazioni.
-  **Esporta dati.** Consente di registrare i dati generali delle postazioni della rete antivirus in un file in formato CSV, HTML o XML. Il formato dell'esportazione viene selezionato nella lista a cascata:
-  **Salva in formato CSV.**
 -  **Salva in formato HTML.**
 -  **Salva in formato XML.**
 -  **Salva in formato PDF.**
 -  **Esporta la configurazione.**
 -  **Importa la configurazione.**
 -  **Propaga la configurazione.**





 **Imposta la visibilità del gruppo.** Consente di modificare i parametri di visualizzazione dei gruppi. Per farlo, selezionare un gruppo dalla lista gerarchica ed indicare nella lista a cascata una delle seguenti varianti (l'icona del gruppo cambierà, v. [tabella 2-1](#)):


 **Nascondi** - significa che la visualizzazione del gruppo nella lista gerarchica è sempre disattivata.


 **Nascondi se vuoto** - significa che la visualizzazione del gruppo nella lista gerarchica è disattivata se il gruppo è vuoto (non contiene postazioni).


 **Mostra** - significa che il gruppo è sempre visualizzato nella lista gerarchica.

 **Gestione dei componenti.** Consente di gestire i componenti antivirus sulle postazioni. Per farlo, selezionare dalla lista a cascata una delle seguenti varianti:

 **Aggiorna i componenti falliti.** Comanda di sincronizzare forzatamente i componenti nell'aggiornamento dei quali è occorso un errore;


 **Aggiorna tutti i componenti.** Comanda di aggiornare tutti i componenti antivirus installati, per esempio se l'**Agent** non si connette al **Server** da molto tempo ecc. (v. p. [Aggiornamento manuale dei componenti Dr.Web Enterprise Security Suite](#));

 **Interrompi i componenti in esecuzione.** Comanda di fermare il funzionamento dei componenti antivirus in esecuzione sulla postazione.


 **Scansiona.** Consente di eseguire la scansione sulla postazione in una delle modalità da selezionare dalla lista a cascata:


 **Dr.Web Scanner. Scansione rapida** . In questa modalità **Dr.Web Agent Scanner** esegue la scansione dei seguenti oggetti:


- ◆ memoria operativa,
- ◆ settori di avvio di tutti i dischi,
- ◆ oggetti in esecuzione automatica,
- ◆ cartella radice del disco di avvio,
- ◆ cartella radice del disco di installazione dell'SO Windows,
- ◆ cartella di sistema dell'SO Windows,
- ◆ cartella `Documenti`,
- ◆ cartella temporanea di sistema,
- ◆ cartella temporanea utente.

 **Dr.Web Scanner. Scansione completa.** In questa modalità **Dr.Web Agent Scanner** esegue la scansione completa di tutti i dischi rigidi e supporti rimovibili (inclusi i settori di avvio).

 **Dr.Web Scanner. Scansione personalizzata.** In questa modalità, è possibile selezionare cartelle e file che verranno scansionati tramite **Dr.Web Agent Scanner**.

 **Postazioni non confermate.** Consente di gestire la lista dei nuovi arrivi, cioè delle postazioni la cui registrazione non è stata ancora confermata. Questa voce è attiva soltanto se le postazioni vengono selezionate dal sottogruppo **Newbies** del gruppo **Status**. Quando la registrazione verrà confermata o l'accesso al **Server** verrà negato, le postazioni verranno cancellate automaticamente dal sottogruppo predefinito **Newbies**. Per gestire i nuovi arrivi, selezionare dalla lista a cascata una delle seguenti varianti:

 **Consenti alle postazioni selezionate di accedere e imposta gruppo primario.** Comanda di confermare l'accesso al **Server** per la postazione e di assegnarle un gruppo primario dall'elenco proposto.

 **Annulla l'azione da eseguire al momento di connessione.** Comanda di annullare l'azione che deve essere eseguita con una postazione non confermata e che è stata impostata in precedenza per essere eseguita al momento della connessione della postazione al **Server**.

 **Proibisci alle postazioni selezionate di accedere.** Comanda di negare alla postazione l'accesso al **Server**.

 **Impostazioni della vista albero** permettono di modificare l'aspetto della lista:

- ◆ per i gruppi:





- **Appartenenza a tutti i gruppi** – consente di duplicare la postazione nella lista se appartiene contemporaneamente a diversi gruppi (soltanto per i gruppi con icona di cartella bianca - v. [tabella 2-1](#)). Se il flag è selezionato, la postazione viene visualizzata in tutti i gruppi di cui fa parte. Se il flag è tolto, la postazione viene visualizzata nella lista una volta sola.
 - **Mostra gruppi nascosti** – comanda di visualizzare tutti i gruppi inclusi nella rete antivirus. Se questo flag viene tolto, i gruppi vuoti (che non contengono postazioni) saranno nascosti. Questo può essere utile per escludere le informazioni eccessive, per esempio se ci sono tanti gruppi vuoti.
- ◆ per le postazioni:
- **Mostra gli identificatori delle postazioni** – attiva/disattiva la visualizzazione degli identificatori unici delle postazioni nella lista gerarchica.
 - **Mostra i nomi delle postazioni** – attiva/disattiva la visualizzazione dei nomi delle postazioni.
 - **Mostra gli indirizzi delle postazioni** – attiva/disattiva la visualizzazione degli indirizzi IP delle postazioni nella lista gerarchica.
 - **Mostra i server delle postazioni** – attiva/disattiva la visualizzazione dei nomi o degli indirizzi IP dei **Server** antivirus a cui sono connesse le postazioni.
 - **Mostra l'icona di errore aggiornamento** – attiva/disattiva la visualizzazione di un indicatore sulle icone delle postazioni su cui l'ultimo aggiornamento è terminato con errore.
- ◆ per tutti gli elementi:
- **Mostra l'icona di impostazioni personalizzate** – attiva/disattiva sulle icone delle postazioni o dei gruppi l'indicatore che segnala la presenza delle impostazioni individuali.
 - **Mostra descrizioni** – attiva/disattiva la visualizzazione delle descrizioni dei gruppi e delle postazioni (le descrizioni vengono impostate nelle proprietà degli elementi).
 - **Mostra il numero di postazioni** – attiva/disattiva la visualizzazione del numero di postazioni per tutti i gruppi della rete antivirus.
 - **Mostra l'icona di regole appartenenza al gruppo** – attiva/disattiva la visualizzazione di un indicatore sulle icone delle postazioni che sono state aggiunte al gruppo in modo automatico secondo le regole dell'appartenenza, nonché sulle icone dei gruppi a cui le postazioni sono state aggiunte in modo automatico.

Barra delle proprietà

La barra delle proprietà serve a visualizzare le proprietà e le impostazioni delle postazioni e dei gruppi.

Per visualizzare la barra delle proprietà:

1. Nella lista gerarchica fare clic sul nome di una postazione o di un gruppo e selezionare  **Generali**
→  **Modifica** nella barra degli strumenti.
2. Nella parte destra della finestra del **Pannello di controllo** si apre la barra contenente le proprietà del gruppo o della postazione selezionata. Queste impostazioni sono descritte in modo dettagliata in p. [Modifica dei gruppi](#) e [Proprietà della postazione](#).

2.3.3. Relazioni

Nel menu principale del **Pannello di controllo** selezionare la voce **Relazioni**. Per scegliere le informazioni da visualizzare, utilizzare il menu di gestione situato nella parte sinistra della finestra.



Amministrazione

La sezione **Amministrazione** del menu di gestione contiene la voce **Relazioni** che si utilizza per gestire le relazioni tra i **Server** in una rete antivirus con diversi server (v. p. [Caratteristiche di una rete con diversi Server Dr.Web](#)).

Nella lista gerarchica sono riportati tutti i **Server Dr.Web** connessi con questo **Server**.

La creazione delle nuove relazioni tra i server è descritta nella sezione [Configurazione delle relazioni tra i Server Dr.Web](#).

Tabelle

Nella sezione **Tabelle** del menu di gestione sono riportate le informazioni su funzionamento della rete antivirus, ricevute da altri **Server** (v. p. [Caratteristiche di una rete con diversi Server Dr.Web](#)).

Per visualizzare le tabelle riassuntive contenenti dati degli altri **Server**, fare clic sulla voce corrispondente della sezione **Tabelle**.

2.3.4. Impostazioni

Per passare alla sezione delle impostazioni del **Pannello di controllo**, nel menu principale fare clic sul pulsante .



Tutte le impostazioni di questa sezione sono valide solo per l'account amministratore corrente.

Il menu di gestione locato nella parte sinistra della finestra contiene i seguenti elementi:

- ◆ **Il mio account.**
- ◆ **Interfaccia.**
- ◆ **Abbonamento.**

Il mio account

Tramite questa sezione, viene gestito l'account amministratore di rete antivirus corrente (v. anche [Amministratori e gruppi di amministratori](#)).



I valori dei campi marcati con il carattere * devono essere impostati obbligatoriamente.

Se necessario, modificare i seguenti parametri:

- ◆ **Nome utente** dell'amministratore - login per accedere al **Pannello di controllo**.
- ◆ Nome e cognome dell'amministratore.
- ◆ **Lingua dell'interfaccia** utilizzata da questo amministratore.
- ◆ **Formato della data** utilizzato da questo amministratore nella modifica delle impostazioni contenenti una data. Sono disponibili i seguenti formati:
 - europeo: DD-MM-YYYY HH:MM:SS
 - americano: MM/DD/YYYY HH:MM:SS
- ◆ **Descrizione** dell'account.



- ◆ Per cambiare la password, premere il pulsante  **Cambia password** nella barra degli strumenti.

I seguenti parametri sono di sola lettura:

- ◆ Data della creazione account e dell'ultima modifica parametri,
- ◆ **Ultimo indirizzo** - visualizza l'indirizzo di rete dell'ultima connessione sotto questo account.


Permessi amministratore

La descrizione dei permessi di amministratore e della sua modifica è riportata nella sezione [Modifica degli amministratori](#).

Dopo aver modificato i parametri, fare clic sul pulsante **Salva**.

Interfaccia

Impostazioni della vista albero

I parametri di questa sottosezione permettono di modificare l'aspetto della lista e sono uguali alle impostazioni locate nella barra degli strumenti della voce  nella sezione del menu principale **Rete antivirus**:

- ◆ per i gruppi:
 - **Appartenenza a tutti i gruppi** – consente di duplicare la postazione nella lista se appartiene contemporaneamente a diversi gruppi (soltanto per i gruppi con icona di cartella bianca - v. [tabella 2-1](#)). Se il flag è selezionato, la postazione viene visualizzata in tutti i gruppi di cui fa parte. Se il flag è tolto, la postazione viene visualizzata nella lista una volta sola.
 - **Mostra gruppi nascosti** – comanda di visualizzare tutti i gruppi inclusi nella rete antivirus. Se questo flag viene tolto, i gruppi vuoti (che non contengono postazioni) saranno nascosti. Questo può essere utile per escludere le informazioni eccessive, per esempio se ci sono tanti gruppi vuoti.
- ◆ per le postazioni:
 - **Mostra gli identificatori delle postazioni** – attiva/disattiva la visualizzazione degli identificatori unici delle postazioni nella lista gerarchica.
 - **Mostra i nomi delle postazioni** – attiva/disattiva la visualizzazione dei nomi delle postazioni.
 - **Mostra gli indirizzi delle postazioni** – attiva/disattiva la visualizzazione degli indirizzi IP delle postazioni nella lista gerarchica.
 - **Mostra i server delle postazioni** – attiva/disattiva la visualizzazione dei nomi o degli indirizzi IP dei **Server** antivirus a cui sono connesse le postazioni.
 - **Mostra l'icona di errore aggiornamento** – attiva/disattiva la visualizzazione di un indicatore sulle icone delle postazioni su cui l'ultimo aggiornamento è terminato con errore.
- ◆ per tutti gli elementi:
 - **Mostra l'icona di impostazioni personalizzate** – attiva/disattiva sulle icone delle postazioni o dei gruppi l'indicatore che segnala la presenza delle impostazioni individuali.
 - **Mostra descrizioni** – attiva/disattiva la visualizzazione delle descrizioni dei gruppi e delle postazioni (le descrizioni vengono impostate nelle proprietà degli elementi).
 - **Mostra il numero di postazioni** – attiva/disattiva la visualizzazione del numero di postazioni per tutti i gruppi della rete antivirus.
 - **Mostra l'icona di regole appartenenza al gruppo** – attiva/disattiva la visualizzazione di un indicatore sulle icone delle postazioni che sono state aggiunte al gruppo in modo automatico secondo le regole dell'appartenenza, nonché sulle icone dei gruppi a cui le postazioni sono state aggiunte in modo automatico.



Scanner di rete



Per il funzionamento dello **Scanner di rete** è necessario che sia installata l'estensione del **Pannello di controllo della sicurezza Dr.Web**.

I parametri di questa sottosezione permettono di definire le impostazioni di default dello [Scanner di rete](#).

Per avviare lo **Scanner di rete**, nel menu principale del **Pannello di controllo** selezionare la voce **Amministrazione**, nel [menu di gestione](#) selezionare la voce **Scanner di rete**.

Impostare i seguenti parametri dello **Scanner di rete**:

1. Nel campo di input **Reti** impostare una lista delle reti nel formato:
 - ◆ con trattino (per esempio, 10.4.0.1-10.4.0.10),
 - ◆ separati da virgola e spazio (per esempio, 10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90),
 - ◆ con il prefisso di rete (per esempio, 10.4.0.0/24).
2. Se necessario, modificare la **Porta** e il valore del parametro **Time-out (s)**.
3. Per salvare i valori di default, fare clic sul pulsante **Salva**. In seguito, quando verrà utilizzato lo [Scanner di rete](#), questi parametri verranno impostati automaticamente.

Intervallo di tempo

In questa sezione viene configurato l'intervallo di tempo per la visualizzazione dei dati statistici (v. p. [Visualizzazione delle statistiche della postazione](#)):

- ◆ Nella lista a cascata **Intervallo predefinito per la visualizzazione delle statistiche** viene impostato l'intervallo di tempo predefinito per tutte le sezioni dei dati statistici.

Alla prima apertura della pagina, le statistiche verranno visualizzate per l'intervallo di tempo indicato. Se necessario, si può modificare l'intervallo di tempo direttamente nelle sezioni delle statistiche.

- ◆ Affinché nelle sezioni delle statistiche venga salvato l'ultimo intervallo impostato, mettere il flag **Salva l'ultimo intervallo di visualizzazione delle statistiche**.

Se il flag è selezionato, alla prima apertura della pagina, verranno visualizzate le statistiche per l'ultimo periodo scelto nel browser.

Se il flag è deselezionato, alla prima apertura della pagina, verranno visualizzate le statistiche per il periodo impostato nella lista **Intervallo predefinito per la visualizzazione delle statistiche**.

Autenticazione

Spuntare il flag **Autenticazione automatica** per consentire nel browser corrente l'autenticazione automatica in tutti i **Pannelli di controllo Dr.Web** con questi nome utente e password amministratore.

Dopo che il flag è stato selezionato, verranno salvati tramite **l'estensione del Pannello di controllo della sicurezza Dr.Web** il nome utente e la password che l'amministratore indica durante l'autenticazione successiva nel **Pannello di controllo**.



Per il funzionamento dell'autenticazione automatica è necessario che sia installata l'estensione del **Pannello di controllo della sicurezza Dr.Web**.



In seguito, se si apre un **Pannello di controllo della sicurezza Dr.Web** in questo browser, l'autenticazione verrà eseguita automaticamente se sul **Server** è disponibile un utente con questi nome utente e password. Se il nome utente e la password non corrispondono (per esempio, tale utente non esiste o l'utente con questo nome ha un'altra password), si aprirà la finestra standard di autenticazione del **Pannello di controllo**.



Se si fa clic sul pulsante **Esci** nel **menu principale** dell'interfaccia del **Pannello di controllo**, vengono eliminate le informazioni su nome utente e password dell'amministratore.

Quando si accederà successivamente al **Pannello di controllo**, si dovrà ripetere la procedura standard di autenticazione, indicando il nome utente e la password. Se è attivata l'autenticazione automatica, le credenziali indicate vengono memorizzate in questo browser, e l'autenticazione nel **Pannello di controllo** verrà eseguita automaticamente (senza dover inserire il nome utente e la password) fino allo successivo clic sul pulsante **Esci**.

Dalla lista a cascata **Durata della sessione**, selezionare un periodo dopo il quale la sessione di utilizzo del **Pannello di controllo** nel browser si interrompe automaticamente.

Esportazione in PDF

In questa sottosezione viene configurato il testo utilizzato nell'esportazione dei dati statistici in formato PDF:

- ◆ Dalla lista a cascata **Tipo carattere dei report**, si può selezionare il tipo di carattere da utilizzare nell'esportazione dei report in formato PDF.
- ◆ Nel campo **Dimensione carattere dei report** si può impostare la dimensione dei caratteri del testo principale delle tabelle statistiche da utilizzare nell'esportazione dei report in formato PDF.

Report

In questa sottosezione si configura la visualizzazione delle statistiche nella sezione **Report** del **Pannello di controllo**:

- ◆ Nel campo **Numero di righe per pagina** viene impostato il numero massimo di righe su una pagina del report per la visualizzazione delle statistiche divisa in pagine.
- ◆ Spuntare il flag **Mostra grafici** per visualizzare diagrammi sulle pagine dei report statistici. Se il flag è tolto, la visualizzazione dei grafici è disattivata.

Abbonamento

In questa sottosezione si configura l'abbonamento alle notizie della società **Doctor Web**.

Spuntare il flag **Abbonamento automatico alle nuove sezioni** per attivare l'aggiunzione automatica di nuove sezioni alla sezione di notizie nel **Pannello di controllo**.

2.3.5. Guida

Per passare alla sezione guida del **Pannello di controllo**, nel menu principale fare clic sul pulsante 

Il menu di gestione locato nella parte sinistra della finestra contiene i seguenti elementi:

1. Generali

- ◆ **Forum** - per passare al forum della società **Doctor Web**.
- ◆ **Notizie** - per passare alla pagina di notizie della società **Doctor Web**.
- ◆ **Fai una domanda** – per passare alla pagina del **Supporto tecnico Doctor Web**.
- ◆ **Spedisci un virus** – per aprire il modulo di invio di un virus al laboratorio **Doctor Web**.



- ◆ **wiki** – per passare alla pagina di Wikipedia – un database di informazioni dedicato ai prodotti della società **Doctor Web**.
 - ◆ **Segnala un falso positivo di Office control** – per aprire un modulo tramite il quale si può inviare un messaggio di falso positivo o di mancato riconoscimento di link malevoli da parte del modulo **Office control**.
- 2. Documentazione dell'amministratore**
- ◆ **Manuale dell'amministratore** – per aprire il manuale dell'amministratore in formato HTML.
 - ◆ **Guida all'installazione** - per aprire la guida all'installazione di **Dr.Web Enterprise Security Suite** in formato HTML.
 - ◆ **Allegati** – per aprire gli allegati al manuale dell'amministratore in formato HTML.
 - ◆ **Guida a Web API** - per aprire la documentazione dell'amministratore su Web API (v. inoltre il documento **Allegati**, p. [Allegato L. Integrazione di Web API e di Dr.Web Enterprise Security Suite](#)) in formato HTML.
 - ◆ **Note di release** – per aprire la sezione dei commenti sul rilascio di **Dr.Web Enterprise Security Suite** per la versione installata.
- 3. Documentazione dell'utente** - per aprire la documentazione dell'utente in formato HTML per il sistema operativo corrispondente, riportato nell'elenco.

2.4. Componenti del Pannello di controllo della sicurezza Dr.Web

2.4.1. Scanner di rete

Una parte di **Server Dr.Web** è lo **Scanner di rete**.



Non si consiglia di avviare lo **Scanner di rete** sotto SO Windows 2000 e inferiori: la panoramica della rete può essere incompleta.

Il funzionamento dello **Scanner di rete** è garantito sotto SO della famiglia UNIX o sotto SO Windows XP e superiori.

Per il funzionamento dello **Scanner di rete** è necessario che sia installata l'estensione del **Pannello di controllo della sicurezza Dr.Web**.

Affinché lo **Scanner di rete** possa funzionare in maniera corretta nel web browser Windows Internet Explorer, è necessario aggiungere l'indirizzo del **Pannello di controllo**, in cui viene avviato lo **Scanner di rete**, all'area attendibile nelle impostazioni del browser: **Tools (Servizio)** → **Internet Options (Opzioni Internet)** → **Security (Sicurezza)** → **Trusted Sites (Siti attendibili)**.

Lo Scanner di rete svolge le seguenti funzioni:

- ◆ Scansione (visualizzazione) della rete per rilevare postazioni.
- ◆ Determina la disponibilità dell'**Agent Dr.Web** su postazioni.
- ◆ Installazione di **Agent Dr.Web** su postazioni rilevate su comando dell'amministratore. L'installazione di **Agent Dr.Web** è descritta dettagliatamente nella **Guida all'installazione**, p. [Installazione di Agent Dr.Web tramite il Pannello di controllo della sicurezza Dr.Web](#).

Per scansionare (visualizzare) la rete, eseguire le seguenti azioni:

1. Aprire la finestra dello **Scanner di rete**. Per farlo, selezionare la voce **Amministrazione** del menu principale del **Pannello di controllo**, nella finestra che si è aperta, selezionare la voce del menu di gestione **Scanner di rete**. Si apre la finestra **Scanner di rete**.
2. Spuntare il flag **Ricerca per indirizzo IP** per cercare postazioni nella rete a seconda degli indirizzi IP impostati. Nel campo di input **Reti** specificare una lista delle reti nel formato:
 - ◆ con trattino (per esempio, 10.4.0.1-10.4.0.10),



- ◆ separati da virgola e spazio (per esempio, 10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90),
 - ◆ con il prefisso di rete (per esempio, 10.4.0.0/24).
3. In caso del SO Windows: spuntare il flag **Cerca le postazioni nel dominio di Active Directory** per cercare le postazioni nel dominio di Active Directory. Inoltre, impostare i seguenti parametri:
- **Domini** - lista dei domini in cui verranno cercate le postazioni. Utilizzare virgola per separare diversi domini.
 - **Controller di Active Directory** - controller di Active Directory, ad esempio, dc.example.com.



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

4. In caso di SO della famiglia UNIX: spuntare il flag **Ricerca LDAP** per cercare le postazioni attraverso LDAP. Inoltre, impostare i seguenti parametri:
- **Domini** - lista dei domini in cui verranno cercate le postazioni. Utilizzare virgola per separare diversi domini.
 - **Server LDAP** - server LDAP, ad esempio, [ldap://ldap.example.com](http://ldap.example.com).
 - **Nome utente** - nome dell'utente di LDAP.
 - **Password** - password dell'utente di LDAP.
5. Nel campo **Porta** indicare il numero di porta per la connessione attraverso il protocollo UDP alla ricerca degli **Agent**.
6. Se necessario, nel campo **Time-out (sec)** modificare il valore di timeout in secondi per l'attesa di una risposta dalle postazioni.
7. Se necessario, mettere il flag **Scansione rapida** per eseguire la scansione nella **modalità accelerata**.
8. Spuntare il flag **Mostra il nome della postazione** per visualizzare non soltanto l'indirizzo IP dei computer trovati nella rete, ma anche il nome a dominio.

Se una postazione non è registrata sul server DNS, viene visualizzato solo il suo indirizzo IP.

9. Mettere il flag **Correla con la lista di postazioni dal database** per attivare la sincronizzazione dei risultati della ricerca fatta da **Scanner di rete** con la lista di postazioni salvata nel database del **Server**. Se il flag è attivato, nella lista delle postazioni trovate nella rete verranno visualizzate anche quelle postazioni che sono presenti nel database del **Server**, ma non sono state rilevate da **Scanner di rete** nel corso della ricerca corrente, per esempio se su queste postazioni è installato un firewall che impedisce la trasmissione di pacchetti necessari per la connessione TCP.







Quando i risultati della ricerca fatta da **Scanner di rete** vengono sincronizzati con le informazioni dal database del **Server**, la priorità è data alle informazioni dal database del **Server**. Cioè, se lo status di postazione rilevato nel corso della ricerca non corrisponde a quello registrato nel database, verrà assegnato lo status registrato nel database.



10. Fare clic sul pulsante **Scansiona**. A questo punto inizia la scansione della rete.
11. Durante la scansione di rete nella finestra viene caricata la directory (la lista gerarchica) dei computer con indicazione di disponibilità su di essi degli **Agent Dr.Web**.

Aprire gli elementi del catalogo corrispondenti ai gruppi di lavoro (domini). Tutti gli elementi del catalogo corrispondenti ai gruppi di lavoro e a singole postazioni sono contrassegnati con varie icone, il cui significato è riportato di seguito.



Tabella 2-2. Possibili tipi di icone

Icona	Descrizione
Gruppi di lavoro	
	Gruppi di lavoro che, oltre ad altri computer, comprendono computer su cui si può installare Dr.Web Enterprise Security Suite .
	Altri gruppi che comprendono computer con il software antivirus installato o computer non disponibili via rete.
Postazioni	
	La postazione trovata è registrata nel database ed è attiva (postazioni attive con il software antivirus installato).
	La postazione trovata è registrata nel database nella tabella di postazioni eliminate.
	La postazione trovata non è registrata nel database (sul computer non è installato il software antivirus).
	La postazione trovata non è registrata nel database (la postazione è connessa a un altro Server).
	La postazione trovata è registrata nel database, non è attiva, e la porta è chiusa.

Si possono aprire inoltre gli elementi del catalogo corrispondenti alle postazioni con le icone  o  per scoprire quali componenti sono installati.

Interazione con gli Agent Dr.Web

Lo strumento **Scanner di rete** fa parte di **Dr.Web Enterprise Security Suite** a partire dalla versione **4.44**.



Lo **Scanner di rete** può rilevare su una postazione la disponibilità dell'**Agent** soltanto delle versioni **4.44** e superiori, ma non può interagire con gli **Agent** delle versioni precedenti.

L'installato **Agent** versioni **4.44** e superiori processa le richieste dello **Scanner di rete**, arrivate su una determinata porta. Di default, si usa la porta `udp/2193`, però, per assicurare la compatibilità con il software delle versioni precedenti, è supportata anche la porta `udp/2372`. Di conseguenza, anche lo **Scanner di rete** usa di default queste porte. Lo **Scanner di rete** conclude che l'**Agent** è disponibile o non disponibile su una postazione basandosi sulla possibilità di scambiare informazioni (richiesta-risposta) sulla porta sopraccitata.



Se su una postazione la ricezione di pacchetti su `udp/2193` è proibita (per esempio tramite il firewall), l'**Agent** non può essere rilevato e quindi lo **Scanner di rete** considera che l'**Agent** non è installato sulla postazione.

Scansione rapida

Se è attiva l'opzione **Scansione rapida**, viene eseguita la seguente sequenza di azioni:

1. Le richieste ping vengono inviate alle postazioni della rete.
2. Soltanto alle postazioni che hanno risposto alle richieste ping vengono inviate le richieste in parallelo per rilevare gli **Agent**.
3. La procedura di rilevazione della presenza dell'**Agent** viene eseguita a secondo delle regole generali.



Le richieste ping possono essere bloccate per criteri di rete (per esempio dalle impostazioni di firewall).

**Per esempio:**

Se in SO Windows Vista e superiori nelle impostazioni di rete è stata impostata la **Rete pubblica**, SO bloccherà tutte le richieste ping.

Durante la scansione normale, le richieste ping non vengono inviate, e a tutte le postazioni vengono inviate in modo consecutivo le richieste per scoprire la presenza dell'**Agent**. Questo metodo può essere utilizzato come quello supplementare di scansione rapida nel caso se nella rete vi sono postazioni su cui le richieste ping vengono bloccate.

La scansione rapida viene eseguita in modo parallelo, quella normale viene eseguita in modo consecutivo.

La velocità dello **Scanner di rete** può essere molto diversa. Il tempo massimo di scansione viene calcolato nel seguente modo:

- ◆ per la scansione normale: $<N> * <timeout>$,
- ◆ per la scansione rapida: $<N>/40 + 2 * <timeout>$,

dove: $<N>$ - numero di postazioni, $<timeout>$ - valore impostato nel campo **Time-out**.

2.4.2. Gestione licenze

Caratteristiche delle licenze

1. Non viene concessa la licenza di **Server Dr.Web**. Il **Server** può essere installato senza la chiave di licenza. La chiave può essere aggiunta in seguito localmente o può essere ricevuta attraverso la comunicazione tra i server.



L'UUID del **Server** che nelle versioni precedenti di **Dr.Web Enterprise Security Suite** veniva conservato nella chiave di licenza del **Server**, a partire dalla versione **10.0** viene conservato nel file di configurazione del **Server**.

- Quando viene installato un nuovo **Server**, viene generato un nuovo UUID.
- Quando il **Server** viene aggiornato dalle versioni precedenti, l'UUID viene preso automaticamente dalla chiave del **Server** della versione precedente (file `enterprise.key` nella cartella `etc` dell'installazione precedente di **Server**) e viene registrato nel file di configurazione del **Server** che viene installato.

Se viene aggiornato un cluster dei **Server**, il **Server** responsabile dell'aggiornamento del database riceve la chiave di licenza, mentre per gli altri **Server** le chiavi di licenza devono essere aggiunte manualmente.

2. Le chiavi di licenza sono necessarie soltanto per le postazioni protette. Si possono assegnare i file della chiave sia a singole postazioni, che ai gruppi di postazioni: in questo caso, la chiave di licenza è valida per tutte le postazioni che la ereditano da questo gruppo. Per assegnare il file della chiave contemporaneamente a tutte le postazioni della rete antivirus, per le quali non sono state assegnate le impostazioni individuali della chiave di licenza, assegnare la chiave di licenza al gruppo **Everyone**.
3. Attraverso la comunicazione tra i server, è possibile trasferire il numero facoltativo di licenze dalle chiavi conservate su un **Server** a un **Server** adiacente per un determinato periodo.
4. Ogni chiave di licenza può essere assegnata contemporaneamente a più oggetti di licenza (gruppi e postazioni). Allo stesso oggetto di licenza è possibile assegnare contemporaneamente più chiavi di licenza.



5. Quando vengono assegnate più chiavi ad un oggetto, prestare attenzione alle seguenti particolarità:
 - a) Se l'elenco dei componenti antivirus consentiti è diverso in diverse chiavi dello stesso oggetto, l'elenco dei componenti consentiti per le postazioni viene determinato tramite l'intersezione degli insiemi dei componenti nelle chiavi. Per esempio, se a un gruppo di postazioni sono state assegnate una chiave con il supporto dell'**Antispam** ed una senza il supporto dell'**Antispam**, l'installazione dell'**Antispam** sulle postazioni è vietata.
 - b) Le impostazioni di licenza di un oggetto vengono calcolate sulla base di tutte le chiavi assegnate a quest'oggetto. Se le scadenze delle chiavi di licenza sono diverse, una volta scaduta la chiave con la scadenza più vicina, è necessario sostituire od eliminare manualmente la chiave scaduta. Se la chiave scaduta limitava l'installazione dei componenti antivirus, è necessario modificare le impostazioni di licenza dell'oggetto nella sezione [Componenti da installare](#).
 - c) Il numero di licenze di un oggetto viene calcolato dalla somma delle licenze di tutte le chiavi assegnate a quest'oggetto. Inoltre, si deve tenere conto della possibilità di trasferire licenze attraverso la comunicazione tra i server su un **Server** adiacente (v. p. 3). In questo caso, dal numero totale di licenze vengono sottratte le licenze trasferite sul **Server** adiacente.

Il file contenente la chiave di licenza viene impostato durante l'installazione di **Server Dr.Web** (v. **Guida all'installazione**, p. [Installazione di Server Dr.Web](#)). In seguito, si potranno ottenere nuove chiavi, per esempio una con una durata di licenza più lunga od una con un altro set dei componenti antivirus per le postazioni protette.



Il file della chiave ha un formato protetto dalle modifiche tramite la firma digitale. Le modifiche del file lo rendono non valido. Per evitare che il file della chiave si danneggi casualmente, non si deve modificarlo e/o salvarlo dopo averlo aperto in un editor di testo.

Interfaccia della Gestione licenze

La **Gestione licenze** fa parte del **Pannello di controllo**. Questo componente si utilizza per gestire le licenze degli oggetti della rete antivirus.

Per aprire la finestra **Gestione licenze**, nel menu principale del **Pannello di controllo** selezionare la voce **Amministrazione**, nella finestra che si è aperta selezionare la voce del [menu di gestione Gestione licenze](#).




Lista gerarchica delle chiavi

La finestra principale **Gestione licenze** contiene l'albero delle chiavi – una lista gerarchica i cui nodi sono le chiavi di licenza, nonché le postazioni e i gruppi a cui sono state assegnate le chiavi di licenza.

La barra degli strumenti contiene i seguenti elementi di gestione:

Opzione	Descrizione	A seconda degli oggetti nell'albero delle chiavi
Aggiungi chiave	Per aggiungere un nuovo record di una chiave di licenza.	L'opzione è sempre disponibile. Le funzioni dipendono da ciò se l'oggetto è selezionato o meno nell'albero delle chiavi (v. Aggiunzione della nuova chiave di licenza).
Rimuovi gli oggetti selezionati	Per cancellare la correlazione tra una chiave e un oggetto di licenza.	L'opzione è disponibile se nell'albero sono selezionati un oggetto di licenza (postazione o gruppo) o una chiave di licenza.



Opzione	Descrizione	A seconda degli oggetti nell'albero delle chiavi
 Propaga la chiave verso i gruppi e le postazioni	Per sostituire una chiave con la chiave selezionata o per aggiungere la chiave selezionata ad un oggetto di licenza.	L'opzione è disponibile se nell'albero è selezionata una chiave di licenza.
 Esporta chiave	Per salvare una copia locale del file della chiave di licenza.	
 Propaga la chiave verso i Server adiacenti	Per trasferire le licenze dalla chiave selezionata ai Server adiacenti.	

 **Le Impostazioni della vista albero** consentono di modificare l'aspetto dell'albero gerarchico:

- ◆ Il flag **Mostra il numero di licenze** attiva/disattiva la visualizzazione nell'albero del numero totale di licenze erogate dai file della chiave.
- ◆ Per modificare la struttura dell'albero, utilizzare le seguenti opzioni:
 - L'opzione **Chiavi** comanda di visualizzare tutte le chiavi di licenza della rete antivirus come nodi radice dell'albero gerarchico. Elementi nidificati delle chiavi di licenza sono tutti i gruppi e tutte le postazioni a cui queste chiavi sono state assegnate. Questa vista ad albero è quella base e consente di gestire gli oggetti di licenza e le chiavi di licenza.
 - L'opzione **Gruppi** comanda di visualizzare come nodi radice dell'albero gerarchico quei gruppi a cui le chiavi di licenza sono state assegnate direttamente. Elementi nidificati dei gruppi sono le postazioni incluse in questi gruppi e le chiavi di licenza assegnate a questi gruppi. Questa vista ad albero si utilizza per visualizzare le informazioni sulla licenza in un modo più comodo e non consente di gestire gli oggetti dell'albero.

Gestione delle licenze

Tramite la Gestione licenze, si possono eseguire le seguenti azioni con le chiavi di licenza:

1. [Visualizzare le informazioni sulla licenza.](#)
2. [Aggiungere una nuova chiave di licenza.](#)
3. [Aggiornare una chiave di licenza.](#)
4. [Sostituire una chiave di licenza.](#)
5. [Ampliare la lista delle chiavi di licenza di un oggetto.](#)
6. [Eliminare una chiave di licenza e cancellare l'oggetto dalla lista delle licenze.](#)
7. [Trasferire licenze su un Server adiacente.](#)
8. [Modificare le licenze trasferite su un Server adiacente.](#)

Visualizzare le informazioni sulla licenza

Per visualizzare le informazioni riassuntive su una chiave di licenza, nella finestra principale **Gestione licenze** selezionare l'account della chiave di cui si vogliono visualizzare le informazioni (fare clic sul nome dell'account della chiave). Il pannello che si è aperto contiene le informazioni quali:


- ◆ utente della licenza,
- ◆ venditore da cui è stata acquistata la licenza,
- ◆ identificatore e numero di serie della licenza,
- ◆ scadenza della licenza,
- ◆ viene indicato se la licenza comprende il supporto del modulo **Antispam**,
- ◆ numero di postazioni indicato nel file della chiave per cui è stata concessa la licenza,



- ◆ MD5 hash della chiave di licenza,
- ◆ lista dei componenti antivirus che la licenza consente di utilizzare.

Aggiungere una nuova chiave di licenza

Per aggiungere una nuova chiave di licenza:


1. Nella finestra principale della **Gestione licenze** premere il pulsante **+ Aggiungi chiave** nella barra degli strumenti.
2. Nel pannello che si è aperto, fare clic sul pulsante  e selezionare un file della chiave di licenza.
3. Premere il pulsante **Salva**.
4. La chiave di licenza viene aggiunta all'albero delle chiavi, però non viene correlata con alcun oggetto. In questo caso, per impostare gli oggetti di licenza, seguire le procedure [Sostituire una chiave di licenza](#) o [Ampliare la lista delle chiavi di licenza di un oggetto](#) descritte sotto.

Aggiornare una chiave di licenza

In caso di aggiornamento di una chiave di licenza, la nuova chiave di licenza verrà assegnata agli stessi oggetti di licenza per i quali valeva la chiave che viene aggiornata.

Adoperare la procedura di aggiornamento chiave per sostituire una chiave scaduta o per sostituire una chiave con un'altra che ha un altro elenco dei componenti da installare, mentre la struttura dell'albero delle chiavi si mantiene.


Per aggiornare una chiave di licenza:

1. Nella finestra principale **Gestione licenze** nell'albero delle chiavi selezionare la chiave che si vuole aggiornare.
2. Nel pannello delle proprietà della chiave, che si è aperto, fare clic sul pulsante  e selezionare il file della chiave di licenza.
3. Fare clic sul pulsante **Salva**. Si apre la finestra delle impostazioni dei componenti da installare, descritta nella sottosezione [Impostazioni per la sostituzione della chiave di licenza](#).
4. Fare clic sul pulsante **Salva** per aggiornare la chiave di licenza.

Sostituire una chiave di licenza

In caso di sostituzione della chiave di licenza, tutte le chiavi di licenza correnti dell'oggetto di licenza vengono cancellate e la nuova chiave viene aggiunta.

Per sostituire la chiave di licenza corrente:


1. Nella finestra principale **Gestione licenze** nell'albero delle chiavi selezionare la chiave che si vuole assegnare a un oggetto di licenza.
2. Nella barra degli strumenti fare clic sul pulsante  **Propaga la chiave verso i gruppi e le postazioni**. Si apre la finestra con la lista gerarchica delle postazioni e dei gruppi della rete antivirus.
3. Selezionare dalla lista gli oggetti di licenza. Per selezionare più postazioni e gruppi, utilizzare i tasti CTRL e MAIUSCOLO.
4. Fare clic sul pulsante **Sostituisci la chiave**. Si apre la finestra delle impostazioni dei componenti da installare, descritta nella sottosezione [Impostazioni per la sostituzione della chiave di licenza](#).
5. Fare clic sul pulsante **Salva** per sostituire la chiave di licenza.



Ampliare la lista delle chiavi di licenza di un oggetto

In caso di aggiunta di una chiave di licenza, tutte le chiavi correnti dell'oggetto di licenza vengono preservate e la nuova chiave di licenza viene aggiunta alla lista delle chiavi.

Per aggiungere una chiave di licenza all'elenco delle chiavi di licenza dell'oggetto:


1. Nella finestra principale **Gestione licenze** nell'albero delle chiavi selezionare la chiave che si vuole aggiungere all'elenco delle chiavi dell'oggetto.
2. Nella barra degli strumenti fare clic sul pulsante  **Propaga la chiave verso i gruppi e le postazioni**. Si apre la finestra con la lista gerarchica delle postazioni e dei gruppi della rete antivirus.
3. Selezionare dalla lista gli oggetti di licenza. Per selezionare più postazioni e gruppi, utilizzare i tasti CTRL e MAIUSCOLO.
4. Fare clic sul pulsante **Aggiungi chiave**. Si apre la finestra delle impostazioni dei componenti da installare, descritta nella sottosezione [Impostazioni per l'aggiunta di una chiave di licenza alla lista della chiavi](#).
5. Fare clic sul pulsante **Salva** per aggiungere la chiave di licenza.

Eliminare una chiave di licenza e cancellare l'oggetto dalla lista delle licenze



Non è possibile cancellare l'ultimo account della chiave del gruppo **Everyone**.


Per cancellare una chiave di licenza o un oggetto dalla lista delle licenze:

1. Nella finestra principale **Gestione licenze** selezionare la chiave che si vuole cancellare o selezionare l'oggetto (postazione o gruppo) a cui è stata assegnata questa chiave e fare clic sul pulsante  **Rimuovi gli oggetti selezionati** nella barra degli strumenti. Tenere presente che:
 - Se è stato selezionato un oggetto di licenza, esso viene cancellato dalla lista degli oggetti a cui è assegnata la stessa chiave. Se la chiave è stata assegnata come l'impostazione individuale a un oggetto, l'oggetto eredita la chiave di licenza dal gruppo.
 - Se è stata selezionata una chiave di licenza, l'account della chiave viene rimosso dalla rete antivirus. Tutti gli oggetti a cui è stata assegnata questa chiave ereditano la chiave di licenza dal gruppo.
2. Si apre la finestra delle impostazioni dei componenti da installare, descritta nella sottosezione [Impostazioni per la sostituzione della chiave di licenza](#).
3. Fare clic sul pulsante **Salva** per cancellare l'oggetto selezionato e per attivare l'ereditarietà della chiave.

Trasferire licenze su un Server adiacente

Se una parte delle licenze libere nella chiave di licenza su un **Server** viene trasferita su un **Server** adiacente, il numero di licenze trasferito sarà non disponibile per l'uso su questo **Server** fino alla fine del periodo di distribuzione di queste licenze.

Per trasferire licenze su un Server adiacente:

1. Nella finestra principale **Gestione licenze** nell'albero delle chiavi selezionare la chiave di cui le licenze libere si vogliono trasferire su un **Server** adiacente.
2. Nella barra degli strumenti fare clic sul pulsante  **Propaga la chiave verso i Server adiacenti**. Si apre la finestra con la lista gerarchica dei **Server** adiacenti.



3. Selezionare dalla lista i **Server** su cui si vogliono distribuire le licenze.
4. Di fronte a ciascun **Server**, configurare i seguenti parametri:
 - **Numero di licenze** – numero di licenze libere che si vuole trasferire da questa chiave su un **Server** adiacente.
 - **Data della scadenza della licenza** – periodo per cui vengono trasferite le licenze. Dopo il periodo indicato, tutte le licenze verranno richiamate dal **Server** adiacente e tornano nella lista delle licenze libere di questa chiave di licenza.
5. Fare clic su uno dei pulsanti:
 - **Aggiungi chiave** – per aggiungere le licenze alla lista delle licenze disponibili dei **Server** adiacenti. Si apre la finestra delle impostazioni dei componenti da installare, descritta nella sottosezione [Impostazioni per l'aggiunta di una chiave di licenza alla lista della chiavi](#).
 - **Sostituisci la chiave** – per cancellare le licenze correnti dei **Server** adiacenti e per assegnare ad essi soltanto le licenze che vengono distribuite. Si apre la finestra delle impostazioni dei componenti da installare, descritta nella sottosezione [Impostazioni per la sostituzione della chiave di licenza](#).
6. Fare clic sul pulsante **Salva** per distribuire le licenze sui **Server** adiacenti.

Modificare le licenze trasferite su un Server adiacente

Per modificare le licenze distribuite su un Server adiacente:

1. Nella finestra principale **Gestione licenze** nell'albero delle chiavi selezionare il **Server** adiacente su cui sono state distribuite le licenze.
2. Nel pannello delle proprietà che si è aperto, modificare i seguenti parametri:
 - **Numero di licenze** - numero di licenze libere trasferite dalla chiave di questo **Server** sul **Server** adiacente.
 - **Data della scadenza della licenza** - periodo per cui vengono trasferite le licenze. Dopo il periodo indicato, tutte le licenze verranno richiamate dal **Server** adiacente e tornano nella lista delle licenze libere della chiave di licenza corrente.
3. Fare clic sul pulsante **Salva** per aggiornare le informazioni sulle licenze distribuite.

Modificare la lista dei componenti da installare

Impostazioni per la sostituzione della chiave di licenza

In questa sottosezione, è descritta la configurazione dei componenti da installare quando vengono eseguite le procedure:

- ◆ Aggiornare una chiave di licenza.
- ◆ Sostituire una chiave di licenza.
- ◆ Cancellare una chiave di licenza.
- ◆ Trasferire licenze su un **Server** adiacente sostituendone la chiave.

Nell'esecuzione di queste procedure, per configurare i componenti da installare:

1. Nella finestra di configurazione dei componenti da installare nella lista degli oggetti sono riportati:
 - Postazioni e gruppi con i suoi elenchi dei componenti da installare.
 - Nella colonna **Chiave corrente** sono riportate la lista delle chiavi dell'oggetto e le impostazioni dei componenti da installare che attualmente valgono per l'oggetto.
 - Nella colonna **Chiave che viene assegnata** sono riportate la chiave e le impostazioni dei componenti da installare, definite nella chiave che verrà assegnata agli oggetti selezionati.



2. Se necessario, spuntare il flag **Mostra soltanto ciò che differisce** affinché nella lista vengano visualizzati soltanto quei componenti le cui impostazioni sono diverse nella chiave corrente e in quella che viene assegnata.
3. Per configurare la lista dei componenti da installare:

a) Nella colonna **Chiave che viene assegnata** si può configurare una lista riassuntiva dei componenti da installare.

- Le impostazioni dei componenti da installare nella colonna **Chiave che viene assegnata** vengono calcolate sulla base di ciò se l'utilizzo di un componente è consentito (+) o non è consentito (-) nelle impostazioni correnti e nella chiave nuova nel seguente modo:

Impostazioni correnti	Impostazioni della chiave che viene assegnata	Impostazioni risultanti
+	+	+
-	+	+
+	-	-
-	-	-

- Si possono modificare le impostazioni dei componenti da installare (abbassare i permessi di installazione) solo se nelle impostazioni calcolate nella colonna **Chiave che viene assegnata** l'utilizzo di questo componente è consentito.

b) Spuntare i flag corrispondenti a quegli oggetti (postazioni e gruppi) per cui l'ereditarietà delle impostazioni verrà disattivata e verranno assegnate le impostazioni dei componenti da installare dalla colonna **Chiave che viene assegnata** come quelle individuali. Per gli altri oggetti (per cui i flag non sono messi) verrà assegnata l'ereditarietà delle impostazioni originarie dalla colonna **Chiave che viene assegnata**.

Impostazioni per l'aggiunta di una chiave di licenza alla lista della chiavi

In questa sottosezione, è descritta la configurazione dei componenti da installare quando vengono eseguite le procedure:

- ◆ Ampliare la lista delle chiavi di licenza di un oggetto.
- ◆ Trasferire licenze su un **Server** adiacente aggiungendo la chiave.

Nell'esecuzione di queste procedure, per configurare i componenti da installare:

1. Nella finestra di configurazione dei componenti da installare nella lista degli oggetti sono riportati:
 - Postazioni e gruppi con i suoi elenchi dei componenti da installare.
 - Nella colonna **Chiave corrente** sono riportate la lista delle chiavi dell'oggetto e le impostazioni dei componenti da installare che attualmente valgono per l'oggetto.
 - Nella colonna **Chiave che viene assegnata** sono riportate la chiave e le impostazioni dei componenti da installare, definite nella chiave che si vuole aggiungere per gli oggetti selezionati.
2. Se necessario, spuntare il flag **Mostra soltanto ciò che differisce** affinché nella lista vengano visualizzati soltanto quei componenti le cui impostazioni sono diverse nella chiave corrente e in quella che viene ereditata. Notare che nella sezione **Chiave che viene assegnata** sono riportate non le impostazioni della chiave che viene assegnata, ma le impostazioni risultanti dei componenti da installare.
3. Per configurare la lista dei componenti da installare:
 - a) Nella colonna **Chiave che viene assegnata** si può configurare una lista riassuntiva dei componenti da installare.
 - Le impostazioni dei componenti da installare nella colonna **Chiave che viene assegnata** vengono calcolate sulla base di ciò se l'utilizzo di un componente è consentito (+) o non è consentito (-) nelle impostazioni correnti e nella chiave nuova nel seguente modo:



Impostazioni correnti	Impostazioni della chiave che viene assegnata	Impostazioni risultanti
+	+	+
-	+	-
+	-	-
-	-	-

- Si possono modificare le impostazioni dei componenti da installare (abbassare i permessi di installazione) solo se nelle impostazioni calcolate nella colonna **Chiave che viene assegnata** l'utilizzo di questo componente è consentito.
- b) Spuntare i flag corrispondenti a quegli oggetti (postazioni e gruppi) per cui l'ereditarietà delle impostazioni verrà disattivata e verranno assegnate le impostazioni dei componenti da installare dalla colonna **Chiave che viene assegnata** come quelle individuali. Per gli altri oggetti (per cui i flag non sono messi) verrà assegnata l'ereditarietà delle impostazioni dalla colonna **Chiave che viene assegnata**.

2.5. Schema interazione dei componenti della rete antivirus

In [immagine 2-2](#) è rappresentato lo schema generale di una parte di rete antivirus.

Questo schema visualizza una rete antivirus che include soltanto un **Server**. In grandi aziende, è preferibile installare una rete antivirus con diversi **Server** per il bilanciamento di carico tra di essi.

In questo esempio la rete antivirus è stata implementata in una rete locale, però per l'installazione e il funzionamento di **Dr.Web Enterprise Security Suite** e dei pacchetti antivirus non è necessario che i computer si trovino in una rete locale, è sufficiente l'accesso Internet.

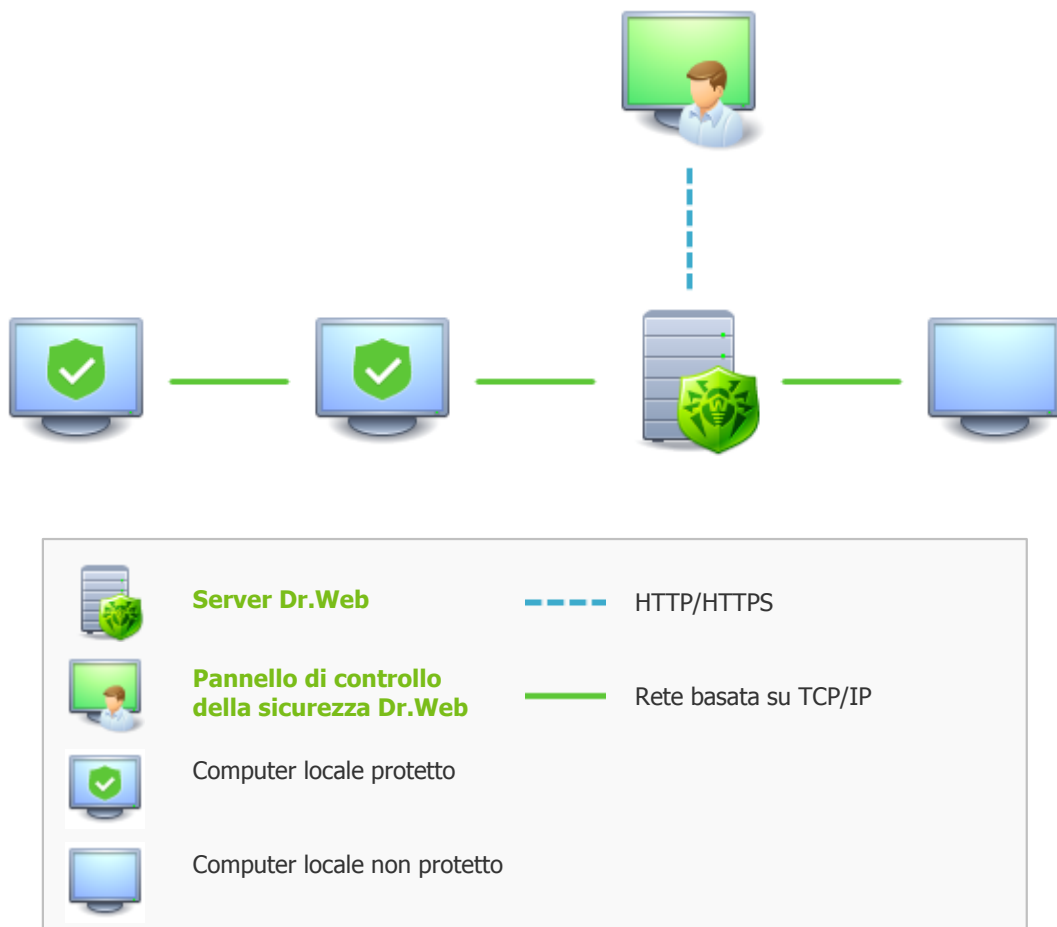


Immagine 2-2. Struttura della rete antivirus

Quando il Server Dr.Web viene eseguita la seguente sequenza di azioni:

1. Vengono caricati i file di **Server Dr.Web** dalla directory `bin`.
2. Viene caricato lo **Scheduler** del **Server**.
3. Vengono caricate la cartella di installazione centralizzata e la cartella di aggiornamenti, viene avviato il sistema di informazione del segnale (sistema di avvisi).
4. Viene controllata l'integrità del database del **Server**.
5. Vengono eseguiti i task dello **Scheduler** del **Server**.
6. Attesa delle informazioni dagli **Agent Dr.Web** e dei comandi dai **Pannelli di controllo**.

L'intero flusso dei comandi, dei dati e delle informazioni statistiche nella rete antivirus passa necessariamente attraverso il **Server Dr.Web**. Anche il **Pannello di controllo** scambia informazioni solamente con il **Server**; il **Server** modifica la configurazione di una postazione e manda comandi all'**Agent Dr.Web** sulla base dei comandi del **Pannello di controllo**.

In questo modo, la parte di rete antivirus ha la struttura logica rappresentata in [immagine 2-3](#).

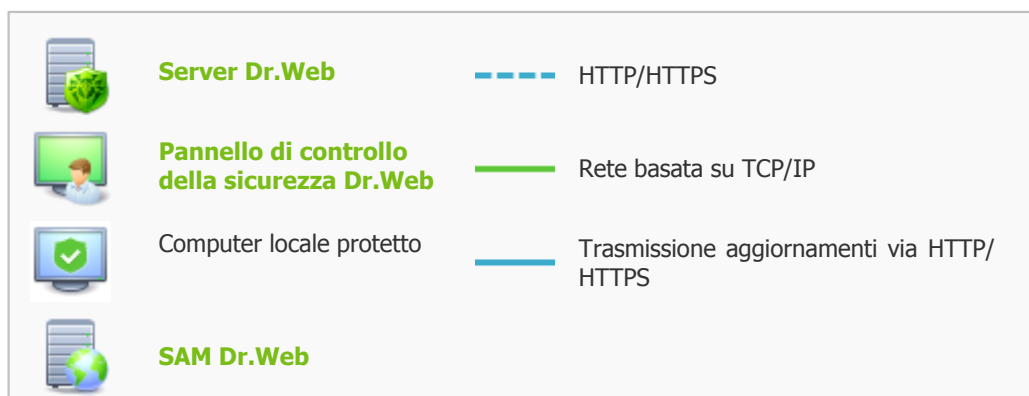
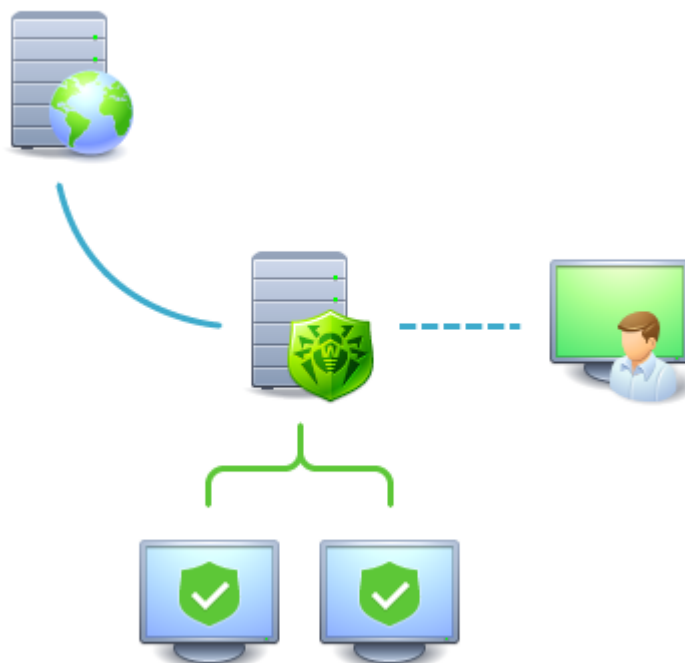


Immagine 2-3. Struttura logica della rete antivirus

Tra il **Server** e le postazioni (una linea continua sottile in [immagine 2-3](#)) vengono trasmessi:

- ◆ le query dell'**Agent** per ottenere il calendario centralizzato e il calendario centralizzato di questa postazione,
- ◆ le impostazioni dell'**Agent** e del pacchetto antivirus,
- ◆ le query per ottenere i task ordinari da eseguire (scansione, aggiornamento dei database dei virus ecc),
- ◆ i file dei pacchetti antivirus – quando l'**Agent** ha ricevuto il task di installazione,
- ◆ gli aggiornamenti del software e dei database dei virus – nel corso dell'esecuzione del task di aggiornamento,
- ◆ gli avvisi dell'**Agent** sulla configurazione della postazione,
- ◆ le statistiche del funzionamento dell'**Agent** e dei pacchetti antivirus che verranno incluse nel log centralizzato,
- ◆ gli avvisi su eventi dei virus e su altri eventi da registrare.



A seconda delle impostazioni e dalla quantità di postazioni, il volume di traffico tra le postazioni e il **Server** può essere abbastanza grande. La rete antivirus **Dr.Web Enterprise Security Suite** prevede la possibilità di compressione di traffico. L'utilizzo di questa modalità opzionale è descritta sotto v. p. [Utilizzo della codifica e della compressione di traffico](#).

Il traffico tra il **Server** e la postazione può essere codificato. Consente di evitare la divulgazione delle informazioni trasmesse via il canale descritto e la sostituzione del software che viene caricato sulle postazioni. Di default, questa possibilità è attivata. L'utilizzo di questa modalità è descritta sotto v. p. [Utilizzo della codifica e della compressione di traffico](#).

Dal server web di aggiornamenti a **Server Dr.Web** (linea continua spessa in [immagine 2-3](#)) attraverso il protocollo HTTP vengono trasmessi i file necessari per la replica delle cartelle centralizzate di installazione e di aggiornamento, nonché le informazioni di servizio sullo stato di tale processo. L'integrità delle informazioni trasmesse (dei file del software **Dr.Web Enterprise Security Suite** e dei pacchetti antivirus) è assicurata dall'utilizzo del metodo checksum: un file danneggiato o sostituito durante la trasmissione non sarà accettato dal **Server**.

Tra il **Server** e il **Pannello di controllo** (linea tratteggiata in [immagine 2-3](#)) vengono trasmesse le informazioni sulla configurazione del **Server** (comprese le informazioni sulla topologia di rete) e le impostazioni delle postazioni. Queste informazioni vengono visualizzate nel **Pannello di controllo** e se qualche impostazione è stata modificata dall'utente (dall'amministratore della rete antivirus), le informazioni sulle modifiche apportate vengono trasmesse sul **Server**.

La connessione del **Pannello di controllo** con il **Server** selezionato viene stabilita soltanto dopo che l'amministratore di rete antivirus si è autenticato, inserendo il nome di registrazione e la password su tale **Server**.



Capitolo 3: Introduzione all'uso. Generalità

3.1. Creazione di una rete antivirus semplice



Prima di iniziare di utilizzare il software antivirus, è consigliabile modificare le impostazioni della directory per il backup di dati critici del **Server** (v. [Configurazione del calendario di Server Dr.Web](#)). Si consiglia di posizionare questa directory su altro disco locale per diminuire i rischi della perdita contemporanea dei file del software **Server** e della copia di riserva.

Connessione attraverso il Pannello di controllo della sicurezza Dr.Web

Di default, il **Server Dr.Web** viene avviato automaticamente dopo l'installazione e dopo ogni riavvio del sistema operativo (v. inoltre p. [Server Dr.Web](#)).

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

Su qualunque computer che abbia una connessione di rete con il **Server Dr.Web**, 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 autenticazione, inserire il nome utente e la password dell'amministratore (il nome utente amministratore predefinito è **admin**, la password è la password che è stata impostata durante l'installazione del **Server**, v. **Guida all'installazione**, p. [Installazione di Server Dr.Web](#)).

Se si è riusciti a connettersi al **Server**, si apre la finestra principale del **Pannello di controllo**. In questa finestra vengono visualizzate le informazioni sulla rete antivirus che viene gestita da questo **Server** (per la descrizione dettagliata consultare il p. [Pannello di controllo della sicurezza Dr.Web](#)).

Gestione della rete antivirus

Tramite il **Pannello di controllo** si possono gestire il **Server** e la rete antivirus, in particolare è possibile:

- ◆ creare postazioni antivirus (v. in **Guida all'installazione**, p. [Installazione di Agent Dr.Web](#)),
- ◆ [approvare postazioni](#),
- ◆ modificare, configurare ed eliminare postazioni antivirus (v. [Capitolo 6: Gestione delle postazioni](#)),
- ◆ configurare e modificare le connessioni con i **Server Dr.Web** adiacenti (v. p. [Caratteristiche di una rete con diversi Server Dr.Web](#)),
- ◆ visualizzare i log di eventi e gli altri dati di questo **Server** e dei server adiacenti.

Gli strumenti principali di gestione sono concentrati nel menu principale, nel menu di gestione e nella barra degli strumenti (v. [Pannello di controllo della sicurezza Dr.Web](#)).



Connessione dell'Agent Dr.Web

Dopo che l'**Agent** è stato installato sulla postazione tramite il pacchetto d'installazione (v. **Guida all'installazione**, p. [File di installazione](#)), l'**Agent** cerca di connettersi al **Server Dr.Web**.

Con le impostazioni predefinite del **Server Dr.Web**, l'amministratore deve approvare manualmente le nuove postazioni in modo da registrarle sul **Server** (per maggiori informazioni sui criteri di approvazione di nuove postazioni, v. p. [Criteri di approvazione delle postazioni](#)). In questo caso, le nuove postazioni non vengono approvate automaticamente, ma vengono messe dal **Server** nel gruppo dei nuovi arrivi (v. p. [Gruppi di sistema e custom](#)).

Installazione del software antivirus

L'installazione di componenti del pacchetto antivirus sulla postazione procede senza l'intervento dell'amministratore.



Sulla postazione vengono installati i componenti del pacchetto antivirus indicati nelle impostazioni del gruppo primario della postazione (per maggiori informazioni v. p. [Componenti da installare del pacchetto antivirus](#)).

Per completare l'installazione di alcuni componenti di postazione antivirus, potrebbe essere richiesto il riavvio del computer. In questo caso sullo sfondo dell'icona di **Agent Dr.Web** nella **Barra degli applicazioni** appare un punto esclamativo nel triangolo giallo (v. anche [Agent Dr.Web](#)).

3.2. Configurazione delle connessioni di rete

Informazioni generali

Al **Server Dr.Web** si connettono i seguenti client:

- ◆ **Agent Dr.Web**,
- ◆ **Installer di rete degli Agent Dr.Web**,
- ◆ altri **Server Dr.Web**.

Una connessione viene sempre stabilita da parte del client.

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

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

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

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

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

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

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

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



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

Durante l'installazione del **Server** l'installer consente di aggiungere automaticamente le eccezioni alle impostazioni del firewall del sistema operativo Windows. Per farlo, basta spuntare il flag **Aggiungi le porte e le interfacce del server alle eccezioni del firewall**.

Se viene utilizzato un firewall diverso da quello del sistema operativo Windows, l'amministratore della rete antivirus deve configurarlo manualmente in modo opportuno.

3.2.1. Connessioni dirette

Configurazione del Server Dr.Web

Nelle impostazioni del **Server** deve essere indicato l'indirizzo (v. documento **Allegati**, p. [Allegato E. Specifica di indirizzo di rete](#)) da "ascoltare" per ricevere le connessioni TCP in arrivo.

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

Di default, per "l'ascolto" da parte del **Server** vengono impostati:

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



Notare: nelle versioni **Server 4.XX** veniva utilizzata la porta 2371. Nella versione **10.0** questa porta non è più supportata.

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

Configurazione dell'Agent Dr.Web

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

```
drwinst <Indirizzo_Server>
```

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

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



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

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

3.2.2. Servizio di rilevamento di Server Dr.Web

Con questo metodo di connessione, il client non conosce inizialmente l'indirizzo del **Server**. Ogni volta prima di stabilire la connessione, il cliente cerca il **Server** nella rete. Per farlo, il client invia nella rete una query broadcast e aspetta la risposta dal **Server** con indicazione del suo indirizzo. Dopo aver ricevuto la risposta, il client stabilisce la 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**.

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

1. Il **Server** viene registrato nel gruppo multicast con l'indirizzo indicato nelle impostazioni del **Server**.
2. Gli **Agent**, alla ricerca del **Server**, inviano nella rete le query multicast all'indirizzo di gruppo definito nel punto 1.

Di default, per "l'ascolto" da parte del **Server** vengono impostati (come per le connessioni dirette):

◆ `udp/231.0.0.1:2193`



Notare: nelle versioni **Server 4.XX** veniva utilizzata la porta 2371. Nella versione **10.0** questa porta non è più supportata.

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

3.2.3. Utilizzo del protocollo SRV

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

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

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



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

2. Quando viene richiesta una connessione al **Server**, l'utente imposta connessione tramite il protocollo `srv`.

Per esempio, l'esecuzione dell'installer di **Agent** con l'esplicita indicazione del **Server**:

```
drwinst srv/drwcs
```

3. Il client utilizza le funzioni del protocollo SRV nel modo trasparente per l'utente per connettersi al **Server**.



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



Capitolo 4: Amministratori della rete antivirus

Si consiglia di nominare amministratore della rete antivirus un dipendente affidabile, qualificato, con esperienza in amministrazione di una rete locale e con buone conoscenze della protezione antivirus. Tale dipendente deve avere l'accesso completo alle directory di installazione di **Server Dr.Web**. A seconda dei criteri di sicurezza della società e della disponibilità del personale, l'amministratore della rete antivirus deve avere i privilegi di amministratore di rete locale o deve lavorare a stretto contatto con tale amministratore.



Per la gestione operativa della rete antivirus, all'amministratore della rete antivirus non sono necessari i privilegi di amministratore sui computer inclusi in questa rete antivirus. Tuttavia, l'installazione e la disinstallazione remota del software **Agent** sono possibili soltanto in una rete locale e richiedono i privilegi di amministratore in questa rete, il debugging di **Server Dr.Web** richiede l'accesso completo alla directory d'installazione server.

4.1. Autenticazione di amministratori

Per connettersi al Server Dr.Web, gli amministratori possono autenticarsi nei seguenti modi:

1. Salvando le informazioni sugli amministratori nel database del **Server**.
2. Tramite Active Directory (nelle versioni del **Server** per SO Windows).
3. Utilizzando il protocollo LDAP.
4. Utilizzando il protocollo RADIUS.
5. Utilizzando PAM (solo nei SO della famiglia UNIX).

I modi di autenticazione vengono utilizzati consecutivamente secondo i seguenti principi:

1. L'ordine di utilizzo dei modi di autenticazione dipende dall'ordine in cui essi sono elencati nelle impostazioni definite tramite il **Pannello di controllo**.
2. Per primo viene eseguito il tentativo di autenticazione amministratore dal database del **Server**.
3. Come seconda, di default, viene utilizzata l'autenticazione tramite LDAP, come terza - tramite Active Directory, come quarta - tramite RADIUS. Nei SO della famiglia UNIX come quinta viene utilizzata l'autenticazione PAM.
4. Nelle impostazioni del **Server** i modi di autenticazione tramite LDAP, Active Directory e RADIUS possono essere scambiati di posto, ma all'inizio viene sempre utilizzato il tentativo di autenticazione dal database.
5. Di default, i modi di autenticazione tramite LDAP, Active Directory e RADIUS sono sempre disattivati.

Per modificare l'ordine di utilizzo dei metodi di autenticazione:

1. Selezionare la voce **Amministrazione** del menu principale del **Pannello di controllo**.
2. Nel menu di gestione selezionare la sezione **Autenticazione**.
3. Nella finestra che si è aperta, viene riportata la lista dei tipi di autenticazione nell'ordine in cui vengono utilizzati. Per modificare la sequenza, trascinare (drag'n'drop) i modi di autenticazione nella lista e metterli nell'ordine in cui si desidera utilizzarli.
4. Per rendere effettive le modifiche apportate, riavviare il **Server**.



Il nome utente amministratore deve essere unico.



Non è possibile connettere un amministratore tramite i sistemi di autenticazione esterni se sul **Server** esiste già un amministratore con lo stesso nome utente.

4.1.1. Autenticazione di amministratori del Server database

Il modo di autenticazione che salva i dati di amministratori nel database del **Server** viene utilizzato di default.

Per gestire la lista degli amministratori:

1. Selezionare la voce **Amministrazione** nel menu principale del **Pannello di controllo**.
2. Nel menu di gestione selezionare la sezione **Amministratori**. Si apre la lista di tutti gli amministratori del **Server**.

Per maggiori informazioni v. [Amministratori e gruppi di amministratori](#).

4.1.2. Autenticazione con utilizzo di Active Directory

Per attivare l'autenticazione tramite Active Directory:

1. Selezionare la voce **Amministrazione** del menu principale del **Pannello di controllo**.
2. Nel menu di gestione selezionare la sezione **Autenticazione**.
3. Nella finestra che si è aperta, entrare nella sezione **Microsoft Active Directory**.
4. Spuntare il flag **Utilizza autenticazione Microsoft Active Directory**.
5. Premere **Salva**.
6. Per rendere effettive le modifiche apportate, riavviare il **Server**.

Se viene utilizzata l'autenticazione di amministratori tramite Active Directory, nel **Pannello di controllo** viene impostato solo il permesso di utilizzo di questo modo di autenticazione.

Le proprietà di amministratori di Active Directory vengono modificate manualmente sul server Active Directory.

Per modificare gli amministratori di Active Directory:



Le seguenti operazioni vengono eseguite su un computer che ha lo snap-in per l'amministrazione di Active Directory.

1. Per poter modificare i parametri di amministratori, è necessario eseguire le seguenti azioni:
 - a) Per modificare lo schema di Active Directory, avviare l'utility `drweb-esuite-modify-ad-schema-xxxxxxxxxxxxxxxx-windows-nt-xYY.exe` (fa parte del pacchetto **Server Dr.Web**).
La modifica dello schema di Active Directory può richiedere un certo tempo. A seconda della configurazione del dominio, ci vogliono fino ai 5 minuti o più per sincronizzare e per applicare lo schema modificato.



Se in precedenza lo schema di Active Directory è stato modificato con utilizzo di questa utility dalla **6°** versione del **Server**, non è necessario modificarlo di nuovo con utilizzo dell'utility dalla **10.0** versione del **Server**.

- b) Per registrare lo snap-in Active Directory Schema (lo Schema di Active Directory), eseguire con i permessi di amministratore il comando `regsvr32 schmmgmt.dll`, dopodiché avviare `mmc` e aggiungere lo snap-in **Active Directory Schema**.



- c) Utilizzando lo snap-in Active Directory Schema, aggiungere alla classe **User** e (se necessario) alla classe **Group** la classe ausiliaria **DrWebEnterpriseUser**.



Se l'applicazione di schema modificato non è ancora finita, la classe **DrWebEnterpriseUser** potrebbe risultare non trovata. In questo caso aspettare per un tempo e ripetere il tentativo secondo il punto **c)**.

- d) Con i permessi di amministratore avviare il file `drweb-esuite-aduac-xxxxxxxxxxxxxxxx-
windows-nt-xYY.msi` (fa parte del pacchetto **Dr.Web Enterprise Security Suite 10.0**) e aspettare il compimento dell'installazione.
2. L'interfaccia grafica di modifica di attributi è disponibile nel pannello di controllo **Active Directory Users and Computers** → nella sezione **Users** → nella finestra di modifica delle proprietà dell'utente selezionato **Administrator Properties** → nella scheda **Dr.Web Authentication**.
 3. Per la modifica è disponibile il seguente parametro (il valore di attributo può essere **yes**, **no** o **not set**):
 - ◆ **User is administrator** - indica che l'utente è un amministratore con i permessi completi.



Gli algoritmi di principio di funzionamento e di analisi degli attributi di autenticazione sono riportati nel documento **Allegati**, in [Allegato C1](#).

4.1.3. Autenticazione con utilizzo di LDAP

Per attivare l'autenticazione tramite LDAP:

1. Selezionare la voce **Amministrazione** del menu principale del **Pannello di controllo**.
2. Nel menu di gestione selezionare la sezione **Autenticazione**.
3. Nella finestra che si è aperta, entrare nella sezione **Autenticazione LDAP**.
4. Spuntare il flag **Utilizza autenticazione LDAP**.
5. Premere **Salva**.
6. Per rendere effettive le modifiche apportate, riavviare il **Server**.

Si può configurare l'autenticazione tramite il protocollo LDAP su qualsiasi server LDAP. Inoltre, con utilizzo dello stesso meccanismo, si può configurare il **Server** sotto SO della famiglia UNIX per l'autenticazione in Active Directory tramite il controller di dominio.



Le impostazioni di autenticazione LDAP vengono salvate nel file di configurazione `auth-ldap.xml`.
I principali attributi xml di autenticazione sono descritti nel documento **Allegati**, in [Allegato C2](#).

A differenza di Active Directory, si può configurare il meccanismo per qualsiasi schema LDAP. Di default, si tenta di utilizzare gli attributi del **Dr.Web Enterprise Security Suite** definiti per Active Directory.

Il processo di autenticazione tramite LDAP consiste nel seguente:

1. L'indirizzo del server LDAP viene impostato attraverso il **Pannello di controllo** o nel file di configurazione xml.
2. Per il nome utente impostato vengono eseguite le seguenti azioni:
 - ◆ Il nome utente viene convertito in DN (Distinguished Name) tramite maschere simili a DOS (con utilizzo del carattere *), se sono impostate regole.
 - ◆ Il nome utente viene convertito in DN con utilizzo di espressioni regolari, se sono impostate regole.



- ◆ Viene utilizzato uno script custom di conversione di nomi in DN, se è specificato nelle impostazioni.
- ◆ Se non è adatta nessuna delle regole di conversione, il nome utente impostato viene utilizzato così com'è.



Il formato di impostazione di nome utente non viene definito o fissato in nessun modo - può essere lo stesso utilizzato dalla società, cioè non è richiesta la modifica coattiva dello schema LDAP. La conversione per tale schema viene eseguita con utilizzo di regole di conversione di nomi in LDAP DN.

3. Come in caso di autenticazione tramite Active Directory, dopo la conversione, si tenta di registrare questo utente sul server LDAP indicato con utilizzo del DN ottenuto e di una password inserita.
4. In seguito, così come in Active Directory, vengono letti gli attributi dell'oggetto LDAP per il DN ottenuto. Si possono ridefinire gli attributi e i valori possibili nel file di configurazione.
5. Se i valori di alcuni attributi dell'amministratore non sono stati definiti, se viene impostata l'ereditarietà (nel file di configurazione), la ricerca di attributi richiesti nei gruppi, di cui l'utente fa parte, viene eseguita così come nel caso quando viene utilizzato Active Directory.

4.1.4. Autenticazione con utilizzo di RADIUS

Per attivare l'autenticazione tramite RADIUS:

1. Selezionare la voce **Amministrazione** del menu principale del **Pannello di controllo**.
2. Nel menu di gestione selezionare la sezione **Autenticazione**.
3. Nella finestra che si è aperta, entrare nella sezione **Autenticazione RADIUS**.
4. Spuntare il flag **Utilizza autenticazione RADIUS**.
5. Premere **Salva**.
6. Per rendere effettive le modifiche apportate, riavviare il **Server**.

Per utilizzare il protocollo di autenticazione e di autorizzazione RADIUS, è necessario installare un server che mette in pratica questo protocollo, per esempio freeradius (per maggiori informazioni consultare <http://freeradius.org/>).

Nel **Pannello di controllo** vengono configurati i seguenti parametri dell'utilizzo di server RADIUS:

- ◆ **Server, Porta, Password** - parametri di connessione al server RADIUS: rispettivamente l'indirizzo IP/ il nome DNS, il numero di porta, la password (segreta) .
- ◆ **Timeout** - tempo di attesa di una risposta del server RADIUS, in secondi.
- ◆ **Numero di tentativi** - numero di tentativi di connessione al server RADIUS.

Inoltre, per configurare i parametri aggiuntivi di RADIUS, si possono utilizzare:

- ◆ File di configurazione `auth-radius.xml` situato nella directory `etc` del **Server**.

Oltre ai parametri configurati tramite il **Pannello di controllo**, nel file di configurazione si può impostare il valore dell'identificatore NAS. Secondo la specifica RFC 2865, questo identificatore può essere utilizzato invece dell'indirizzo IP/del nome DNS come l'identificatore del client che si connette al server RADIUS. Nel file di configurazione l'identificatore si conserva nella seguente forma:

```
<!-- NAS identifier, optional, default - hostname -->  
<nas-id value="drwcs"/>
```

- ◆ Dizionario `dictionary.drweb` situato nella directory `etc` del **Server**.

Il dizionario conserva un set di attributi di RADIUS della società **Doctor Web** (VSA - Vendor-Specific Attributes).



4.1.5. Autenticazione con utilizzo di PAM

Per attivare l'autenticazione tramite PAM:

1. Selezionare la voce **Amministrazione** del menu principale del **Pannello di controllo**.
2. Nel menu di gestione selezionare la sezione **Autenticazione**.
3. Nella finestra che si è aperta, entrare nella **sezione** Autenticazione PAM.
4. Spuntare il flag **Utilizza autenticazione PAM**.
5. Premere **Salva**.
6. Per rendere effettive le modifiche apportate, riavviare il **Server**.

Nei sistemi operativi Unix, l'autenticazione PAM viene effettuata tramite plugin di autenticazione.

Per configurare parametri dell'autenticazione PAM, si possono utilizzare i seguenti metodi:

- ◆ Configurare il metodo di autenticazione tramite il **Pannello di controllo**: nella sezione **Amministrazione** → **Autenticazione** → **Autenticazione PAM**.
- ◆ File di configurazione `auth-pam.xml`, situato nella directory `etc` del **Server**. Esempio di file di configurazione:

```

...
<!-- Enable this authorization module -->
<enabled value="no" />
<!-- This authorization module number in the stack -->
<order value="50" />
<!-- PAM service name -->
<service name="drwcs" />
<!-- PAM data to be queried: PAM stack must return INT zero/non-zero -->
<admin-flag mandatory="no" name="DrWeb_ESuite_Admin" />
...

```

Descrizione dei parametri dell'autenticazione PAM che vengono configurati sul lato Dr.Web Enterprise Security Suite

Elemento Pannello controllo	di di	Elementi del file auth-pam.xml			Descrizione
		Blocco	Parametro	Valori ammissibili	
Flag Utilizza autenticazione PAM		<enabled>	value	yes no	Il flag che determina se verrà utilizzato il metodo di autenticazione PAM.
Utilizzare Drag and Drop		<order>	value	valore di numero intero concordato con i valori degli altri metodi	Il numero di sequenza dell'autenticazione PAM se vengono utilizzati più metodi di autenticazione.
Campo Nome del servizio		<service>	name	-	Il nome del servizio che verrà utilizzato per creare un contesto di PAM. PAM può leggere i criteri per questo servizio da <code>/etc/pam.d/<nome servizio></code> o da <code>/etc/pam.conf</code> se il file non esiste. Se il parametro non è impostato (il tag <service> non c'è nel file di configurazione), di default, viene utilizzato il nome <code>drwcs</code> .
Flag Il flag di controllo è obbligatorio		<admin-flag>	mandatory	yes no	Il parametro che determina se il file di controllo è obbligatorio per l'identificazione di un utente come amministratore. Di default, è <code>yes</code> .



Elemento Pannello controllo	di di	Elementi del file auth-pam.xml			Descrizione
		Blocco	Parametro	Valori ammissibili	
Campo Nome del flag di controllo		<code><admin-flag></code>	<code>name</code>	-	Stringa chiave in base alla quale verrà letto il flag dei moduli PAM. Di default, DrWeb_ESuite_Admin.

Quando si configurano i moduli di autenticazione PAM, utilizzare i parametri impostati sul lato **Dr.Web Enterprise Security Suite** e anche tenere presenti i valori che vengono attribuiti di default anche se nessun parametro è stato impostato.

4.2. Amministratori e gruppi di amministratori

Per aprire la sezione di gestione degli account amministratori, selezionare la voce **Amministrazione** del menu principale del **Pannello di controllo**, e nella finestra che si è aperta selezionare la voce del menu di gestione **Amministratori**.



La sezione **Amministratori** è disponibile a tutti gli amministratori del **Pannello di controllo**. Tuttavia, l'intero albero gerarchico degli amministratori è disponibile soltanto agli amministratori appartenenti al gruppo **Administrators** a cui è consentito il permesso di **Visualizzazione delle proprietà e della configurazione dei gruppi di amministratori**. Per gli altri amministratori, nell'albero gerarchico vengono mostrati soltanto il proprio gruppo e i sottogruppi con gli account che ne fanno parte.

Lista gerarchica degli amministratori

La lista gerarchica degli amministratori rispecchia una struttura ad albero dei gruppi di amministratori e degli account amministratori. Nodi di questa struttura sono i gruppi di amministratori e gli amministratori che ne fanno parte. Ciascun amministratore fa parte di solo un gruppo. Il livello di nidificazione di gruppi non è limitato.

Gruppi predefiniti

Dopo l'installazione del **Server**, due gruppi vengono creati in modo automatico:

- ◆ **Administrators**. Inizialmente nel gruppo rientra solo un amministratore **admin** con il completo set di permessi che viene creato automaticamente all'installazione del **Server** (v. sotto).
- ◆ **Newbies**. Inizialmente il gruppo è vuoto. In questo gruppo vengono messi automaticamente gli amministratori che utilizzano il tipo di autenticazione esterno tramite LDAP, Active Directory e RADIUS.

Di default, agli amministratori appartenenti al gruppo **Newbies** vengono assegnati i permessi di sola lettura.

Amministratori predefiniti

Dopo l'installazione del **Server**, un account amministratore viene creato in modo automatico:

Parametro	Valore
Nome utente	admin
Password	Viene impostata all'installazione del Server (passo 15 nella procedura di installazione).



Parametro	Valore
Permessi	Completo set di permessi.
Modifica dell'account	I permessi dell'amministratore non possono essere modificati, l'amministratore non può essere rimosso.

Visualizzazione di liste gerarchiche

- ◆ Nella lista gerarchica della rete antivirus: un amministratore vede soltanto quei gruppi custom che sono consentiti nel premesso **Visualizza le proprietà dei gruppi di postazioni**. Anche tutti i gruppi di sistema vengono visualizzati nell'albero della rete antivirus, ma in essi sono visibili soltanto le postazioni appartenenti ai gruppi custom dalla lista indicata.
- ◆ Nella lista gerarchica degli amministratori: un amministratore dal gruppo **Newbies** vede un albero di cui la radice è il gruppo in cui si trova, cioè vede gli amministratori dal suo gruppo e dai sottogruppi dello stesso. Un amministratore dal gruppo **Administrators** vede tutti gli amministratori a prescindere dai loro gruppi.

Permessi degli amministratori

Tutte le azioni degli amministratori nel **Pannello di controllo** vengono determinate da un set di permessi che può essere assegnato a un singolo account oppure a un gruppo di amministratori.

Il sistema dei permessi da amministratore include le seguenti possibilità di gestione dei permessi:

- **Assegnazione dei permessi**

I permessi vengono assegnati durante la creazione di amministratore o di gruppo di amministratori. L'account o il gruppo eredita permessi dal gruppo padre in cui viene messo quando viene creato. Durante la creazione non vi è la possibilità di modificare i permessi.

- **Ereditarietà dei permessi**

Di default, gli amministratori o i gruppi di amministratori ereditano permessi dal gruppo padre, ma l'ereditarietà può essere disattivata.

Per un account amministratore può essere impostato qualsiasi set di permessi individuali, e l'account eredita gli altri permessi dal gruppo padre a cui appartiene. Se l'amministratore o il gruppo eredita permessi, i suoi permessi non vengono sostituiti con quelli del gruppo padre, ma piuttosto il permesso viene ricalcolato sulla base di tutti i permessi dei gruppi padre che si trovano più in alto nell'albero gerarchico. La tabella di calcolo del permesso riassuntivo di un oggetto a seconda dell'ereditarietà e dei permessi dei gruppi padre è riportata nel documento **Allegati**, in [Allegato C3](#).

- **Modifica dei permessi**

Quando vengono creati amministratori e gruppi di amministratori, non vi è la possibilità di modificare i permessi. Si possono modificare i permessi soltanto degli oggetti già creati nella sezione delle impostazioni dell'account o del gruppo. Nella modifica si possono soltanto abbassare i permessi. Non è possibile modificare i permessi dell'amministratore predefinito **admin**.

La procedura di modifica di permessi è riportata nel p. [Modifica di account amministratori e di gruppi](#).



I permessi di amministratori e le sezioni del **Pannello di controllo** di cui concreti permessi sono responsabili sono descritti nel documento **Allegati**, in [Allegato C4](#).



4.3. Gestione degli account amministratori e dei gruppi di amministratori

4.3.1. Creazione ed eliminazione di account amministratori e di gruppi



Il nome utente amministratore deve essere unico.


Non è possibile connettere un amministratore tramite i sistemi di autenticazione esterni se sul **Server** esiste già un amministratore con lo stesso nome utente.

Aggiunzione di amministratori



Per poter creare nuovi account amministratori, si deve avere il permesso di **Creazione degli amministratori, dei gruppi di amministratori**.

Per aggiungere un nuovo account amministratore:

1. Selezionare la voce **Amministrazione** del menu principale del **Pannello di controllo**, nella finestra che si è aperta selezionare la voce del menu di gestione **Amministratori**.
2. Premere nella barra degli strumenti l'icona  **Crea account**. Si apre la finestra delle impostazioni dell'account che viene creato.
3. Nella sottosezione **Generali**, impostare i seguenti parametri:
 - ◆ Nel campo **Nome utente** indicare il nome utente amministratore da utilizzare per accedere al **Pannello di controllo**. Sono permesse le minuscole (a-z), le maiuscole (A-Z), le cifre (0-9), i caratteri "_" e ".".
 - ◆ Nell'elenco **Tipo di autenticazione** selezionare una delle varianti:
 - **Interna** - l'amministratore si autentica nel **Pannello di controllo** sulla base delle credenziali salvate nel database del **Server Dr.Web**.
 - **Esterna** - l'amministratore si autentica nel **Pannello di controllo** tramite i sistemi esterni LDAP, Active Directory, RADIUS o PAM.



Per maggiori informazioni consultare la sezione [Autenticazione di amministratori](#).

- ◆ Nei campi **Password** e **Digitare di nuovo la password** impostare la password di accesso al **Server** e al **Pannello di controllo**.



Nella password amministratore non possono essere utilizzati i caratteri di alfabeto nazionale.

- ◆ Nei campi **Cognome**, **Nome** e **Patronimico** si possono indicare i dati personali dell'amministratore.
- ◆ Dalla lista a cascata **Lingua interfaccia** selezionare la lingua dell'interfaccia del **Pannello di controllo**, che verrà utilizzata dall'amministratore che viene creato (di default, è la lingua impostata nel browser o l'inglese).



- ◆ Dalla lista a cascata **Formato della data** selezionare il formato che verrà utilizzato da questo amministratore quando modifica impostazioni che contengono date. Sono disponibili i seguenti formati:
 - europeo: DD-MM-YYYY HH:MM:SS
 - americano: MM/DD/YYYY HH:MM:SS
- ◆ Nel campo **Descrizione** si può impostare una descrizione dell'account.



I valori dei campi marcati con il carattere * devono essere impostati obbligatoriamente.

4. Nella sottosezione **Gruppi** viene impostato il gruppo padre di amministratori. Nella lista sono riportati i gruppi disponibili a cui si può assegnare l'amministratore. Un flag è spuntato di fronte al gruppo a cui verrà assegnato l'amministratore che viene creato. Di default, gli amministratori che vengono creati vengono messi nel gruppo padre dell'amministratore corrente. Per cambiare il gruppo impostato, spuntare il flag di fronte al gruppo desiderato.

Ciascun amministratore può rientrare in solo un gruppo.

L'amministratore eredita i permessi dal gruppo padre (v. p. [Permessi degli amministratori](#)).


5. Una volta impostati tutti i parametri necessari, premere il pulsante **Salva** per creare l'account amministratore.

Aggiunzione di gruppi di amministratori



Per poter creare gruppi di amministratori, si deve avere il permesso di **Creazione degli amministratori, dei gruppi di amministratori**.

Per aggiungere un nuovo account del gruppo di amministratori:

1. Selezionare la voce **Amministrazione** del menu principale del **Pannello di controllo**, nella finestra che si è aperta selezionare la voce del menu di gestione **Amministratori**.
2. Premere nella barra degli strumenti l'icona  **Crea un gruppo**. Si apre la finestra delle impostazioni del gruppo che viene creato.
3. Nella sottosezione **Generali**, impostare i seguenti parametri:
 - ◆ Nel campo **Gruppo** impostare il nome del gruppo di amministratori. Sono permesse le minuscole (a-z), le maiuscole (A-Z), le cifre (0-9), i caratteri "_" e ".".
 - ◆ Nel campo **Descrizione** si può impostare una descrizione del gruppo.
4. Nella sottosezione **Gruppi** viene impostato il gruppo padre di amministratori. Nella lista sono riportati i gruppi disponibili che possono essere assegnati come gruppo padre. Di fronte al gruppo, di cui farà parte il gruppo che viene creato, è spuntato un flag. Di default, i gruppi che vengono creati vengono messi nel gruppo padre dell'amministratore corrente. Per cambiare il gruppo impostato, spuntare il flag di fronte al gruppo desiderato.

Può essere assegnato solo un gruppo padre.

Il gruppo di amministratori eredita i permessi dal gruppo padre (v. p. [Permessi degli amministratori](#)).

5. Una volta impostati tutti i parametri necessari, premere il pulsante **Salva** per creare il gruppo di amministratori.



Eliminazione di amministratori e di gruppi di amministratori



Per poter eliminare account amministratori e gruppi di amministratori, si devono avere i permessi rispettivi di **Rimozione degli account amministratori** e di **Modifica delle proprietà e della configurazione dei gruppi di amministratori**.

Per eliminare un account amministratore o un gruppo:

1. Selezionare la voce **Amministrazione** del menu principale del **Pannello di controllo**, nella finestra che si è aperta selezionare la voce del menu di gestione **Amministratori**.
2. Nella lista gerarchica degli amministratori, selezionare l'account amministratore o il gruppo di amministratori che si vuole eliminare.
3. Nella barra degli strumenti premere l'icona **X** **Rimuovi gli oggetti selezionati**.

4.3.2. Modifica di account amministratori e di gruppi



Per poter modificare gli account amministratori e gruppi di amministratori, si devono avere i permessi rispettivamente di **Modifica degli account amministratori** e di **Modifica delle proprietà e della configurazione dei gruppi di amministratori**.

I valori dei campi marcati con il carattere * devono essere impostati obbligatoriamente.

Modifica degli amministratori

Per modificare un account amministratore:

1. Dalla lista degli amministratori, selezionare l'account che si vuole modificare. Quando si fa clic sul nome dell'account nella lista degli amministratori, si apre la sezione di modifica delle proprietà.
2. Nella sottosezione **Generali** si possono modificare i parametri che sono stati impostati durante la **creazione**, in particolare:
 - a) Per modificare la password di accesso all'account amministratore, nella barra degli strumenti selezionare l'icona **Cambia password**.



L'amministratore che ha i relativi permessi può modificare le password di tutti gli altri amministratori.



Nel nome utente amministratore non possono essere utilizzati i caratteri di alfabeto nazionale.

b) I seguenti parametri dell'amministratore sono di sola lettura:

- ◆ Data di creazione dell'account e data dell'ultima modifica dei parametri,
 - ◆ **Stato** - visualizza l'indirizzo di rete dell'ultima connessione sotto questo account.
3. Nella sottosezione **Gruppi** si può cambiare il gruppo di amministratori. Nella lista sono riportati i gruppi disponibili a cui può essere assegnato l'amministratore. Un flag è spuntato di fronte al gruppo padre corrente dell'amministratore. Per cambiare il gruppo impostato, spuntare il flag di fronte al gruppo desiderato.



Il gruppo padre deve essere assegnato obbligatoriamente a un amministratore. Ciascun amministratore può rientrare in solo un gruppo. L'amministratore eredita permessi dal gruppo padre impostato.

V. inoltre la sottosezione [Modifica dell'appartenenza](#).

4. Nella sottosezione **Permessi** si può modificare la lista delle azioni consentite all'amministratore. La procedura di modifica dei permessi è riportata nella sottosezione [Modifica dei permessi](#).
5. Per rendere effettive le modifiche apportate, premere il pulsante **Salva**.

Modifica dei gruppi di amministratori

Per modificare un gruppo di amministratori:

1. Dalla lista degli amministratori, selezionare il gruppo che si vuole modificare. Quando si fa clic sul nome del gruppo nella lista degli amministratori, si apre la sezione di modifica delle proprietà.
2. Nella sottosezione **Generali** si possono modificare i parametri che sono stati impostati durante la [creazione](#).
3. Nella sottosezione **Gruppi** si può cambiare il gruppo padre. Nella lista sono riportati i gruppi disponibili che possono essere assegnati come gruppo padre. Un flag è spuntato di fronte al gruppo padre corrente. Per cambiare il gruppo impostato, spuntare il flag di fronte al gruppo desiderato.

Il gruppo padre deve essere assegnato obbligatoriamente a un gruppo di amministratori. Il gruppo eredita permessi dal gruppo padre impostato.

V. inoltre la sottosezione [Modifica dell'appartenenza](#).

4. Nella sottosezione **Permessi** si può modificare la lista delle azioni consentite. La procedura di modifica dei permessi è riportata nella sottosezione [Modifica dei permessi](#).
5. Per rendere effettive le modifiche apportate, premere il pulsante **Salva**.

Modifica dei permessi

Per modificare i permessi degli amministratori e dei gruppi di amministratori nella sezione di modifica delle proprietà:

1. Per modificare l'ereditarietà, nell'intestazione della tabella dei permessi, colonna **Ereditarietà** fare clic su **attivato/disattivato** e dalla lista a cascata selezionare il valore desiderato.
2. La lista dei permessi è divisa in tre sottosezioni:
 - permessi di gestione delle postazioni/dei gruppi di postazioni,
 - permessi di gestione degli amministratori/dei gruppi di amministratori,
 - permessi con flag.
3. I permessi delle prime due sottosezioni possono essere modificati nelle colonne **Concesso** e **Negato**.

I permessi sono distribuiti nel seguente modo:

Contenuti della cella	Valore dei contenuti della colonna	
	Concesso	Negato
Nome gruppo o lista dei nomi di gruppi	Il permesso è concesso soltanto ai gruppi elencati	Il permesso è negato soltanto ai gruppi elencati



Contenuti della cella	Valore dei contenuti della colonna	
	Concesso	Negato
Tutti	Il permesso è concesso a tutti i gruppi	Il permesso è negato a tutti i gruppi
Nessuno	Il permesso non è concesso a nessuno dei gruppi	Il permesso non è negato a nessuno dei gruppi

Per modificare un permesso, fare clic sul valore della cella che contiene questo permesso. Si apre la finestra di scelta dei gruppi per cui il permesso è valevole. Dalla lista proposta selezionare uno dei due valori:

Nome impostazione	Azione in caso di assegnazione dell'impostazione
Alle postazioni	
Tutte	Assegnare l'impostazione del permesso a tutte le postazioni connesse a questo Server .
Selezionare un gruppo di postazioni	Assegnare l'impostazione del permesso soltanto alle postazioni nei gruppi selezionati. Per designare gruppi concreti, selezionare un gruppo con un singolo clic del mouse dalla lista Rete antivirus . Per selezionare diversi gruppi, utilizzare i tasti CTRL o SHIFT.
Agli amministratori	
Tutti	Assegnare l'impostazione del permesso a tutti gli amministratori di questo Server .
Selezionare un gruppo di amministratori	Assegnare l'impostazione del permesso soltanto agli amministratori nei gruppi di amministratori selezionati. Per designare gruppi concreti, selezionare un gruppo con un singolo clic del mouse dalla lista Amministratore . Per selezionare diversi gruppi, utilizzare i tasti CTRL o SHIFT.

4. Per gestire i permessi dalla terza sottosezione, in una delle colonne **Concesso** e **Proibito** spuntare il flag di fronte a un permesso per consentire o vietare rispettivamente questo permesso agli amministratori del gruppo di amministratori che viene modificato.
5. Per applicare l'impostazione selezionata, premere il pulsante **Salva**.

Modifica dell'appartenenza

Vi sono diversi modi di assegnazione del gruppo padre agli amministratori e ai gruppi di amministratori:

1. Si possono modificare le impostazioni dell'amministratore o del gruppo secondo il modo descritto [sopra](#).
2. Si può trascinare (drag'n'drop) un amministratore o un gruppo di amministratori nella lista gerarchica sopra il gruppo il quale si desidera assegnare come gruppo padre.



Capitolo 5: Gestione integrata delle postazioni

Il metodo di gruppi è progettato per la semplificazione della gestione delle postazioni della rete antivirus.

L'unione delle postazioni in gruppi può essere utilizzata per:

- ◆ Applicare operazioni di gruppo a tutte le postazioni che fanno parte di tale gruppo.
Sia per un gruppo singolo che per diversi gruppi selezionati si possono avviare, visualizzare e terminare task di scansione delle postazioni che fanno parte di tale gruppo. Si possono inoltre visualizzare le statistiche (tra l'altro, infezioni, virus, avvio/terminazione, errori scansione e di installazione ecc.) e le statistiche complessive di tutte le postazioni di un gruppo o di più gruppi.
- ◆ Configurare impostazioni comuni delle postazioni attraverso il gruppo di cui fanno parte (v. p. [Utilizzo dei gruppi per configurare postazioni](#)).
- ◆ Sistemare (strutturare) la lista delle postazioni.

Si possono creare anche gruppi nidificati.

5.1. Gruppi di sistema e custom

Gruppi di sistema

Inizialmente **Dr.Web Enterprise Security Suite** contiene un set di gruppi di sistema predefiniti. Questi gruppi vengono creati durante l'installazione del **Server Dr.Web** e non possono essere eliminati. Tuttavia, se necessario, l'amministratore può nascondere la loro visualizzazione.

Ogni gruppo di sistema (salvo il gruppo **Everyone**) contiene un set di sottogruppi raggruppati secondo un determinato criterio.



Dopo che il **Server** è stato installato e fino a quando le postazioni non si connetteranno ad esso, soltanto il gruppo **Everyone** viene visualizzato nella lista dei gruppi di sistema. Per visualizzare tutti i gruppi di sistema, utilizzare l'opzione **Mostra gruppi nascosti** nella sezione **Impostazioni della vista albero** nella [barra degli strumenti](#).

Everyone

Il gruppo che comprende tutte le postazioni conosciute dal **Server Dr.Web**. Il gruppo **Everyone** contiene le impostazioni predefinite di ogni postazione e gruppo.

Configured

Il gruppo contiene le postazioni per cui sono state definite le impostazioni individuali.

Sistema operativo

Questa categoria dei sottogruppi visualizza i sistemi operativi attuali delle postazioni. Questi gruppi non sono virtuali e possono contenere impostazioni di postazioni ed essere gruppi primari.

- ◆ I sottogruppi della famiglia **Android**. Questa famiglia include un set dei gruppi che corrispondono ad una versione concreta del sistema operativo mobile Android.



- ◆ I sottogruppi della famiglia **Mac OS X**. Questa famiglia include un set dei gruppi che corrispondono ad una versione concreta del sistema operativo Mac OS X.
- ◆ Il sottogruppo **Netware**. Questo sottogruppo include le postazioni con il sistema operativo mobile Novell NetWare.
- ◆ I sottogruppi della famiglia **UNIX**. Questa famiglia include un set dei gruppi che corrispondono agli sistemi operativi della famiglia UNIX, per esempio, Linux, FreeBSD, Solaris ecc.
- ◆ I sottogruppi della famiglia **Windows**. Questa famiglia include un set dei gruppi che corrispondono ad una versione del sistema operativo Windows.

Status

Il gruppo **Status** contiene gruppi nidificati che visualizzano lo stato corrente delle postazioni: se al momento sono connesse o meno al **Server**, nonché lo stato del software antivirus: se il software è rimosso o il periodo di utilizzo è scaduto. Questi gruppi sono virtuali e non possono contenere impostazioni od essere gruppi primari.

- ◆ Il gruppo **Deinstalled**. Non appena rimosso da una postazione il software **Agent Dr.Web**, la postazione viene trasferita automaticamente nel gruppo **Deinstalled**.
- ◆ Il gruppo **Deleted**. Contiene le postazioni che l'amministratore ha rimosso dal **Server**. È possibile recuperare queste postazioni (v. p. [Rimozione e recupero della postazione](#)).
- ◆ Il gruppo **New**. Contiene le postazioni nuove create dall'amministratore attraverso il **Pannello di controllo**, ma l'**Agent** non è ancora stato installato su di esse.
- ◆ Il gruppo **Newbies**. Contiene tutte le postazioni non approvate di cui la registrazione sul **Server** al momento non è ancora stata confermata. Dopo che la registrazione verrà confermata oppure verrà negato l'accesso al **Server**, le postazioni verranno cancellate automaticamente da questo gruppo.
- ◆ Il gruppo **Offline**. Contiene tutte le postazioni non connesse al momento.
- ◆ Il gruppo **Online**. Contiene tutte le postazioni connesse al momento (che rispondono alle query del **Server**).
- ◆ Il gruppo **Update Errors**. Contiene le postazioni sui cui l'aggiornamento del software antivirus non è riuscito.

Transport

Questi sottogruppi definiscono il protocollo attraverso cui le postazioni al momento sono connesse al **Server**. Questi sottogruppi sono virtuali e non possono contenere impostazioni od essere gruppi primari.

- ◆ Il gruppo **TCP/IP**. Il gruppo contiene le postazioni connesse al momento attraverso il protocollo TCP/IP versione 4.
- ◆ Il gruppo **TCP/IP Version 6**. Il gruppo contiene le postazioni connesse al momento attraverso il protocollo TCP/IP versione 6.

Ungrouped

Questo gruppo contiene le postazioni che non fanno parte di nessuno dei gruppi custom.



Gruppi custom

Sono gruppi creati dall'amministratore della rete antivirus per le proprie esigenze. L'amministratore può creare propri gruppi, nonché gruppi nidificati, e può aggiungerci postazioni. **Dr.Web Enterprise Security Suite** non impone alcuna restrizione sui contenuti o sui nomi di tali gruppi.

Per comodità, la tabella [5-1](#) riassume tutti i gruppi possibili e i tipi di gruppo, nonché i parametri supportati (+) o non supportati (-) da questi gruppi.

Vengono considerati i seguenti parametri:

- ◆ **Appartenenza automatica.** Il parametro determina se è possibile includere automaticamente postazioni nel gruppo (supporto dell'appartenenza automatica), nonché se è possibile cambiare automaticamente gli elementi del gruppo nel corso del funzionamento del **Server**.
- ◆ **Gestione dell'appartenenza.** Il parametro determina se l'amministratore può gestire l'appartenenza al gruppo: aggiunta o cancellazione di postazioni dal gruppo.
- ◆ **Gruppo primario.** Il parametro determina se questo gruppo può essere primario per la postazione.
- ◆ **Inclusione di impostazioni.** Il parametro determina se il gruppo può contenere impostazioni di componenti antivirus (affinché le postazioni possano ereditarle).

Tabella 5-1. Gruppi e parametri supportati

Gruppo/tipo gruppo	Parametro			
	Appartenenza automatica	Gestione dell'appartenenza	Gruppo primario	Inclusione di impostazioni
Everyone	+	-	+	+
Configured	+	-	-	-
Sistema operativo	+	-	+	+
Status	+	-	-	-
Transport	+	-	-	-
Ungrouped	+	-	-	-
Gruppi custom	-	+	+	+



Quando si utilizza un account *Amministratore del gruppo*, il gruppo custom gestito da quest'amministratore viene visualizzato nella radice dell'albero gerarchico, anche se effettivamente abbia gruppo padre. In tale caso saranno disponibili tutti i gruppi figlio del gruppo gestito dall'amministratore.



5.2. Gestione dei gruppi

5.2.1. Creazione ed eliminazione di gruppi

Creazione del gruppo

Per creare un nuovo gruppo:

1. Selezionare la voce **+** **Aggiungi una postazione o un gruppo** nella barra degli strumenti, quindi dal sottomenu selezionare la voce **+** **Crea un gruppo**.

Si apre la finestra di creazione del gruppo.

2. Il campo di input **Identificatore** viene riempito in modo automatico. Se necessario, si può modificarlo durante la creazione. L'identificatore non deve includere spazi. In seguito, non si può modificare l'identificatore.
3. Inserire nel campo **Nome** il nome del gruppo.
4. Per gruppi nidificati, nel campo **Gruppo padre** selezionare dalla lista a cascata un gruppo da assegnare come il gruppo padre dal quale il nuovo gruppo eredita la configurazione, se non sono indicate le impostazioni personalizzate. Per un gruppo radice (che non ha padre) lasciare questo campo vuoto, il gruppo viene aggiunto alla radice della lista gerarchica. In questo caso, il gruppo eredita le impostazioni dal gruppo **Everyone**.
5. Inserire un commento nel campo **Descrizione**.
6. Premere il pulsante **Salva**.

I gruppi creati sono inizialmente vuoti. La procedura di aggiunta di postazioni ai gruppi è descritta nella sezione [Sistemazione delle postazioni in gruppi custom](#).

Eliminazione del gruppo

Per eliminare un gruppo esistente:

1. Selezionare il gruppo custom nella lista gerarchica del **Pannello di controllo**.
2. Nella barra degli strumenti premere **★ Generali** → **✗ Rimuovi gli oggetti selezionati**.



I gruppi predefiniti non si possono eliminare.

5.2.2. Modifica dei gruppi

Per modificare le impostazioni dei gruppi:

1. Selezionare la voce **Rete antivirus** del menu principale del **Pannello di controllo**, nella finestra che si è aperta nella lista gerarchica selezionare un gruppo.
2. Aprire la sezione delle impostazioni del gruppo in uno dei seguenti modi:
 - a) Premere **★ Generali** → **✎ Modifica** nella barra degli strumenti. Nella parte destra della finestra del **Pannello di controllo** si apre una sezione con le proprietà del gruppo.
 - b) Selezionare la voce **Proprietà del menu di gestione**. Si apre la finestra con le proprietà del gruppo.
3. La finestra delle proprietà del gruppo contiene le schede **Generali** e **Configurazione**. I contenuti e la configurazione delle schede sono descritti sotto.



Se si aprono le proprietà del gruppo nella parte destra della finestra del **Pannello di controllo** (v. punto **2.a**) è inoltre disponibile la sezione **Informazioni sulle postazioni** in cui si trovano le informazioni generali sulle postazioni che fanno parte di tale gruppo.

- Per salvare le modifiche apportate, premere il pulsante **Salva**.

Generali

Nella sezione **Generali** vengono riportate le seguenti informazioni:

- ◆ **Identificatore** - l'identificatore unico del gruppo. Non modificabile.
- ◆ **Nome** - il nome del gruppo. Se necessario, si può modificare il nome di un gruppo custom. In caso dei gruppi predefiniti, il campo **Nome** non è modificabile.
- ◆ **Gruppo padre** - il gruppo padre di cui fa parte tale gruppo e da cui eredita la sua configurazione, se non ce ne sono delle impostazioni personalizzate. Se nessun gruppo padre è assegnato, il gruppo eredita le impostazioni dal gruppo **Everyone**.
- ◆ **Descrizione** - campo non obbligatorio di descrizione del gruppo.

Informazioni sulle postazioni

Nella sezione **Informazioni sulle postazioni** vengono riportate le seguenti informazioni:

- ◆ **Postazioni** - numero totale di postazioni che rientrano in questo gruppo.
- ◆ **Gruppo primario per** - numero di postazioni per cui questo gruppo è quello primario.
- ◆ **Postazioni online** - numero di postazioni in questo gruppo che sono attualmente in rete (online).

Configurazione



Per le informazioni dettagliate su ereditarietà di impostazioni dei gruppi da parte delle postazioni per cui tale gruppo è primario, v. sezione [Utilizzo dei gruppi per configurare postazioni](#).

Nella sezione **Configurazione** si può modificare la configurazione dei gruppi che include:

Icona	Impostazioni	Sezione con la descrizione
	Permessi degli utenti delle postazioni che ereditano quest'impostazione dal gruppo se è primario. I permessi dei gruppi vengono configurati nello stesso modo dei permessi di singole postazioni.	Permessi dell'utente della postazione
	Calendario centralizzato per l'esecuzione di task sulle postazioni che ereditano quest'impostazione dal gruppo se è primario. Il calendario dei gruppi viene configurato nello stesso modo del calendario di singole postazioni.	Calendario dei task della postazione
	Chiavi di licenza per le postazioni per cui questo gruppo è primario.	Gestione licenze
	Restrizioni di distribuzione di aggiornamenti di software antivirus sulle postazioni che ereditano quest'impostazione dal gruppo se è primario.	Limitazione degli aggiornamenti delle postazioni
	Lista dei componenti da installare sulle postazioni che ereditano quest'impostazione dal gruppo se è primario. La lista di componenti per i gruppi viene modificata nello stesso modo della lista di componenti per le postazioni.	Componenti da installare del pacchetto antivirus



Icona	Impostazioni	Sezione con la descrizione
	Configurazione della sistemazione automatica di postazioni in tale gruppo. È disponibile solo per i gruppi custom.	Configurazione dell'appartenenza automatica a un gruppo
	Configurazioni dei componenti di pacchetto antivirus. I componenti di pacchetto antivirus per il gruppo vengono configurati nello stesso modo dei componenti per una postazione.	Configurazione dei componenti antivirus

5.3. Sistemazione delle postazioni in gruppi custom

Dr.Web Enterprise Security Suite mette a disposizione i seguenti modi per sistemare postazioni in gruppi custom:

1. [Sistemazione manuale delle postazioni in gruppi.](#)
2. [Utilizzo delle regole di appartenenza automatica a un gruppo.](#)

5.3.1. Sistemazione manuale delle postazioni in gruppi

Vi sono diversi modi per aggiungere postazioni manualmente ai gruppi custom:

1. [Modificare le impostazioni della postazione.](#)
2. [Trascinare le postazioni nella lista gerarchica](#) (drag-and-drop).

Per modificare la lista dei gruppi, di cui fa parte la postazione, tramite le impostazioni della postazione:

1. Selezionare la voce **Rete antivirus** del menu principale, nella finestra che si è aperta nella lista gerarchica premere il nome della postazione.
2. Aprire la sezione delle impostazioni della postazione in uno dei seguenti modi:
 - ◆ Dal [menu di gestione](#) selezionare la voce **Proprietà**.
 - ◆ Premere **Generali** → **Modifica** nella barra degli strumenti.
3. Nel pannello **Proprietà della postazione** che si è aperto, passare alla sezione **Gruppi**.
Nella lista **Appartenenza** sono elencati tutti i gruppi di cui la postazione fa parte e in cui essa può essere inclusa.
4. Per aggiungere la postazione a un gruppo custom, spuntare il flag di fronte a questo gruppo nella lista **Appartenenza**.
5. Per eliminare la postazione da un gruppo custom, togliere il flag di fronte a questo gruppo nella lista **Appartenenza**.



Non è possibile eliminare postazioni dai gruppi predefiniti.

6. Per salvare le modifiche apportate, premere il pulsante **Salva**.

Inoltre nella sezione **Proprietà** della postazione, si può assegnare il gruppo primario alla postazione (per maggiori informazioni v. [Ereditarietà della configurazione da parte della postazione. Gruppi primari](#)).



Per modificare la lista dei gruppi, di cui fa parte la postazione, tramite la lista gerarchica:

1. Selezionare la voce **Rete antivirus** del menu principale e aprire la lista gerarchica dei gruppi e delle postazioni.
2. Per aggiungere una postazione a un gruppo custom, premere e tenere premuto il tasto CTRL e trascinare la postazione con il mouse nel gruppo necessario (drag'n'drop).
3. Per spostare la postazione da un gruppo custom in un altro, trascinarla con il mouse (drag'n'drop) dal gruppo custom da cui la postazione viene eliminata nel gruppo custom a cui la postazione viene aggiunta.



Se la postazione viene trascinata da un gruppo predefinito secondo la voce 2 o 3, essa viene aggiunta al gruppo custom e non viene eliminata dal gruppo predefinito.



5.3.2. Configurazione dell'appartenenza automatica a un gruppo

Dr.Web Enterprise Security Suite dà la possibilità di configurare le regole di inclusione automatica di postazioni in gruppi.

Per configurare le regole di inclusione automatica di postazioni in un gruppo:

1. Selezionare la voce **Rete antivirus** del menu principale del **Pannello di controllo**.
2. Dalla lista gerarchica della rete antivirus selezionare il gruppo custom per cui si vogliono creare regole di appartenenza.
3. Passare nella sezione di modifica delle regole di appartenenza in uno dei seguenti modi:
 - Nel [menu di gestione](#), nella sezione **Generali** selezionare la voce **Regole di appartenenza al gruppo**.
 - Premere **Generali** → **Modifica** nella barra degli strumenti. Nel pannello delle proprietà del gruppo nella parte destra della finestra, nella sezione **Configurazione** premere **Regole di appartenenza al gruppo**.
 - Nel [menu di gestione](#), nella sezione **Generali** selezionare la voce **Proprietà**, passare alla scheda **Configurazione**, premere **Regole di appartenenza al gruppo**.
4. Nella finestra che si è aperta, impostare una lista delle condizioni, verificate le quali, le postazioni verranno inserite in questo gruppo:
 - a) Se per il gruppo prima non sono stati impostati le regole di appartenenza, premere **Aggiungi regola**.
 - b) Per ciascun blocco delle regole, configurare le seguenti impostazioni:
 - Selezionare una delle opzioni che imposta il principio di unione delle regole nel blocco: **Soddisfa tutte le condizioni**, **Soddisfa qualsiasi delle condizioni**, **Non soddisfa alcuna delle condizioni**.
 - Dalle liste a cascata delle regole selezionare: uno dei parametri della postazione che verrà controllato per corrispondenza alle condizioni, il principio di corrispondenza a questa condizione e, se il parametro della postazione l'implica, inserire la stringa della condizione.
 - Per aggiungere un'altra condizione a questo blocco, premere a destra della stringa della condizione.
 - c) Per aggiungere un nuovo blocco di regole, premere a destra del blocco. Inoltre, impostare il principio di unione di questo blocco di condizioni con gli altri blocchi:
 - **E** - le condizioni dei blocchi devono essere soddisfatte allo stesso tempo.
 - **O** - devono essere soddisfatte le condizioni di almeno uno dei blocchi.
5. Per salvare ed applicare le regole impostate, premere uno dei seguenti pulsanti:








- **Applica adesso** - per salvare le regole di appartenenza impostate e per applicare queste regole allo stesso tempo a tutte le postazioni registrate su questo **Server**. In caso di un grande numero di postazioni connesse al **Server**, l'esecuzione di quest'azione potrebbe richiedere un certo tempo. Le regole di nuovo raggruppamento di postazioni vengono applicate a tutte le postazioni già registrate subito quando viene impostata l'azione e verranno applicate a tutte le postazioni, anche a quelle che verranno registrate sul **Server** per la prima volta, al momento della loro connessione.
 - **Applica alla connessione delle postazioni** - per salvare le regole di appartenenza impostate e per applicare queste regole alle postazioni al momento quando si connettono al **Server**. Le regole di nuovo raggruppamento di postazioni vengono applicate a tutte le postazioni già registrate al momento della loro successiva connessione al **Server** e verranno applicate a tutte le postazioni che vengono registrate sul **Server** per la prima volta al momento della loro prima connessione.
6. Quando vengono impostate le regole di appartenenza automatica per un gruppo custom, nella lista gerarchica della rete antivirus accanto all'icona di questo gruppo compare l'icona , a condizione che sia spuntato il flag **Mostra l'icona di regole appartenenza al gruppo** nella lista  **Impostazioni della vista albero** nella barra degli strumenti.



Se una postazione è stata trasferita in un gruppo custom sulla base delle regole di appartenenza in modo automatico, è inutile eliminare manualmente la postazione da questo gruppo in quanto al momento della successiva connessione al **Server** la postazione verrà restituita automaticamente a questo gruppo.

Per eliminare le regole di inclusione automatica di postazioni in un gruppo:

1. Selezionare la voce **Rete antivirus** del menu principale del **Pannello di controllo**.
2. Dalla lista gerarchica della rete antivirus selezionare il gruppo custom per cui si vogliono eliminare le regole di appartenenza.
3. Eseguire una delle seguenti azioni:
 - Nella barra degli strumenti premere il pulsante  **Rimuovi le regole di appartenenza**.
 - Premere  **Generali** →  **Modifica** nella barra degli strumenti. Nel pannello delle proprietà del gruppo nella parte destra della finestra, nella sezione **Configurazione** premere  **Rimuovi le regole di appartenenza**.
 - Nel [menu di gestione](#), nella sezione **Generali** selezionare la voce **Proprietà**, passare alla scheda **Configurazione**, premere  **Rimuovi le regole di appartenenza**.
4. Dopo la rimozione delle regole di appartenenza del gruppo, tutte le postazioni sistemate in questo gruppo sulla base delle regole di appartenenza verranno eliminate da questo gruppo. Se ad alcune delle postazioni questo gruppo è stato assegnato dall'amministratore come il gruppo primario, al momento dell'eliminazione delle postazioni dal gruppo ad esse verrà assegnato come primario il gruppo **Everyone**.

5.4. Utilizzo dei gruppi per configurare postazioni

Le postazioni possono avere impostazioni:

1. [Ereditate dal gruppo primario](#).
2. [Definite in modo individuale](#).

Ereditarietà delle impostazioni

Quando viene creato un nuovo gruppo, esso eredita le impostazioni dal gruppo padre o dal gruppo **Everyone** se il gruppo padre non è assegnato.

Quando viene creata una nuova postazione, essa eredita le impostazioni dal gruppo primario.



Per maggiori informazioni v. p. [Ereditarietà della configurazione da parte della postazione. Gruppi primari](#).


Quando vengono visualizzate o modificate le impostazioni di una postazione, ereditate dal gruppo primario, nelle relative finestre viene segnalato che tali impostazioni sono ereditate dal gruppo primario.

Si possono impostare varie configurazioni per vari [gruppi](#) e [postazioni](#), modificando le impostazioni corrispondenti.

Impostazioni individuali

Per configurare in modo individuale una postazione, modificare la sezione corrispondente delle impostazioni (v. p. [Proprietà della postazione - Configurazione](#)). Nella sezione delle impostazioni verrà segnalato che un'impostazione è individuale per la postazione.

Se una postazione ha delle impostazioni personalizzate, le impostazioni del gruppo primario ed eventuali modifiche non valgono per la postazione.

È possibile tornare alla configurazione ereditata dal gruppo primario. Per farlo, premere il pulsante  **Rimuovi le impostazioni personalizzate** nella barra degli strumenti del **Pannello di controllo** nella sezione delle impostazioni corrispondenti o nella sezione delle proprietà della postazione.

5.4.1. Ereditarietà della configurazione da parte della postazione

Principio di ereditarietà delle impostazioni

Quando viene creata una postazione nuova, essa eredita la sua configurazione da uno dei gruppi di cui fa parte. Tale gruppo si chiama *primario*. Se vengono modificate le impostazioni del gruppo primario, le postazioni che fanno parte del gruppo ereditano le modifiche, salvo che le postazioni avessero impostazioni individuali. Quando viene creata una postazione, si può indicare quale gruppo verrà assegnato come quello primario. Di default, il gruppo primario è **Everyone**.



Se il gruppo primario non è **Everyone** e se il gruppo primario assegnato, che è un nodo radice della lista gerarchica della rete antivirus, non ha impostazioni personalizzate, la nuova postazione eredita le impostazioni del gruppo **Everyone**.

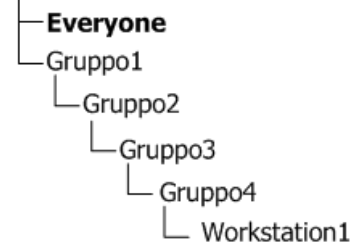
Se ci sono dei gruppi nidificati, se per la postazione non sono state definite impostazioni personalizzate, essa eredita la configurazione secondo la struttura dei gruppi nidificati. La ricerca viene eseguita dal basso in alto dell'albero gerarchico, partendo dal gruppo primario della postazione, dal suo gruppo padre e così via fino all'elemento radice dell'albero. Se durante la ricerca non sono state scoperte impostazioni personalizzate, la postazione eredita le impostazioni del gruppo **Everyone**.




Per esempio:

La struttura della lista gerarchica è il seguente albero:

Rete antivirus





Il Gruppo `Group4` è primario per la postazione `Station1`. Quando la postazione `Station1` eredita impostazioni, la ricerca delle impostazioni viene eseguita nel seguente ordine: `Station1` → `Group4` → `Group3` → `Group2` → `Group1` → `Everyone`.

Di default, la struttura di rete è presentata in modo tale da dimostrare l'appartenenza della postazione a tutti i gruppi di cui fa parte. Se si vuole visualizzare nella directory di rete l'appartenenza della postazione solo ai gruppi primari, nella barra degli strumenti del **Pannello di controllo** nella voce  **Impostazioni della vista albero** togliere il flag **Appartenenza a tutti i gruppi**.



Assegnazione del gruppo primario



Vi sono diversi modi per assegnare il gruppo primario alla postazione e a un gruppo di postazioni.

Per assegnare il gruppo primario a una postazione:

1. Selezionare la voce **Rete antivirus** del menu principale, nella finestra che si è aperta nella lista gerarchica premere il nome della postazione.
2. Nel **menu di gestione** selezionare la voce **Proprietà** o nella barra degli strumenti premere  **Generali** →  **Modifica**. Nella finestra che si è aperta passare alla scheda **Gruppi**.
3. Se è necessario cambiare il gruppo primario, premere l'icona del gruppo richiesto nella sezione **Appartenenza**. Dopo questo, sull'icona del gruppo compare **1**.
4. Premere il pulsante **Salva**.

Per assegnare il gruppo primario a diverse postazioni:

1. Selezionare la voce **Rete antivirus** del menu principale, nella finestra che si è aperta nella lista gerarchica premere i nomi delle postazioni (si possono selezionare anche gruppi – in tale caso l'azione verrà applicata a tutte le postazioni che ne fanno parte) a cui si desidera assegnare un gruppo primario. Per selezionare diverse postazioni o gruppi, si può utilizzare la selezione con il mouse con i tasti della tastiera premuti CTRL o SHIFT.
2. Nella barra degli strumenti premere  **Generali** →  **Imposta il gruppo primario per le postazioni**. Si apre la finestra con una lista dei gruppi che possono essere assegnati come primati a queste postazioni.
3. Per indicare il gruppo primario, premere il nome del gruppo.

Si può impostare il gruppo come primario per tutte le postazioni che ne fanno parte. Per farlo, selezionare il gruppo richiesto nella lista gerarchica, dopodiché nella barra degli strumenti del **Pannello di controllo** premere  **Generali** →  **Imposta questo gruppo come primario**.








5.4.2. Copiatura delle impostazioni in altri gruppi/postazioni

Le impostazioni riguardanti i componenti antivirus, calendari, permessi degli utenti e le altre impostazioni di un gruppo o di una postazione possono essere copiate (propagate) in uno o più gruppi e postazioni.

Per copiare le impostazioni:

1. Premere il pulsante **Propaga queste impostazioni verso un altro oggetto:**

- ◆  nella finestra di modifica della configurazione del componente antivirus,
- ◆  nella finestra di modifica del calendario,
- ◆  nella finestra di configurazione delle limitazioni degli aggiornamenti,
- ◆  nella finestra dei componenti da installare,
- ◆  nella finestra di configurazione dei permessi degli utenti della postazione.

Si apre la finestra con la lista gerarchica della rete antivirus.

2. Selezionare nella lista i gruppi e le postazioni verso cui si desidera propagare le impostazioni.
3. Per poter apportare le modifiche alla configurazione di questi gruppi, premere il pulsante **Salva**.

5.5. Comparazione delle postazioni e dei gruppi

Si possono comparare le postazioni e i gruppi secondo i parametri principali.

Per comparare diversi oggetti della rete antivirus:

1. Selezionare la voce **Rete antivirus** del menu principale, nella finestra che si è aperta nella lista gerarchica selezionare oggetti da confrontare. Per farlo, utilizzare i tasti della tastiera CTRL e SHIFT. Sono possibili le seguenti varianti:
 - ◆ scelta di diverse postazioni - per comparare le postazioni selezionate;
 - ◆ scelta di diversi gruppi - per comparare i gruppi selezionati e tutti i gruppi nidificati;
 - ◆ scelta di diverse postazioni e gruppi - per comparare tutte le postazioni: sia quelle selezionate direttamente nella lista gerarchica che quelle che fanno parte dei gruppi selezionati e dei loro gruppi nidificati.
2. Nel [menu di gestione](#) premere la voce **Comparazione**.
3. Si apre una tabella comparativa per gli oggetti selezionati.
 - ◆ Parametri di confronto per i gruppi:
 - **Postazioni** - numero totale di postazioni nel gruppo.
 - **Postazioni online** - numero di postazioni attive al momento.
 - **Gruppo primario per** - numero di postazioni per cui il gruppo selezionato è quello primario.
 - **Configurazione individuale** - una lista dei componenti che hanno le impostazioni individuali, non ereditate dal gruppo padre.
 - ◆ Parametri di confronto per le postazioni:
 - **Data di creazione** della postazione.
 - **Gruppo primario** per la postazione.
 - **Configurazione individuale** - una lista dei componenti che hanno le impostazioni individuali, non ereditate dal gruppo primario.
 - **Componenti installati** - una lista dei componenti antivirus installati sulla postazione.



Capitolo 6: Gestione delle postazioni

La rete antivirus gestita tramite **Dr.Web Enterprise Security Suite** consente di configurare in maniera centralizzata i pacchetti antivirus su postazioni. **Dr.Web Enterprise Security Suite** consente di:

- ◆ configurare le impostazioni degli elementi antivirus,
- ◆ configurare il calendario di esecuzione dei task di scansione,
- ◆ avviare singoli task su postazioni a prescindere dalle impostazioni del calendario,
- ◆ avviare il processo di aggiornamento di postazioni, anche dopo un errore di aggiornamento con il resettaggio dello stato di errore.

In particolare, l'amministratore della rete antivirus può lasciare all'utente di postazione i permessi per la configurazione indipendente del software antivirus e per l'avvio dei task, può proibire tali attività o limitarle in gran parte.

Le modifiche nella configurazione di una postazione si possono apportare perfino quando la postazione non è disponibile al **Server**. Queste modifiche verranno accettate dalla postazione non appena si riconnetterà al **Server**.

6.1. Gestione degli account di postazioni

6.1.1. Criteri di approvazione delle postazioni



La procedura di creazione della postazione attraverso il **Pannello di controllo** è descritta nella **Guida all'installazione**, p. [Creazione di nuovo account](#).

La possibilità di gestire l'autenticazione delle postazioni su **Server Dr.Web** dipende dai seguenti parametri:

1. Se quando l'**Agent** veniva installato su postazione, il flag **Autenticazione manuale sul server** era deselezionato, la modalità di accesso delle postazioni al **Server** viene determinata sulla base delle impostazioni definite sul **Server** (si usa di default), v. [sotto](#).
2. Se quando l'**Agent** veniva installato su postazione, il flag **Autenticazione manuale sul server** era selezionato ed erano impostati i parametri **Identificatore** e **Password**, quando la postazione si connette al **Server**, essa viene autenticata automaticamente a prescindere dalle impostazioni del **Server** (si usa di default nell'installazione di **Agent** mediante il pacchetto di installazione *drweb-esuite-install* – v. **Guida all'installazione**, p. [File di installazione](#)).



Come configurare il tipo di autenticazione dell'**Agent** al momento dell'installazione viene descritto nel **Manuale dell'utente**.

Per modificare la modalità di accesso delle postazioni al Server Dr.Web:

1. Aprire le impostazioni di **Server**. Per farlo, selezionare la voce **Amministrazione** del menu principale, nella finestra che si è aperta selezionare la voce del [menu di gestione Configurazione](#) del **Server Dr.Web**.
2. Nella scheda **Generali** nella lista a cascata **Registrazione dei nuovi arrivi** scegliere uno dei seguenti valori:
 - ◆ **Conferma manuale dell'accesso** (modalità predefinita, se non modificata durante l'installazione del **Server**),







- ◆ **Sempre nega l'accesso,**
- ◆ **Consenti l'accesso automaticamente.**

Conferma manuale dell'accesso

Nella modalità **Conferma manuale dell'accesso** le nuove postazioni vengono collocate nel sottogruppo di sistema **Newbies** del gruppo **Status** e ci restano fino a quando non verranno considerate dall'amministratore.

Per gestire l'accesso delle postazioni non confermate:

1. Selezionare la voce **Rete antivirus** del menu principale del **Pannello di controllo**. Selezionare postazioni nella lista gerarchica di rete antivirus, nel sottogruppo **Newbies** del gruppo **Status**.
2. Per configurare l'accesso al **Server**, nella barra degli strumenti nella sezione  **Postazioni non confermate** impostare l'azione che verrà applicata alle postazioni selezionate:
 -  **Consenti alle postazioni selezionate di accedere e imposta gruppo primario** – per confermare l'accesso della postazione al **Server** e per assegnare ad essa un gruppo primario dalla lista proposta.
 -  **Annulla l'azione da eseguire al momento di connessione** – per annullare l'azione impostata per essere applicata alla postazione non confermata al momento quando essa si conetterà al **Server**.
 -  **Proibisci alle postazioni selezionate di accedere** – per proibire alla postazione di accedere al **Server**.

Negare l'accesso

Nella modalità **Sempre nega l'accesso** il **Server** nega l'accesso se riceve le query di nuove postazioni. L'amministratore deve creare gli account di postazioni manualmente e assegnare ad essi le password di accesso.



Consenti l'accesso automaticamente

Nella modalità **Consenti l'accesso automaticamente** tutte le postazioni che richiedono l'accesso al **Server** vengono approvate automaticamente senza ulteriori query inviate all'amministratore. In questo caso, come gruppo primario, ad esse viene assegnato il gruppo impostato nella lista a cascata **Gruppo primario** nella sezione **Configurazione** del **Server Dr.Web** nella scheda **Generali**.

6.1.2. Rimozione e recupero della postazione

Rimozione di postazioni

Per rimuovere l'account di una postazione:

1. Selezionare la voce del menu principale **Rete antivirus**, nella finestra che si è aperta, nella barra degli strumenti fare clic su  **Generali** →  **Rimuovi gli oggetti selezionati**.
2. Si apre la finestra di conferma della rimozione della postazione. Fare clic su **OK**.

Dopo la rimozione delle postazioni dalla lista gerarchica, esse vengono collocate nella tabella delle postazioni rimosse, da cui è possibile recuperare oggetti attraverso il **Pannello di controllo**.



Recupero di postazioni

Per recuperare l'account di una postazione:

1. Selezionare la voce **Rete antivirus** del menu principale, nella finestra che si è aperta, nella lista gerarchica selezionare la postazione rimossa o alcune postazioni che si vogliono recuperare.



Tutte le postazioni rimosse si trovano nel sottogruppo **Deleted** del gruppo **Status**.

2. Nella barra degli strumenti selezionare la voce **Generali** → **Recupera le postazioni rimosse**.
3. Si apre la sezione di recupero di postazioni rimosse. Si possono impostare i seguenti parametri di postazione che verranno assegnati alla postazione recuperata:
 - ◆ **Gruppo primario** – selezionare il gruppo primario a cui verrà aggiunta la postazione recuperata. Di default, è selezionato il gruppo primario impostato per la postazione prima della rimozione.



Se vengono recuperate più postazioni simultaneamente, di default è selezionata l'opzione **Ex gruppo primario** che significa che per ciascuna postazione recuperata verrà impostato il gruppo primario a cui apparteneva prima della rimozione. Se viene selezionato un determinato gruppo, per tutte le postazioni recuperate verrà impostato lo stesso gruppo.

- ◆ Nella sezione **Appartenenza** si può modificare l'elenco dei gruppi di cui la postazione farà parte. Di default, è impostato l'elenco dei gruppi a cui la postazione apparteneva prima della rimozione. Nella lista **Appartenenza** è riportato l'elenco dei gruppi in cui si può includere la postazione. Spuntare i flag accanto ai gruppi in cui si desidera includere la postazione.
4. Per recuperare la postazione con i parametri impostati, fare clic sul pulsante **Recupera**.

6.1.3. Unione delle postazioni

Quando vengono eseguite operazioni con il database o viene reinstallato il software di postazioni antivirus, nella lista gerarchica della rete antivirus potrebbero comparire diverse postazioni con lo stesso nome (solo uno di questi sarà correlato con la postazione antivirus corrispondente).

Per eliminare i nomi duplicati di postazioni:

1. Selezionare tutti i nomi duplicati della stessa postazione. Per farlo, utilizzare il tasto CTRL.
2. Nella barra degli strumenti selezionare **Generali** → **Unisci le postazioni**.
3. Nella colonna scegliere la postazione che verrà considerata master. Tutte le altre postazioni verranno eliminate, e i loro dati verranno attribuiti a quella scelta.
4. Nella colonna scegliere la postazione, le cui configurazioni verranno impostate per la postazione master scelta.
5. Premere **Salva**.



6.2. Impostazioni generali della postazione

6.2.1. Proprietà della postazione

Proprietà della postazione

Per visualizzare e per modificare le proprietà di una postazione:

1. Selezionare la voce **Rete antivirus** del menu principale del **Pannello di controllo**, nella finestra che si è aperta nella lista gerarchica selezionare una postazione.
2. Aprire la sezione delle impostazioni della postazione in uno dei seguenti modi:
 - a) Premere **★ Generali** → **✏ Modifica** nella barra degli strumenti. Nella parte destra della finestra del **Pannello di controllo** si apre 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. La finestra delle proprietà della postazione contiene i seguenti gruppi di parametri: **Generali**, **Configurazione**, **Gruppi**, **Sicurezza**, **Posizione**. I loro contenuti e la loro configurazione sono descritti sotto.
4. Per salvare le modifiche apportate, premere il pulsante **Salva**.

Eliminazione delle impostazioni individuali della postazione

Per eliminare le impostazioni individuali di una postazione:

1. Selezionare la voce **Rete antivirus** del menu principale del **Pannello di controllo**, nella finestra che si è aperta nella lista gerarchica selezionare una postazione e nella barra degli strumenti premere **★ Generali** → **✖ Rimuovi le impostazioni personalizzate**. Si apre l'elenco delle impostazioni di questa postazione, le impostazioni individuali vengono contrassegnate con dei flag.
2. Togliere i flag delle impostazioni individuali che si vogliono eliminare e premere **Rimuovi**. Vengono ripristinate le impostazioni della postazione, ereditate dal gruppo primario.



Quando viene modificata la configurazione della postazione per i componenti **SpIDer Guard per Windows**, nonché **Dr.Web Scanner per Windows**, consultare le raccomandazioni sull'utilizzo dei programmi antivirus sui computer Windows Server 2003 e Windows XP. L'articolo che contiene le informazioni necessarie si trova all'indirizzo – <http://support.microsoft.com/kb/822158/ru>. Il materiale di questo articolo è progettato per aiutare ad ottimizzare le prestazioni del sistema.

A condizione che la chiave **Agent** (`agent.key`) disponibile permetta l'utilizzo del filtro antispam per il componente **SpIDer Mail**, nella scheda **Antispam** si può configurare il filtro (dal menu contestuale di un gruppo o di una postazione selezionare la voce **SpIDer Mail per postazioni**).

A partire dalla versione **5.0** il pacchetto antivirus **Dr.Web Enterprise Security Suite** include i prodotti **SpIDer Gate** e **Office Control**, per poter utilizzarli, è necessario che siano indicati nella licenza a disposizione (**Antivirus + Antispam**) che può essere visualizzata nella chiave **Agent**.

Le impostazioni del filtro antispam e dei componenti **SpIDer Gate** e **Office Control** sono descritte nel manuale **Agent Dr.Web® per Windows. Manuale dell'utente**.



6.2.1.1. Generali

Nella sezione **Generali** vengono riportati i seguenti campi di sola lettura:

- ◆ **Identificatore della postazione** - identificatore unico della postazione.
- ◆ **Nome** - nome della postazione.
- ◆ **Data di creazione** - data di creazione della postazione sul **Server**.
- ◆ **Scadenza del periodo agevolato** - data di scadenza del periodo agevolato di utilizzo dell'**Antivirus** sulla postazione.

Inoltre, si possono impostare o modificare i valori dei seguenti campi:

- ◆ Nel campo **Password** impostare una password per l'autenticazione della postazione sul **Server** (è necessario ripetere la stessa password nel campo **Digita di nuovo la password**). Quando la password viene cambiata, affinché l'**Agent** possa connettersi, è necessario fare la stessa procedura nelle impostazioni della connessione dell'**Agent** sulla postazione.
- ◆ Nel campo **Descrizione** si possono inserire le informazioni supplementari circa la postazione.



I valori dei campi marcati con il carattere * devono essere impostati obbligatoriamente.

Inoltre, in questa sezione sono riportati i seguenti link:

- ◆ Nel punto **File d'installazione** - un link al download dell'installer **Agent** per questa postazione.
Subito dopo la creazione della postazione fino al momento quando verrà impostato il sistema operativo della postazione, nella sezione di download del pacchetto, i link sono riportati separatamente per tutti i SO supportati da **Dr.Web Enterprise Security Suite**.
- ◆ Nel punto **File di configurazione** - un link per il download del file con le impostazioni di connessione al **Server Dr.Web** per le postazioni SO Android, Mac OS X e SO Linux.


6.2.1.2. Configurazione

Nella sezione **Configurazione** si può modificare la configurazione delle postazioni, che include:

Icona	Impostazioni	Sezione con la descrizione
	Permessi dell'utente della postazione	Permessi dell'utente della postazione
	Orario centralizzato dell'avvio dei task sulla postazione	Calendario dei task della postazione
	Chiavi di licenza per la postazione	Gestione licenze
	Limitazioni di propagazione degli aggiornamenti del software antivirus	Limitazione degli aggiornamenti delle postazioni
	Lista dei componenti da installare	Componenti da installare del pacchetto antivirus
	Impostazioni dei componenti di pacchetto antivirus per questa postazione	Configurazione dei componenti antivirus

Inoltre, nel **Pannello di controllo** sono disponibili i pulsanti di eliminazione di impostazioni individuali. Si trovano a destra dei relativi pulsanti di configurazione. Quando viene eliminata la configurazione individuale di una postazione, viene ristabilita la configurazione ereditata dal gruppo primario.



Se vengono modificate le impostazioni di **SpIDer Gate** e/o di **Office control**, si deve tenere presente che le impostazioni di questi componenti sono interrelate, dunque se le impostazioni individuali di uno di essi sono state rimosse tramite il pulsante  **Rimuovi le impostazioni personalizzate**, le impostazioni dell'altro componente anche verranno rimosse (viene impostata l'ereditarietà delle impostazioni dal gruppo padre).

6.2.1.3. Gruppi

Nella sezione **Gruppi** viene configurata una lista dei gruppi di cui fa parte questa postazione. Nella lista **Appartenenza** sono elencati tutti i gruppi di cui la postazione fa parte e in cui essa può essere inclusa.

Per gestire l'appartenenza di una postazione, è necessario:

1. Per aggiungere la postazione a un gruppo custom, spuntare il flag di fronte a questo gruppo nella lista **Appartenenza**.
2. Per eliminare la postazione da un gruppo custom, togliere il flag di fronte a questo gruppo nella lista **Appartenenza**.



Non è possibile eliminare postazioni dai gruppi predefiniti.

3. Se è necessario assegnare un altro gruppo primario, premere l'icona del gruppo desiderato nella sezione **Appartenenza**. Dopo questo, sull'icona del gruppo compare **1**.

6.2.1.4. Sicurezza



Nella sezione **Sicurezza** vengono impostate le restrizioni sugli indirizzi di rete da cui l'**Agent** installato su questa postazione può accedere al **Server**.

Per consentire tutte le connessioni, togliere il flag da **Usa questa lista di accesso**. Per impostare liste di indirizzi consentiti o bloccati, spuntare questo flag.

Per consentire l'accesso da un determinato indirizzo TCP, includerlo nella lista **TCP: Consentito** o **TCPv6: Consentito**.

Per proibire qualche indirizzo TCP, includerlo nella lista **TCP: Negato** o **TCPv6: Negato**.

Per modificare gli indirizzi nella lista:

1. Inserire un indirizzo di rete nel relativo campo nel seguente formato: `<indirizzo IP>/ [<prefisso rete>]`.
2. Per aggiungere un nuovo campo di indirizzo, premere il pulsante  della sezione corrispondente.
3. Per eliminare un campo, premere il pulsante  di fronte all'indirizzo da eliminare.
4. Per applicare le impostazioni, premere il pulsante **Salva**.

Esempio di utilizzo del prefisso:

1. Il prefisso 24 sta per la maschera di rete: 255.255.255.0

Contiene 254 indirizzi

Gli indirizzi di host in queste reti sono del tipo: 195.136.12.*

2. Il prefisso 8 sta per la maschera di rete 255.0.0.0



Contiene fino a 16387064 indirizzi (256*256*256)

Gli indirizzi di host in queste reti sono del tipo: 125.*.*.*

Inoltre, si possono eliminare gli indirizzi dalla lista e modificare gli indirizzi inseriti nella lista.

Gli indirizzi non inclusi in nessuna lista vengono consentiti o proibiti a seconda della selezione del flag **Priorità di negazione**. Se il flag è selezionato, la lista **Negato** ha la precedenza rispetto alla lista **Consentito**. Gli indirizzi non inclusi in nessuna lista o inclusi in tutte e due vengono proibiti. Vengono consentiti soltanto gli indirizzi che sono inclusi nella lista **Consentito** e non sono inclusi nella lista **Negato**.

6.2.1.5. Posizione

Nella scheda **Posizione** si possono indicare le informazioni supplementari circa la posizione fisica della postazione.

Inoltre, in questa scheda si può visualizzare la posizione della postazione su una mappa.

Per visualizzare la posizione della postazione sulla mappa:

1. Inserire nei campi **Latitudine** e **Longitudine** le coordinate geografiche della postazione nel formato gradi decimali (Decimal Degrees).
2. Premere il pulsante **Salva** per memorizzare i dati inseriti.
3. Nella scheda **Posizione** viene visualizzata l'anteprima della mappa OpenStreetMaps con un'etichetta corrispondente alle coordinate inserite.

Se l'anteprima non può essere caricata, viene visualizzato il testo **Mostra sulla mappa**.

4. Per visualizzare la mappa di grandezza piena, fare clic sull'anteprima o sul testo **Mostra sulla mappa**.

6.2.2. Componenti installati del pacchetto antivirus

Componenti

Per scoprire quali componenti del pacchetto antivirus sono installati su una postazione:

1. Selezionare la voce **Rete antivirus** del 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. Dal [menu di gestione](#) che si è aperto selezionare dalla sottosezione **Generali** la voce **Componenti installati**.
3. Si apre la finestra con le informazioni circa i componenti installati: nome del componente; tempo di installazione; indirizzo del **Server** da cui è stato installato questo componente; directory di installazione del componente sulla postazione.



L'elenco dei componenti installati dipende da:

- ◆ Componenti il cui utilizzo è consentito dalla chiave di licenza.
- ◆ SO della postazione.
- ◆ Impostazioni definite dall'amministratore sul **Server** della rete antivirus. L'amministratore può cambiare l'elenco dei componenti del pacchetto antivirus sulla postazione sia prima dell'installazione dell'**Agent** che in qualsiasi momento dopo l'installazione (v. [Componenti da installare del pacchetto antivirus](#)).



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**, **SpIDer Mail** e **Firewall Dr.Web** per evitare eventuali conflitti dei servizi di rete e dei componenti interni dell'antivirus Dr.Web.

Database dei virus

Per scoprire quali database dei virus sono installati su una postazione:

1. Selezionare la voce **Rete antivirus** del menu principale del **Pannello di controllo**, nella finestra che si è aperta nella lista gerarchica fare clic sul nome di una postazione.
2. Dal **menu di gestione** che si è aperto selezionare dalla sottosezione **Statistiche** la voce **Database dei virus**.
3. Si apre la finestra con le informazioni circa i database dei virus installati: nome del file di un concreto database dei virus; versione del database dei virus; data di creazione del database dei virus; numero di record nel database dei virus.



Se la visualizzazione della voce **Database dei virus** è disattivata, per attivarla, selezionare la voce **Amministrazione** del menu principale, nella finestra che si è aperta selezionare la voce del menu di gestione **Configurazione del Server Dr.Web**. Nella scheda **Statistiche** spuntare i flag **Stato dei database dei virus** e **Stato delle postazioni**, dopodiché riavviare il **Server**.

6.2.3. Hardware e software sulle postazioni SO Windows®

Dr.Web Enterprise Security Suite consente di accumulare e di visualizzare le informazioni circa l'hardware e il software delle postazioni protette SO Windows.

Per raccogliere le informazioni circa l'hardware e il software delle postazioni:

1. Attivare la raccolta delle statistiche sul **Server**:
 - a) Selezionare la voce **Amministrazione** del menu principale del **Pannello di controllo**.
 - b) Selezionare la voce del menu di gestione **Configurazione** del **Server Dr.Web**.
 - c) Nelle impostazioni del **Server** aprire la scheda **Statistiche** e spuntare il flag **Hardware e software**, se è deselezionato.
 - d) Per accettare le modifiche apportate, premere **Salva** e riavviare il **Server**.
2. Consentire la raccolta delle statistiche sulle postazioni:
 - a) Selezionare la voce **Rete antivirus** del menu principale del **Pannello di controllo**.
 - b) Nella lista gerarchica della rete antivirus, selezionare una postazione o un gruppo di postazioni per cui si vuole consentire la raccolta delle statistiche. Quando si seleziona un gruppo di postazioni, prestare attenzione all'ereditarietà di impostazioni: se alle postazioni del gruppo selezionato sono assegnate impostazioni individuali, la modifica delle impostazioni del gruppo non porterà alla modifica delle impostazioni della postazione.
 - c) Nel menu di gestione, nella sezione **Configurazione** → **Windows** selezionare la voce **Agent Dr.Web**.
 - d) Nelle impostazioni dell'**Agent**, nella scheda **Generali** spuntare il flag **Raccogli le informazioni sulle postazioni**, se è deselezionato. Se necessario, modificare il valore del parametro **Periodo di raccolta delle informazioni delle postazioni (min)**.
 - e) Per accettare le modifiche apportate, premere **Salva**. Le impostazioni verranno trasferite sulle postazioni.

Per visualizzare l'hardware e il software delle postazioni:

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



2. Nella lista gerarchica della rete antivirus, selezionare la postazione desiderata.
3. Nel menu di gestione, nella sezione **Generali** selezionare la voce **Hardware e software**.
4. Nella finestra che si è aperta viene riportato l'albero con l'elenco dell'hardware e del software che contiene le seguenti informazioni circa questa postazione:
 - **Application** - un elenco dei prodotti di programma installati sulla postazione.
 - **Hardware** - un elenco dell'hardware della postazione.
 - **Operating System** - informazioni sul sistema operativo della postazione.
 - **Windows Management Instrumentation** - informazioni sulla strumentazione di gestione SO Windows.
5. Per visualizzare informazioni dettagliate di un concreto oggetto hardware o software, selezionare l'oggetto desiderato nell'albero.

Per confrontare l'hardware e il software di diverse postazioni:

1. Selezionare la voce **Rete antivirus** del menu principale del **Pannello di controllo**.
2. Nella lista gerarchica della rete antivirus, selezionare diverse postazioni o gruppi di postazioni. Per visualizzare una pagina di confronto, si devono selezionare due o più postazioni SO Windows.
3. Nel menu di gestione, nella sezione **Generali** selezionare la voce **Comparazione dell'hardware e del software**.
4. Nella finestra che si è aperta sono disponibili le seguenti informazioni:
 - l'albero con l'elenco dell'hardware e del software;
 - una tabella di confronto delle postazioni selezionate.
5. Per visualizzare i dati confrontati, selezionare l'elemento desiderato nell'albero dell'hardware e del software. Tutti i valori disponibili dell'elemento selezionato verranno visualizzati nell'albero di comparazione.

6.3. Configurazione delle impostazioni della postazione

6.3.1. Permessi dell'utente della postazione



Per configurare i permessi dell'utente di postazione tramite il Pannello di controllo della sicurezza Dr.Web:

1. Selezionare la voce **Rete antivirus** del menu principale, nella finestra che si è aperta nella lista gerarchica fare clic sul nome di una postazione. Nel [menu di gestione](#) che si è aperto selezionare la voce **Permessi**. Si apre la finestra di configurazione dei permessi.
2. I permessi vengono modificati nelle schede che corrispondono al sistema operativo della postazione. Per modificare (concedere o togliere) un permesso, selezionare o deselezionare il flag di questo permesso.
3. I permessi per le postazioni SO Windows, Mac OS X, Linux e Android vengono modificati nelle seguenti schede:
 - ◆ **Componenti** - vengono configurati i permessi per la gestione dei componenti antivirus. Di default, l'utente ha il diritto di avvio di ciascun componente, però gli è vietato modificare la configurazione dei componenti e terminare i componenti.



- ◆ **Generali** - vengono configurati i permessi per la gestione dell'**Agent Dr.Web** e delle sue funzioni:

Tabella 6-1. Configurazione dei permessi della postazione nella scheda **Generali**

Flag della sezione Permessi	Azione del flag	Il risultato sulla postazione se il flag è deselezionato
Postazioni SO Windows		
Avvio nella modalità mobile	Spuntare il flag per permettere agli utenti su postazione di passare alla modalità mobile e di ricevere aggiornamenti direttamente dal Sistema d'aggiornamento mondiale Dr.Web se non è disponibile una connessione con il Server Dr.Web .	Nelle impostazioni di Agent , nella sezione Generali > Modalità non è disponibile l'impostazione Utilizza la Modalità mobile se non è disponibile la connessione al server .
Cambio della modalità di funzionamento	Spuntare il flag per permettere agli utenti su postazione di impostare le modalità di funzionamento di Agent Dr.Web .	Nelle impostazioni di Agent , nella sezione Generali > Modalità non sono disponibili le seguenti impostazioni: <ul style="list-style-type: none">• Accetta aggiornamenti dal server,• Accetta task dal server,• Accumula eventi.
Modifica della configurazione di Agent Dr.Web	Spuntare il flag per permettere agli utenti su postazione di modificare le impostazioni di Agent Dr.Web .	Nelle impostazioni di Agent , nella sezione Generali non sono disponibili le impostazioni delle seguenti sezioni: <ul style="list-style-type: none">• Avvisi: tutte le impostazioni non sono disponibili.• Modalità: non sono disponibili le impostazioni di connessione al Server e il flag Sincronizza l'ora del sistema con l'ora del server.• Auto-protezione: non sono disponibili le impostazioni Impedisci la modifica della data e dell'ora di sistema, Proibisci l'emulazione delle azioni dell'utente.• Avanzate: nelle impostazioni della sottosezione Log non sono disponibili le voci Aggiornamento di Dr.Web, Servizi Dr.Web, Crea memory dump in caso di errori di scansione.
Modifica della configurazione della protezione preventiva	Spuntare il flag per permettere agli utenti su postazione di modificare le impostazioni della protezione preventiva.	Nelle impostazioni di Agent , nella sezione Componenti di protezione > Protezione preventiva tutte le impostazioni non sono disponibili.
Disattivazione dell'auto-protezione	Spuntare il flag per permettere agli utenti su postazione di terminare l'auto-protezione.	Nelle impostazioni di Agent , nella sezione Principali > Auto-protezione non è disponibile l'impostazione Attiva l'auto-protezione .
Disinstallazione di Agent Dr.Web	Spuntare il flag per permettere agli utenti su postazione di disinstallare l' Agent Dr.Web .	Vieta la rimozione dell' Agent su postazione tramite l'installer e tramite i mezzi standard del SO Windows. In questo caso, la rimozione dell' Agent è possibile soltanto tramite la voce  Generali →  Disinstalla Agent Dr.Web nella barra degli strumenti del Pannello di controllo .
Postazioni Mac OS X		
Avvio nella modalità mobile	Spuntare il flag per permettere agli utenti su postazione di passare alla modalità mobile e di	Nella finestra principale dell'applicazione la sezione Aggiornamento è bloccato.



Flag della sezione Permessi	Azione del flag	Il risultato sulla postazione se il flag è deselezionato
	ricevere aggiornamenti direttamente dal Sistema d'aggiornamento mondiale Dr.Web se non è disponibile una connessione con il Server Dr.Web .	
Postazioni SO famiglia Linux		
Avvio nella modalità mobile	Spuntare il flag per permettere agli utenti su postazione di passare alla modalità mobile e di ricevere aggiornamenti direttamente dal Sistema d'aggiornamento mondiale Dr.Web se non è disponibile una connessione con il Server Dr.Web .	Per la modalità di funzionamento console dell'applicazione: il comando <code>drweb-ctl update</code> di aggiornamento dei database dei virus da SAM non è disponibile.
Postazioni SO Android		
Avvio nella modalità mobile	Spuntare il flag per permettere agli utenti di dispositivi mobili di passare alla modalità mobile e di ricevere aggiornamenti direttamente dal Sistema d'aggiornamento mondiale Dr.Web se non è disponibile una connessione con il Server Dr.Web .	Nella schermata principale dell'applicazione la sezione Aggiornamento è bloccato.



Quando viene disattivata un'impostazione responsabile per la modifica della configurazione dell'**Agent**, verrà utilizzato il valore assegnato a quest'impostazione per l'ultima volta prima della disattivazione.

Le azioni eseguite dalle relative voci del menu sono descritte nella documentazione **Dr.Web per Windows. Manuale dell'utente**.

4. Si possono propagare queste impostazioni ad un altro oggetto, premendo il pulsante **Propaga queste impostazioni verso un altro oggetto**.
5. Per esportare queste impostazioni in file, fare clic su **Esporta impostazioni da questa sezione in file**.
6. Per importare queste impostazioni da file, fare clic su **Importa impostazioni in questa sezione da file**.
7. Per accettare le modifiche fatte, premere il pulsante **Salva**.



Se al momento della modifica delle impostazioni, la postazione non è connessa al **Server**, le impostazioni verranno accettate non appena l'**Agent** si riconetterà al **Server**.

6.3.2. Calendario dei task della postazione

Dr.Web Enterprise Security Suite fornisce la possibilità di tenere un *calendario dei task centralizzato* che viene creato dall'amministratore di rete antivirus ed è aderente a tutte le regole di ereditarietà delle configurazioni.



Il *calendario dei task* è un elenco delle azioni che vengono eseguite automaticamente su postazioni all'ora stabilita. I calendari vengono utilizzati principalmente per eseguire le scansioni antivirus delle postazioni al momento più conveniente per gli utenti senza la necessità dell'avvio manuale dello **Scanner**. Inoltre, l'**Agent Dr.Web** consente di eseguire alcuni altri tipi di azioni che vengono descritti di seguito.

Il calendario centralizzato di esecuzione regolare dei task di concreti postazioni e gruppi viene modificato tramite il **Pannello di controllo**.

Per modificare il calendario centralizzato, eseguire le seguenti azioni:

1. Selezionare la voce **Rete antivirus** del 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. Nel **menu di gestione** che si è aperto selezionare la voce **Scheduler**. Si apre una lista dei task per le postazioni.



Di default, per le postazioni SO Windows il calendario contiene il task **Daily scan** - scansione quotidiana di postazione (vietata).

2. Per gestire il calendario, vengono utilizzati gli elementi corrispondenti nella barra degli strumenti:
 - a) Gli elementi generali della barra degli strumenti vengono utilizzati per creare nuovi task e per gestire la sezione calendario in generale. Questi strumenti sono sempre disponibili nella barra degli strumenti.



Crea task - aggiungere un nuovo task. Quest'azione viene descritta in dettaglio sotto nella sottosezione **Editor dei task**.



Propaga queste impostazioni verso un altro oggetto - copiare i task dal calendario in altri oggetti - postazioni o gruppi. Per maggiori informazioni consultare la sezione **Copiatura delle impostazioni in altri gruppi/postazioni**.



Esporta impostazioni da questa sezione in file - per esportare il calendario in un file dell'apposito formato.



Importa impostazioni in questa sezione da file - per importare il calendario da un file dell'apposito formato.

- b) Per gestire i task esistenti, spuntare i flag di fronte ai task richiesti oppure il flag nell'intestazione della tabella se si vogliono selezionare tutti i task nella lista. Con questo diventano disponibili gli elementi della barra degli strumenti utilizzati per la gestione di task selezionati.

Tabella 6-2. Elementi della barra degli strumenti utilizzati per gestire i task selezionati

Impostazione		Azione
Stato	Permetti l'esecuzione	Attivare l'esecuzione dei task selezionati secondo il calendario impostato se erano proibiti.
	Proibisci l'esecuzione	Proibire l'esecuzione dei task selezionati. I task saranno presenti nella lista ma non verranno eseguiti.






L'azione simile viene eseguita tramite l'editor del task nella scheda **Generali** con l'ausilio del flag **Permetti l'esecuzione**.

Importanza	Rendi critico	Eseguire il task in modo straordinario al successivo avvio di Agent Dr.Web se l'esecuzione di questo task è stata omessa nell'ora programmata.
	Rendi critico non	Eseguire il task solo nell'ora programmata, indipendentemente dall'omissione o dall'esecuzione del task.



L'azione simile viene eseguita tramite l'editor del task nella scheda **Generali** con l'ausilio del flag **Task critico**.



Impostazione	Azione
 Duplica le impostazioni	Duplicare i task selezionati nella lista del calendario corrente. Tramite l'azione Duplicare le impostazioni vengono creati nuovi task che hanno le impostazioni uguali a quelle dei task selezionati.
 Programma un'altra esecuzione dei task	Per i task per cui è impostata l'esecuzione singola: eseguire il task ancora una volta secondo le impostazioni di ora (ciò come cambiare la frequenza di esecuzione del task è descritto sotto nella sottosezione Editor dei task).
 Rimuovi i task selezionati	Rimuovere dal calendario il task selezionato.


3. Per modificare i parametri di un task, selezionarlo dalla lista dei task. Si apre la finestra **Editor dei task** descritta [sotto](#).
4. Dopo aver finito di modificare il calendario, fare clic su **Salva** per accettare le modifiche.



Se come risultato della modifica viene creato un calendario vuoto (che non contiene task), il **Pannello di controllo** chiede se si vuole utilizzare il calendario ereditato dai gruppi o il calendario vuoto. Si deve impostare il calendario vuoto se si vuole rifiutare il calendario ereditato dai gruppi.

Editor dei task

Tramite l'editor dei task si possono definire le impostazioni per:

1. Creare un nuovo task.
A questo fine fare clic sul pulsante  **Crea task** nella barra degli strumenti.
2. Modificare un task esistente.
A questo fine fare clic sul nome di uno dei task nella lista dei task.

Si apre la finestra di modifica dei parametri dei task. Le impostazioni di task per la modifica di un task esistente sono simili alle impostazioni per la creazione di un task nuovo.



I valori dei campi marcati con il carattere * devono essere impostati obbligatoriamente.

Per modificare i parametri di un task:

1. Nella scheda **Generali** vengono impostati i seguenti parametri:
 - ◆ Nel campo **Nome** viene definito il nome del task sotto cui verrà visualizzato nel calendario.
 - ◆ Per attivare l'esecuzione del task, spuntare il flag **Permetti l'esecuzione**. Se il flag non è selezionato, il task sarà presente nella lista ma non verrà eseguito.



L'azione simile viene eseguita nella finestra principale del calendario tramite l'elemento **Stato** della barra degli strumenti.

- ◆ Il flag spuntato **Task critico** comanda di avviare il task in modo straordinario alla prossima volta che si avvia l'**Agent Dr.Web** se l'esecuzione di tale task è stata omessa secondo il calendario (l'**Agent Dr.Web** è disattivato al momento di esecuzione del task). Se in un periodo il task viene omesso più volte, quando si avvia l'**Agent Dr.Web**, il task viene eseguito una volta.



L'azione simile viene eseguita nella finestra principale del calendario tramite l'elemento **Importanza** della barra degli strumenti.



Se in tale caso sono da essere eseguiti più task di scansione, ne viene eseguito solamente uno – il primo nella coda.

Per esempio, se è consentito il task **Daily scan** ed è stata rinviata la scansione critica tramite **Agent Scanner**, verrà eseguito **Daily scan**, e la scansione critica rinviata non potrà essere eseguita.

- Nella scheda **Azione** selezionare il tipo di task dalla lista a cascata **Azione** e configurare i parametri del task, richiesti per l'esecuzione.

Tabella 6-3. Tipi di task e i loro parametri

Tipo di task	Parametri e descrizione
Registrazione nel file di log	Stringa - testo del messaggio da registrare nel file di log.
Avvio del programma	<p>Impostare i seguenti parametri:</p> <ul style="list-style-type: none"> ◆ Nel campo Percorso — nome completo (con il percorso) del file eseguibile del programma da avviare. ◆ Nel campo Argomenti — parametri da riga di comando per il programma da avviare. ◆ Spuntare il flag Esegui in modo sincrono per attendere che sia finita l'esecuzione di questo programma prima di eseguire gli altri task del tipo Avvio del programma. Se il flag Esegui in modo sincrono non è spuntato, l'Agent avvia il programma e registra nel log soltanto il suo avvio. Se il flag Esegui in modo sincrono è spuntato, l'Agent registra nel log il suo avvio, il codice di restituzione e l'ora di conclusione del programma.
Scanner Dr.Web. Scansione rapida	I parametri di configurazione della scansione sono descritti nel p. Scansione antivirus della postazione .
Scanner Dr.Web. Scansione personalizzata	
Scanner Dr.Web. Scansione completa	



L'avvio remoto dello **Scanner** è possibile soltanto sulle postazioni SO Windows, SO della famiglia UNIX e Mac OS X.

- Nella scheda **Tempo**:
 - ◆ Dalla lista a cascata **Periodicità** selezionare la modalità di avvio del task e impostare il tempo secondo la periodicità scelta.

Tabella 6-4. Modalità di avvio e i loro parametri

Modalità di avvio	Parametri e descrizione
Iniziale	<p>Il task verrà eseguito all'avvio di Agent.</p> <p>Viene avviato senza parametri supplementari.</p>
Tra N minuti dopo il task iniziale	<p>Dalla lista a cascata Task iniziale è necessario scegliere il task rispetto al quale viene impostata l'ora di esecuzione del task corrente.</p> <p>Nel campo Minuto impostare o selezionare dalla lista il numero di minuti da aspettare dopo l'esecuzione del task iniziale prima che venga avviato il task corrente.</p>
Ogni giorno	È necessario inserire l'ora e il minuto — il task verrà avviato ogni giorno all'ora indicata.
Ogni mese	È necessario selezionare un giorno (giorno del mese), immettere l'ora e il minuto — il task verrà avviato nel giorno del mese selezionato all'ora indicata.
Ogni settimana	È necessario selezionare un giorno della settimana, immettere l'ora e il minuto — il task verrà avviato nel giorno della settimana selezionato all'ora indicata.



Modalità di avvio	Parametri e descrizione
Ogni ora	È necessario immettere un numero dallo 0 ai 59 che indica il minuto di ogni ora in cui il task verrà avviato.
Ogni N minuti	È necessario immettere il valore N per definire l'intervallo di tempo dell'esecuzione del task. Se N è pari ai 60 o superiore, il task verrà avviato ogni N minuti. Se N è inferiore ai 60, il task verrà avviato ogni minuto dell'ora multiplo di N .

- ◆ Spuntare il flag **Proibisci dopo la prima esecuzione** per eseguire il task soltanto una volta secondo l'ora impostata. Se il flag è tolto, il task verrà eseguito molte volte con la periodicità selezionata.

Per ripetere l'esecuzione di un task la cui esecuzione è definita come singola e che è già stato eseguito, utilizzare il pulsante **Programma un'altra esecuzione dei task** che si trova nella barra degli strumenti della sezione calendario.

4. Finite le modifiche dei parametri del task, fare clic sul pulsante **Salva** per accettare le modifiche dei parametri del task, se veniva modificato un task esistente, oppure per creare un nuovo task con i parametri impostati, se veniva creato un nuovo task.

6.3.3. Componenti da installare del pacchetto antivirus

Per configurare la lista dei componenti da installare del pacchetto antivirus:

1. Selezionare la voce **Rete antivirus** del menu principale del **Pannello di controllo**, nella finestra che si è aperta nella lista gerarchica selezionare una postazione o. Nel [menu di gestione](#) che si è aperto, selezionare la voce **Componenti da installare**.
2. Per i componenti richiesti, dalla lista a cascata selezionare una delle opzioni:
 - ◆ **Deve essere installato** – comanda la disponibilità obbligatoria del componente sulla postazione. Quando viene creata una nuova postazione, il componente viene incluso obbligatoriamente nel pacchetto antivirus da installare. Quando il valore **Deve essere installato** viene impostato per una postazione già esistente, il componente viene aggiunto al pacchetto antivirus disponibile.
 - ◆ **Può essere installato** – determina la possibilità di installare il componente antivirus. L'utente decide se vuole installare il componente quando installa l'**Agent**.
 - ◆ **Non può essere installato** – vieta la disponibilità del componente sulla postazione. Quando viene creata una nuova postazione, il componente non viene incluso nel pacchetto antivirus da installare. Quando il valore **Non può essere installato** viene impostato per una postazione già esistente, il componente viene rimosso dal pacchetto antivirus.

Nella tabella 6-5 è indicato se il componente verrà installato su una postazione (+) a seconda delle impostazioni configurate dall'utente e di quelle configurate dall'amministratore sul **Server**.

Tabella 6-6.

Parametri impostati dall'utente	Parametri impostati sul Server		
	Deve	Può	Non può
Installa	+	+	
Non installare	+		

3. Fare clic sul pulsante **Salva** per salvare le impostazioni e la relativa modifica dei componenti del pacchetto antivirus sulla postazione.



Il componente **Antsipam Dr.Web** non può essere installato se non è stato installato almeno uno dei seguenti prodotti:

- ◆ **SpIDer Mail**,
- ◆ **Dr.Web per Microsoft Outlook**.

6.4. Configurazione dei componenti antivirus

Per visualizzare o modificare le impostazioni dei componenti antivirus sulla postazione:

1. Selezionare la voce **Rete antivirus** del menu principale del **Pannello di controllo**.
2. Nella finestra che si è aperta, nella lista gerarchica fare clic sul nome di una postazione o di un gruppo.
3. Nel menu di gestione che si è aperto, nella sezione **Configurazione**, nella sottosezione corrispondente al sistema operativo delle postazioni selezionate, selezionare il componente richiesto.
4. Si apre la finestra di configurazione del componente antivirus.



Le impostazioni dei componenti e le raccomandazioni per la configurazione sono riportate nel **Manuale dell'utente** per il relativo sistema operativo.

Tuttavia, alcune impostazioni di componenti nel **Pannello di controllo** e sulle postazioni potrebbero essere diverse per livello di dettaglio.

In questo Manuale vengono riportate le impostazioni dell'**Agent Dr.Web per Windows** che sono impostazioni avanzate dell'**Agent** disponibili all'utente sulla postazione, nonché le impostazioni dei componenti antivirus non disponibili su postazioni protette.



Configurando i componenti antivirus per le postazioni SO Windows, prestare attenzione alle seguenti caratteristiche della registrazione del log:


- Sul lato **Pannello di controllo** le impostazioni di log vengono configurate separatamente per ciascuno componente nelle sezioni **Log**. Sulla postazione le impostazioni di log vengono configurate nella sezione unica **Avanzate**.
- Quando viene abilitata l'opzione **Registra log dettagliato**, il log di funzionamento del rispettivo componente viene registrato in modalità di debug con il livello di dettagli massimo. In questa modalità vengono tolte le limitazioni su dimensione di file. Questo comporta un notevole aumento della dimensione del file di log. Inoltre, prestare attenzione a ciò che la rotazione del file di log non viene eseguita (questo riguarda tutte le modalità di registrazione di log).
La modalità di debug della registrazione di log riduce le prestazioni dell'antivirus e del sistema operativo della postazione. Utilizzare questa modalità solo se si verificano problemi nel funzionamento dei componenti, a richiesta del servizio di supporto tecnico. Non è consigliabile abilitare la modalità di debug della registrazione di log per un tempo lungo.


La gestione delle impostazioni di componenti antivirus attraverso il **Pannello di controllo** presenta alcune differenze rispetto alla gestione delle impostazioni direttamente attraverso i relativi componenti dell'antivirus sulla postazione:


- ◆ per gestire singoli parametri, utilizzare i pulsanti locati a destra delle impostazioni corrispondenti:
 - ↶ **Imposta il valore iniziale** - per ripristinare il parametro nel valore che aveva prima della modifica.
 - ↶ **Resetta al valore di default** - per ripristinare il parametro nel valore di default.
- ◆ per gestire un insieme di parametri, utilizzare i pulsanti nella barra degli strumenti:
 - ⚙️ **Resetta tutti i parametri ai valori iniziali** - per ripristinare tutti i parametri di questa sezione ai valori che avevano prima della modifica corrente (ultimi valori salvati).





 **Resetta tutti i parametri ai valori default** - per ripristinare tutti i parametri di questa sezione ai valori di default.

 **Propaga queste impostazioni verso un altro oggetto** - per copiare le impostazioni da questa sezione nella configurazione di un'altra postazione, di un altro gruppo o di alcuni gruppi e postazioni.

 **Imposta l'ereditarietà delle impostazioni dal gruppo primario** - per eliminare le impostazioni individuali delle postazioni e per impostare l'ereditarietà delle impostazioni di questa sezione dal gruppo primario.

 **Copia le impostazioni dal gruppo primario e impostale come individuali** - per copiare le impostazioni di questa sezione dal gruppo primario e per assegnarle alle postazioni selezionate. In questo caso, l'ereditarietà non viene impostata e le impostazioni della postazione vengono considerate individuali.

 **Esporta le impostazioni da questa sezione in file** - per salvare tutte le impostazioni da questa sezione in un file di un apposito formato.

 **Importa le impostazioni in questa sezione da file** - per sostituire tutte le impostazioni in questa sezione con le impostazioni salvate in un file dell'apposito formato.

5. Dopo aver apportato delle modifiche nelle impostazioni tramite il **Pannello di controllo**, per accettare queste modifiche, premere il pulsante **Salva**. Le impostazioni verranno trasferite sulle postazioni. Se le postazioni non sono online al momento della modifica, le impostazioni verranno trasferite dopo che le postazioni si conatteranno al **Server**.

6.4.1. Componenti

A seconda del sistema operativo della postazione, vengono forniti i seguenti componenti antivirus:

Postazioni SO Microsoft® Windows®

Scanner Dr.Web, Dr.Web Agent Scanner

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

SpIDer Guard

Scansione continua del file system in tempo reale. Controllo di ogni processo avviato e dei file che vengono creati su dischi rigidi e vengono aperti su supporti rimovibili.

SpIDer Mail

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).

SpIDer Gate

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 alle 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 occasionali o contro l'infezione di virus, e vieta ai dipendenti l'accesso alle informazioni indesiderate.

Firewall

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



Quarantena

Isolamento di oggetti dannosi e sospettosi in apposita cartella.

Auto-protezione

Protezione dei file e delle cartelle **Dr.Web Enterprise Security Suite** contro la rimozione o la modifica non autorizzata o accidentale da parte dell'utente e contro la rimozione o la modifica da parte del malware. Quando l'auto-protezione è attivata, l'accesso ai file e alle cartelle **Dr.Web Enterprise Security Suite** è consentito solamente ai processi **Dr.Web**.

Protezione preventiva (le impostazioni sono disponibili nelle impostazioni dell'Agent Dr.Web)

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

Postazioni SO famiglia UNIX®

Scanner Dr.Web, Dr.Web Agent Scanner

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**.

SpIDer Guard

Scansione continua del file system in tempo reale. Controllo di ogni processo avviato e dei file che vengono creati su dischi rigidi e vengono aperti su supporti rimovibili.

SpIDer Gate

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 sospettosi in apposita cartella.



Gli altri componenti, di cui le impostazioni sono riportate nel **Pannello di controllo** per le postazioni SO della famiglia UNIX, sono aggiuntive e servono per la configurazione interna del funzionamento del software antivirus.

Postazioni Mac OS® X

Scanner Dr.Web, Dr.Web Agent Scanner

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**.

SpIDer Guard

Scansione continua del file system in tempo reale. Controllo di ogni processo avviato e dei file che vengono creati su dischi rigidi e vengono aperti su supporti rimovibili.

Quarantena

Isolamento di oggetti dannosi e sospettosi in apposita cartella.

Dispositivi mobili SO Android

Scanner Dr.Web, Dr.Web Agent Scanner

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**.

SpIDer Guard

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



Filtraggio di chiamate e di messaggi

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

Antifurto

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

Cloud Checker

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

Firewall (le impostazioni sono disponibili soltanto sul dispositivo mobile)

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

Security auditor (le impostazioni sono disponibili soltanto sul dispositivo mobile)

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

Filtro delle applicazioni

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

Server SO Novell® NetWare®

Scanner Dr.Web

Scansione del computer on demand e secondo il calendario.

SpIDer Guard

Scansione continua del file system in tempo reale. Controllo di ogni processo avviato e dei file che vengono creati su dischi rigidi e vengono aperti su supporti rimovibili.

6.4.2. Configurazione di Agent Dr.Web per Windows®

Per visualizzare o modificare le impostazioni di un Agent Dr.Web installato su una postazione Windows:

1. Selezionare la voce **Rete antivirus** del menu principale del **Pannello di controllo**.
2. Nella finestra che si è aperta, nella lista gerarchica fare clic sul nome di una postazione o di un gruppo.
3. Nel **menu di gestione** che si è aperto selezionare la voce **Configurazione > Windows > Agent Dr.Web**.
4. Si apre la finestra di configurazione dell'**Agent**.



Se in queste impostazioni si apportano delle modifiche non coerenti con le impostazioni del **Server** (in particolare, modifica della modalità di cifratura e di compressione e della chiave di cifratura), questo provoca la perdita di connessione tra l'**Agent** e il **Server**.

5. Dopo aver apportato delle modifiche nelle impostazioni dell'**Agent** tramite il **Pannello di controllo**, per accettare queste modifiche, premere il pulsante **Salva**.



6.4.2.1. Generali

Nella scheda **Generali** vengono impostati i seguenti parametri dell'**Agent**:

- ◆ Nel campo **Differimento di avvio dello scheduler (min)** impostare il valore di timeout che intercorre tra la partenza del sistema operativo e l'inizio di esecuzione del task iniziale di scansione, se è impostato nel calendario dei task dell'**Agent**. Di default, è impostato 1 minuto. Se viene impostato il valore 0, il task di scansione viene avviato senza differimento, cioè subito dopo il caricamento dell'SO.
- ◆ Nel campo **Periodicità di invio delle statistiche (min)** impostare il valore dell'intervallo di tempo in minuti in cui l'**Agent** invia sull'**Server** tutte le informazioni statistiche raccolte dai componenti **SpIDer Guard**, **SpIDer Mail** e **SpIDer Gate** sulla postazione. Impostare 0 per disattivare l'invio delle statistiche.
- ◆ Nella lista a cascata **Lingua** viene impostata la lingua dell'interfaccia dell'**Agent** e dei componenti dell'**Antivirus Dr.Web** su una postazione o in un gruppo di postazioni.
- ◆ Spuntare il flag **Abilita Microsoft Network Access Protection** per abilitare il monitoraggio dello stato delle postazioni con utilizzo della tecnologia *Microsoft® Network Access Protection*. In questo caso viene attivato *Agent di operatività del sistema (System Health Agent - SHA) che viene installato automaticamente insieme al software Agent Dr.Web su postazione* (per maggiori informazioni v. p. [NAP Validator](#)).
- ◆ Spuntare il flag **Consenti la gestione remota della quarantena** per consentire di gestire la quarantena sulle postazioni su remoto dal **Server**.



La voce **Consenti la gestione remota della quarantena** è disponibile se nella sezione **Amministrazione** → **Configurazione del Server Dr.Web** → scheda **Statistiche** è spuntato il flag **Stato della quarantena**.

- ◆ Spuntare il flag **Raccogli le informazioni sulle postazioni** per permettere di raccogliere le informazioni riguardanti l'hardware e il software delle postazioni. Se il flag è spuntato, dalla lista a cascata **Periodo di raccolta delle informazioni delle postazioni (min)**, selezionare la periodicità in minuti con cui gli **Agent** inviano sul **Server** le informazioni attuali circa l'hardware e il software sulla postazione.
- ◆ Spuntare il flag **Sincronizza l'ora** per abilitare la sincronizzazione dell'ora sulla postazione su cui è installato l'**Agent** con l'ora di sistema sul computer su cui è installato il **Server Dr.Web**.
- ◆ Spuntare il flag **Impedisci la modificazione della data e dell'ora di sistema** per impedire la modifica manuale e automatica delle impostazioni di data e di ora di sistema, fatta eccezione per la sincronizzazione dell'ora con il **Server Dr.Web** (viene impostata tramite il flag **Sincronizza l'ora**).
- ◆ Spuntare il flag **Proibisci l'emulazione delle azioni dell'utente** per proibire qualsiasi modifica nel funzionamento del **Dr.Web**, fatta eccezione per modifiche apportate manualmente dall'utente.
- ◆ Spuntare il flag **Connettiti ai servizi basati sul cloud** per connettere la postazione ai servizi basati sul cloud di **Doctor Web**. Questo consentirà ai componenti antivirus della postazione di controllare dati alla ricerca di minacce utilizzando le informazioni trasmesse in tempo reale dai server di **Doctor Web**. In questo caso sui server di **Doctor Web** verranno inviate automaticamente le informazioni su funzionamento dei componenti **Dr.Web** sulla postazione.

6.4.2.2. Rete


Nella scheda **Rete** vengono impostati i parametri che configurano la comunicazione con il **Server**:


- ◆ Nel campo **Chiave pubblica** viene impostata la chiave di cifratura pubblica di **Server Dr.Web** (`drwcsd.pub`) conservata sulla postazione. Per selezionare il file della chiave, fare clic sul pulsante





Più chiavi pubbliche potrebbero essere memorizzate contemporaneamente su una postazione, per esempio, durante la sostituzione delle chiavi di cifratura o durante il trasferimento da un **Server** su un altro. Le chiavi devono essere uniche, cioè non si devono impostare due chiavi pubbliche identiche.


Per aggiungere un'altra chiave pubblica, fare clic sul pulsante  e selezionare il file della chiave.

Per rimuovere una chiave esistente dalla postazione, fare clic sul pulsante .



Se il flag **Consenti il funzionamento senza una chiave pubblica** non è spuntato, è vietata la rimozione dell'ultima chiave pubblica.

- ◆ Spuntare il flag **Consenti il funzionamento senza una chiave pubblica** per consentire la connessione degli **Agent** se non hanno la chiave di cifratura pubblica (`drwcsd.pub`) o se il file della chiave ha una struttura non valida.
- ◆ Spuntare il flag **Consenti il funzionamento con una chiave pubblica non valida** per consentire la connessione degli **Agent** se hanno la chiave di cifratura pubblica non valida (`drwcsd.pub`).
- ◆ Nel campo **Server** viene impostato l'indirizzo di **Server Dr.Web**. Questo campo può rimanere vuoto. In questo caso l'**Agent** utilizza come indirizzo di **Server Dr.Web** il valore del parametro indicato nelle impostazioni del computer locale dell'utente (indirizzo del **Server** da cui è stata eseguita l'installazione).

È possibile impostare un indirizzo di **Server** o più indirizzi di diversi **Server**. Per aggiungere un altro indirizzo di **Server**, fare clic sul pulsante  e inserire l'indirizzo nel campo che è stato aggiunto. Il formato in cui si devono impostare gli indirizzi di rete di **Server** è descritto nel documento **Allegati**, sezione [Allegato E. Specifica indirizzo di rete](#).

Esempio di come si imposta l'indirizzo di **Server**:

```
tcp/10.4.0.18:2193  
tcp/10.4.0.19  
10.4.0.20
```



Se viene impostato un valore non corretto/non valido del parametro **Server**, gli **Agent** si sconnettono dal **Server** e non possono più connettersi ad esso. In questo caso, l'indirizzo del **Server** deve essere impostato direttamente sulla postazione.

- ◆ Nel campo **Numero di tentativi di ricerca** impostare il parametro che determina il numero di tentativi di ricerca di **Server Dr.Web** per la connessione nella modalità [Mulicasting](#).
- ◆ Nel campo **Time-out di ricerca (s)** impostare un intervallo in secondi tra i tentativi di **ricerca di Server Dr.Web** per la connessione nella modalità [Mulicasting](#).
- ◆ I campi **Modalità di compressione** e **Modalità di cifratura** definiscono le impostazioni rispettive della compressione e della cifratura del traffico dati di rete (inoltre v. p. [Utilizzo di cifratura e di compressione traffico dati](#)).
- ◆ Nel campo **Parametri di ascolto della rete** indicare la porta UDP utilizzata dal **Pannello di controllo** per cercare nella rete gli **Agent Dr.Web** operativi. Impostare il valore **NONE** per vietare l'ascolto su porte.

Il parametro viene impostato nel formato di indirizzo di rete riportato nel documento **Allegati**, sezione [Allegato E. Specifica indirizzo di rete](#).

Di default si utilizza **udp/:2193** che significa "tutte le interfacce, porta 2193".



6.4.2.3. Mobilità

Nella scheda **Mobilità** si impostano i parametri della *Modalità mobile Agent*:

- ◆ Nel campo **Periodicità degli aggiornamenti (sec)** impostare un intervallo di tempo in secondi tra gli aggiornamenti del software antivirus.
- ◆ Spuntare il flag **Utilizza server proxy** per utilizzare un server proxy HTTP per la ricezione degli aggiornamenti da Internet. Con questo vengono attivati i campi delle impostazioni del server proxy in uso.

6.4.2.4. Log

Nella scheda **Log** vengono impostati i parametri di gestione del log dell'**Agent** e di alcuni componenti dell'**Antivirus Dr.Web**:

- ◆ Il parametro **Livello di dettaglio del log di Agent** definisce il livello di dettaglio del log di funzionamento **Agent**.
- ◆ Il parametro **Livello di dettaglio del log del motore** definisce il livello di dettaglio del log di funzionamento del motore di ricerca (Scanning Engine).
- ◆ Il parametro **Livello di dettaglio del log degli aggiornamenti** il livello di dettaglio del log di funzionamento del modulo di aggiornamento **Dr.Web**.
- ◆ Spuntare il flag **Crea memory dump in caso di errori di scansione** per creare memory dump in caso di errori di scansione. Si consiglia di attivare quest'opzione per l'analisi di errori nel funzionamento di **Dr.Web**.

6.4.2.5. Interfaccia

Nella scheda **Interfaccia** si impostano le opzioni dell'interfaccia di **Agent Dr.Web**:

- ◆ Spuntare il flag **Mostra l'icona nella barra delle applicazioni** per visualizzare l'icona dell' **Agent** nella barra delle applicazioni. Se l'icona è disattivata, l'utente non potrà visualizzare e modificare le impostazioni dell'**Agent** e del pacchetto antivirus.
- ◆ Spuntare il flag **Visualizza la richiesta di riavvio** per visualizzare la richiesta di riavvio della postazione. Se il flag è tolto, l'avviso non viene visualizzato sulla postazione e il riavvio automatico della postazione non viene eseguito. Nelle statistiche della postazione ricevute dal **Pannello di controllo**, viene segnalata la necessità di riavviare la postazione. Le informazioni sullo stato che richiede il riavvio vengono visualizzate nella tabella **Stati**. Se necessario, l'amministratore può riavviare la postazione dal **Pannello di controllo** (v. sezione [Rete antivirus](#)).

Per marcare il tipo di avvisi di eventi che l'utente riceverà, mettere il flag corrispondente:

- ◆ **Avvisi critici** - per ricevere solamente gli avvisi critici. Ad essi appartengono gli avvisi periodici:
 - di errore di aggiornamento del software antivirus o di un suo componente;
 - di necessità di riavviare il computer dopo l'aggiornamento.

L'avviso viene visualizzato solamente se l'utente ha privilegi di amministratore.

- ◆ **Avvisi di minacce** – per ricevere solamente gli avvisi dei virus. Ad essi appartengono gli avvisi di rilevamento di un virus (di più virus) da uno dei componenti del software antivirus.
- ◆ **Avvisi importanti** – per ricevere solamente gli avvisi importanti. Ad essi appartengono gli avvisi:
 - di errori durante l'avvio di un componente del software antivirus;
 - di errori di aggiornamento del software antivirus o di un suo componente, viene visualizzato subito dopo la chiusura anormale della procedura di aggiornamento;
 - di necessità di riavviare il computer dopo l'aggiornamento, viene visualizzato subito dopo l'aggiornamento;



- di necessità di aspettare la richiesta di riavvio per completare l'installazione dei componenti.
- ◆ **Avvisi secondari** – per ricevere solamente gli avvisi secondari. Ad essi appartengono gli avvisi:
 - di avvio della scansione remota;
 - di completamento della scansione remota;
 - di avvio dell'aggiornamento del software antivirus o di un suo componente;
 - di completamento con successo dell'aggiornamento del software antivirus o di un suo componente (senza la necessità di riavvio).

Affinché l'utente riceva tutti i gruppi di avvisi, spuntare tutti i quattro flag. Altrimenti, verranno visualizzati solo gli avvisi dei gruppi indicati.



L'utente può gestire la ricezione degli avvisi, ad eccezione degli **Avvisi critici** di cui la ricezione può essere configurata solamente dall'amministratore.

La ricezione degli avvisi può essere configurata tramite il **Pannello di controllo** fino alla prima modifica di queste impostazioni sul lato utente. Una volta sono state definite le impostazioni personalizzate sul lato utente, la ricezione degli avvisi può essere configurata solamente tramite il menu contestuale dell'**Agent**.

Nella sottosezione **Avanzate** vengono definite le seguenti impostazioni:

- ◆ Spuntare il flag **Non visualizzare avvisi in modalità a schermo intero** per disattivare gli avvisi pop-up se un programma è in esecuzione in modalità a schermo intero.
- ◆ Spuntare il flag **Visualizza avvisi Firewall su uno schermo separato in modalità a schermo intero** affinché gli avvisi del **Firewall Dr.Web** vengano visualizzati su un desktop separato, ovvero sopra un'applicazione in esecuzione a schermo intero. È consigliabile attivare quest'opzione per evitare che le connessioni di rete dell'applicazione in esecuzione a schermo intero vengano bloccate senza che sia possibile consentirle al momento della richiesta fatta dal **Firewall Dr.Web**.

6.4.2.6. Protezione preventiva

Nella scheda **Protezione preventiva**, sezione **Livello di proibizione delle azioni sospette** si può definire la reazione di **Dr.Web** alle azioni di programmi estranei che potrebbero portare all'infezione della postazione. Inoltre, si possono proteggere le informazioni degli utenti contro le modifiche indesiderate.

Selezionare uno dei livelli della protezione fornita dall'antivirus:

- ◆ **Paranoide** – il livello massimo di protezione adatto quando è necessario il completo controllo dell'accesso agli oggetti critici di Windows.



In questa modalità di protezione sono possibili conflitti di compatibilità con programmi di terzi che utilizzano i rami di registro protetti.

- ◆ **Medio** – il livello di protezione adatto quando esiste l'alto rischio di infezione. In questa modalità, viene proibito additionally l'accesso a quegli oggetti critici che potenzialmente potrebbero essere sfruttati da programmi malevoli.
- ◆ **Minimo** – il livello di protezione che proibisce le modifiche automatiche degli oggetti di sistema di cui una modifica sarebbe un chiaro segno di un tentativo di effetto nocivo sul sistema operativo.
- ◆ **Personalizzato** – il livello di protezione che viene definito dall'utente (amministratore di **Server**) sulla base delle impostazioni definite nella tabella sottostante.

Per definire le impostazioni personalizzate di protezione preventiva, nella tabella di questa sezione mettere i flag in una delle seguenti posizioni:

- **Consenti** – per consentire sempre le azioni con questo oggetto o da parte di questo oggetto.



- **Chiedi** – per visualizzare una finestra di dialogo affinché l'utente possa impostare l'azione necessaria per il concreto oggetto.
- **Proibisci** – per proibire sempre le azioni con questo oggetto o da parte di questo oggetto.

Se le impostazioni nella tabella vengono modificate, se in precedenza nel campo **Livello di proibizione delle azioni sospette** è stato impostato uno dei livelli predefiniti, il livello cambia automaticamente in quello **Personalizzato**.

Le impostazioni di protezione preventiva consentono di controllare i seguenti oggetti:

- ◆ **Integrità delle applicazioni in esecuzione** – per cercare processi che si incorporano nelle applicazioni in esecuzione, il che costituisce una minaccia alla sicurezza del computer. Non viene monitorato il comportamento dei processi che sono stati aggiunti alle esclusioni del componente **SpIDer Guard**.
- ◆ **Integrità dei file degli utenti** – per cercare processi che modificano file degli utenti secondo un algoritmo conosciuto che è un segno di ciò che tali processi sono una minaccia alla sicurezza del computer. Non viene monitorato il comportamento dei processi che sono stati aggiunti alle esclusioni del componente **SpIDer Guard**. Per proteggere le informazioni degli utenti contro le modifiche non autorizzate, si consiglia di configurare la creazione dei backup dei file importanti.
- ◆ **File HOSTS** – questo file viene utilizzato dal sistema operativo per semplificare l'accesso a Internet. Le modifiche di questo file potrebbero essere il risultato del funzionamento di un virus o di un altro programma malevolo.
- ◆ **Accesso di basso livello al disco** – proibisce alle applicazioni la registrazione su disco settore per settore senza l'utilizzo del file system.
- ◆ **Caricamento driver** – proibisce alle applicazioni di caricare driver nuovi o sconosciuti.

Le altre impostazioni sono responsabili delle aree critiche di Windows e consentono di proteggere rami di registro contro le modifiche (sia nel profilo di sistema che nei profili di tutti gli utenti).

Tabella 6–7. Rami di registro protetti

Impostazione	Ramo di registro
Accesso a Image File Execution Options	Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
Accesso a User Drivers	Software\Microsoft\Windows NT\CurrentVersion\Drivers32 Software\Microsoft\Windows NT\CurrentVersion\Userinstallable.drivers
Parametri della shell Winlogon	Software\Microsoft\Windows NT\CurrentVersion\Winlogon, Userinit, Shell, UIHost, System, Taskman, GinaDLL
Notifiche di Winlogon	Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify
Avvio automatico della shell di Windows	Software\Microsoft\Windows NT\CurrentVersion\Windows, AppInit_DLLs, LoadAppInit_DLLs, Load, Run, IconServiceLib
Associazione di file eseguibili	Software\Classes\.exe, .pif, .com, .bat, .cmd, .scr, .lnk (chiavi) Software\Classes\exefile, piffile, comfile, batfile, cmdfile, scrfile, lnkfile (chiavi)
Criteri restrizione software (SRP)	Software\Policies\Microsoft\Windows\Safer
Plugin di Internet Explorer (BHO)	Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
Esecuzione automatica programmi	Software\Microsoft\Windows\CurrentVersion\Run Software\Microsoft\Windows\CurrentVersion\RunOnce Software\Microsoft\Windows\CurrentVersion\RunOnceEx Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup Software\Microsoft\Windows\CurrentVersion\RunOnceEx\Setup Software\Microsoft\Windows\CurrentVersion\RunServices Software\Microsoft\Windows\CurrentVersion\RunServicesOnce



Impostazione	Ramo di registro
Esecuzione automatica criteri	Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
Configurazione della modalità provvisoria	SYSTEM\ControlSetXXX\Control\SafeBoot\Minimal SYSTEM\ControlSetXXX\Control\SafeBoot\Network
Parametri di Session Manager	System\ControlSetXXX\Control\Session Manager\SubSystems, Windows
Servizi di sistema	System\CurrentControlXXX\Services



In caso di problemi con l'installazione degli aggiornamenti critici di Microsoft o con l'installazione e con il funzionamento dei programmi (compresi programmi di deframmentazione), disattivare le opzioni corrispondenti in questo gruppo di opzioni.

6.4.3. Configurazione di SpIDer Mail per Windows®. Filtro delle applicazioni

Il **Filtro delle applicazioni** consente di configurare un'intercettazione manuale delle connessioni ai server di posta. In questa modalità **SpIDer Mail** svolge il ruolo di un server proxy tra i mail client e i mail server e tiene d'occhio soltanto quelle connessioni che sono specificate nelle impostazioni in una forma esplicita. L'utilizzo di questo tipo di intercettazione richiede [la modifica delle impostazioni](#) di connessione dei mail client su postazioni.

La lista degli indirizzi da intercettare consiste in record, ciascuno di cui stabilisce una corrispondenza tra le impostazioni di **SpIDer Mail** e quelle del server di posta.



Di default, la lista di intercettazione è vuota. Si possono aggiungere record desiderati.

Configurazione dell'intercettazione di connessioni



1. Fare una lista dei server di posta, le connessioni a cui si vogliono intercettare, e assegnare numeri di porta a questi server in ordine casuale. Utilizzare soltanto le porte libere, non di sistema. Di seguito queste porte verranno denominate le *porte di SpIDer Mail*.



SpIDer Mail supporta i server di posta che utilizzano i protocolli POP3, SMTP, IMAP4 o NNTP.

2. Selezionare la voce **Rete antivirus** del menu principale del **Pannello di controllo**.
3. Nella finestra che si è aperta, nella lista gerarchica fare clic sul nome di una postazione o di un gruppo.
4. Nel [menu di gestione](#) che si è aperto selezionare la voce **Configurazione > Windows > SpIDer Mail**. Passare alla scheda **Filtro delle applicazioni**.
5. Nella sezione **Configurazione delle connessioni di SpIDer Mail**, impostare i seguenti parametri:
 - ◆ **Porta di SpIDer Mail** – la *porta di SpIDer Mail* selezionata per un server di posta nel passo 1;
 - ◆ **Server** – il nome a dominio o l'indirizzo IP del server di posta;
 - ◆ **Porta** – il numero di porta utilizzato dal server di posta.
6. Se necessario, ripetere il passo 5 per ulteriori server. Per aggiungere un altro server di posta alla lista, premere il pulsante .
7. Per smettere di intercettare le connessioni a un determinato server di posta, premere il pulsante  di fronte all'elemento di lista che corrisponde a questo server.
8. Nella lista **Applicazioni da escludere** si può impostare un elenco delle applicazioni di cui il traffico dati non verrà intercettato e, di conseguenza, non verrà analizzato dal componente **SpIDer Mail**:



- a) Per escludere un'applicazione dalla scansione, impostare il percorso del file eseguibile dell'applicazione.
 - b) In ogni campo viene impostato soltanto un'applicazione da escludere. Per aggiungere un altro elemento alla lista, premere il pulsante .
 - c) Per cancellare un'applicazione dalla lista delle eccezioni, premere il pulsante  di fronte all'elemento di lista che corrisponde a quest'applicazione.
9. Dopo aver assegnato tutte le impostazioni necessarie, premere il pulsante **Salva** per applicare le modifiche sulla postazione.



Il **Filtro delle applicazioni** del componente **SpIDer Mail** può essere configurato soltanto sul lato **Server Dr.Web**. Le relative impostazioni sulla postazione non sono disponibili.

10. Configurare il client di posta sulla postazione per l'interazione con il componente **SpIDer Mail** per l'intercettazione manuale di connessioni.

Configurazione del client di posta

Se **SpIDer Mail** è configurato per l'intercettazione manuale delle connessioni con i server di posta, modificare le impostazioni del client di posta su postazione in un modo appropriato:

1. Come l'indirizzo del server delle email in arrivo e in uscita, indicare `localhost`.
2. Come la porta del server di posta, indicare la *porta di SpIDer Mail* assegnata al relativo server di posta.

Di regola, a tale scopo è necessario indicare nelle impostazioni dell'indirizzo del server di posta:

`localhost:<porta_di_SpIDer_Mail>`

dove `<porta_di_SpIDer_Mail>` – la porta assegnata al relativo server di posta.

Per esempio:

Se al server di posta con l'indirizzo `pop.mail.ru` e con la porta 110 è stata assegnata la *porta di SpIDer Mail* 7000, allora nelle impostazioni del client di posta è necessario indicare `localhost` come il server delle email in arrivo e 7000 come la porta.

6.5. Scansione antivirus delle postazioni



L'utente della postazione può eseguire la scansione antivirus da solo, utilizzando il componente **Dr.Web Scanner per Windows**. L'icona di avvio di questo componente viene messa sul desktop al momento dell'installazione del software antivirus. Lo **Scanner** può essere avviato e può funzionare anche se l'**Agent** non è operativo, anche in modalità provvisoria del SO Windows.

Tramite il Pannello di controllo è possibile:

- ◆ Visualizzare la lista di tutti i componenti antivirus in esecuzione al momento.
- ◆ Interrompere l'esecuzione di componenti antivirus per tipo.
- ◆ Avviare i task di scansione antivirus con la configurazione dei parametri di scansione.



6.5.1. Visualizzazione ed interruzione dell'esecuzione dei componenti

Per visualizzare una lista dei componenti avviati e per interromperne l'esecuzione:

1. Selezionare la voce **Rete antivirus** del 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. Nel [menu di gestione](#) che si è aperto selezionare la voce **Componenti in esecuzione**.

Si apre una lista di tutti i componenti attivi al momento, sia di quelli avviati tramite il **Pannello di controllo** manualmente dall'amministratore o secondo il calendario, che di quelli avviati dall'utente sulla postazione.

2. Se è necessario interrompere l'esecuzione di uno dei componenti, spuntare il flag di fronte a questo componente, dopo di che nella barra degli strumenti premere il pulsante **Interrompi**. Il componente viene arrestato e viene eliminato dalla lista dei componenti in esecuzione.



Quando viene utilizzata questa opzione, le scansioni in corso vengono interrotte, lo **Scanner** viene arrestato, il funzionamento dei monitor in esecuzione viene sospeso.

Attenzione! Non è possibile avviare i monitor **SpIDer Guard**, **SpIDer Mail** e **SpIDer Gate** dal **Pannello di controllo**.



6.5.2. Interruzione dell'esecuzione dei componenti per tipo



Quando viene utilizzata questa opzione, le scansioni in corso vengono interrotte, lo **Scanner** viene arrestato, il funzionamento dei monitor in esecuzione viene sospeso.

Attenzione! Non è possibile avviare i monitor **SpIDer Guard**, **SpIDer Mail** e **SpIDer Gate** dal **Pannello di controllo**.

Per interrompere l'esecuzione di tutti i componenti di un determinato tipo, avviati su postazioni:

1. Selezionare la voce **Rete antivirus** del menu principale del **Pannello di controllo**, nella finestra che si è aperta nella lista gerarchica selezionare il gruppo richiesto o singole postazioni.
 2. Nella barra degli strumenti del catalogo della rete antivirus premere **Gestione dei componenti**. Dalla lista a cascata selezionare la voce **Interrompi i componenti in esecuzione**.
 3. Nel pannello che si è aperto, spuntare i flag di fronte ai tipi di componenti da interrompere immediatamente:
 - ◆ **Interrompi Dr.Web Agent Scanner avviato secondo il calendario** - per fermare una scansione attiva tramite **Dr.Web Agent Scanner**, avviata secondo i task del calendario centralizzato.
 - ◆ **Interrompi Dr.Web Agent Scanner avviato dall'amministratore** - per fermare una scansione attiva tramite **Dr.Web Agent Scanner**, avviata manualmente dall'amministratore tramite il **Pannello di controllo**.
 - ◆ **Interrompi Scanner Dr.Web avviato dall'utente** - per fermare una scansione attiva tramite **Scanner Dr.Web**, avviata dall'utente su postazione.
 - ◆ **Interrompi SpIDer Guard, SpIDer Mail, SpIDer Gate, Office control, Firewall e Auto-protezione** - per sospendere il funzionamento dei componenti **SpIDer Guard**, **SpIDer Mail**, **SpIDer Gate**, **Firewall** e **Auto-protezione**.
- Per selezionare tutti i tipi di componenti da arrestare, spuntare il flag di fronte all'intestazione del pannello **Interruzione dei componenti in esecuzione**.
4. Premere il pulsante **Interrompi**.


6.5.3. Avvio della scansione della postazione


Per avviare la scansione antivirus delle postazioni:

1. Selezionare la voce **Rete antivirus** del menu principale del **Pannello di controllo**.
2. Nella finestra che si è aperta, nella lista gerarchica fare clic sul nome di una postazione o di un gruppo.
3. Nella barra degli strumenti premere sulla voce **Scansiona**. Nella lista che si è aperta nella barra degli strumenti selezionare una delle modalità di scansione:
 - Scanner Dr.Web. Scansione rapida**. In questa modalità vengono scansionati i seguenti oggetti:
 - ◆ memoria operativa,
 - ◆ settori di avvio di tutti i dischi,
 - ◆ oggetti in esecuzione automatica,
 - ◆ cartella radice del disco di avvio,
 - ◆ cartella radice del disco di installazione dell'SO Windows,
 - ◆ cartella di sistema dell'SO Windows,
 - ◆ cartella `Documenti`,



- ◆ cartella temporanea di sistema,
- ◆ cartella temporanea utente.

 **Scanner Dr.Web. Scansione completa.** In questa modalità viene eseguita la scansione completa di tutti i dischi rigidi e supporti rimovibili (inclusi i settori di avvio).

 **Scanner Dr.Web. Scansione personalizzata.** Questa modalità permette di scegliere qualsiasi directory o file per la successiva scansione, nonché di configurare le impostazioni avanzate di scansione.



L'avvio remoto dello **Scanner** è possibile soltanto se vengono selezionate le postazioni attive gestite da un sistema operativo che consente l'avvio dello **Scanner**: SO Windows, SO della famiglia UNIX e Mac OS X.

4. Dopo che è stata scelta una variante di scansione, si apre la finestra delle impostazioni dello **Scanner**. Se necessario, modificare le impostazioni di scansione (v. sezione [Configurazione dei parametri di Scanner](#)).
5. Premere il pulsante **Controlla per i virus** per avviare il processo di scansione sulle postazioni selezionate.



La scansione della postazione tramite **Dr.Web Agent Scanner** avviato su remoto viene eseguita in modalità silenziosa senza visualizzare gli avvisi all'utente della postazione.

6.5.4. Configurazione dello Scanner

Tramite il Pannello di controllo si possono configurare le seguenti impostazioni di scansione antivirus:

- ◆ Impostazioni di **Scanner Dr.Web**. Questo **Scanner** viene avviato dagli utenti su postazioni e non può essere avviato su remoto tramite il **Pannello di controllo**. Tuttavia, l'amministratore può modificarne le impostazioni in modo centralizzato che verranno trasmesse e salvate successivamente sulle postazioni.
- ◆ Impostazioni di **Dr.Web Agent Scanner**. Questo **Scanner** viene avviato su remoto tramite il **Pannello di controllo** ed esegue la scansione antivirus della postazione in un modo simile a **Scanner Dr.Web**. Le impostazioni di **Dr.Web Agent Scanner** sono impostazioni estese di **Scanner Dr.Web** e vengono configurate quando viene avviata la scansione antivirus delle postazioni.

Configurazione di Dr.Web Scanner

1. Selezionare la voce **Rete antivirus** del menu principale del **Pannello di controllo**.
2. Nella finestra che si è aperta, nella lista gerarchica fare clic sul nome di una postazione o di un gruppo.
3. Nel [menu di gestione](#) che si è aperto, nella sezione **Configurazione** nella sottosezione del sistema operativo richiesto, selezionare la voce **Scanner**. Si apre la finestra di configurazione di **Scanner**.
4. Impostare i parametri di scansione richiesti. I parametri di **Scanner Dr.Web** sono descritti nel **Manuale dell'utente** per il sistema operativo corrispondente.
5. Fare clic sul pulsante **Salva**. Le impostazioni verranno salvate nel **Pannello di controllo** e verranno trasferite sulle postazioni corrispondenti.

Configurazione di Dr.Web Agent Scanner

Le impostazioni di **Dr.Web Agent Scanner** vengono configurate quando viene avviata la scansione delle postazioni, come è descritto in p. [Avvio della scansione di postazioni](#).




La lista delle sezioni delle impostazioni di **Scanner** che saranno disponibili (+) o non disponibili (-) dipende dalla variante di avvio della scansione di postazioni ed è riportata nella tabella sotto.

Tabella 6–8. Lista delle sezioni delle impostazioni dello scanner a seconda della variante di avvio

Variante di avvio della scansione	Sezioni delle impostazioni			
	Generali	Azioni	Limitazioni	Esclusioni
 Dr.Web Scanner. Scansione personalizzata	+	+	+	+
 Dr.Web Scanner. Scansione rapida	-	+	+	-
 Dr.Web Scanner. Scansione completa	-	+	+	-


A seconda del sistema operativo della postazione su cui viene avviata la scansione remota, sarà disponibile solo quella parte delle impostazioni di **Scanner** che è supportata dal sistema operativo della postazione.








Le impostazioni che non sono supportate per la scansione delle postazioni UNIX e Mac OS X sono contrassegnate con .

6.5.4.1. Generali



Le impostazioni che non sono supportate per la scansione delle postazioni UNIX e Mac OS X sono contrassegnate con .

Nella sezione **Generali** si possono configurare le seguenti impostazioni della scansione antivirus:

- ◆ Spuntare il flag **Utilizza l'analisi euristica** affinché lo **Scanner** cerchi virus sconosciuti utilizzando l'analisi euristica. In questa modalità, sono possibili falsi positivi di **Scanner**.
- ◆ Spuntare il flag **Controlla settori di avvio** affinché lo **Scanner** scansioni i settori di avvio. Vengono scansionati sia i settori di avvio dei dischi logici, che i master boot record dei dischi fisici.
- ◆ Spuntare il flag **Controlla programmi avviati automaticamente** per scansionare programmi eseguiti automaticamente alla partenza del sistema operativo.
- ◆ Spuntare il flag **Segui collegamenti simbolici** affinché la scansione segua collegamenti simbolici.
- ◆ Spuntare il flag **Controlla programmi e moduli in esecuzione** per scansionare i processi in esecuzione nella memoria operativa.
- ◆ Spuntare il flag **Scansione alla ricerca di rootkit** per abilitare la ricerca dei programmi malevoli che nascondono la propria presenza nel sistema operativo.
- ◆ Spuntare il flag **Sospendi la scansione se computer passa all'alimentazione da batteria** per sospendere la scansione antivirus se il computer dell'utente passa all'alimentazione da batteria.
- ◆ La lista a cascata **Priorità di scansione** determina la priorità del processo di scansione relativamente alle risorse di elaborazione del sistema operativo.
- ◆ Spuntare il flag **Limita l'utilizzo delle risorse del computer** per limitare l'utilizzo delle risorse del computer da parte della scansione, e dalla lista a cascata selezionare il tasso massimo di utilizzo delle risorse da parte di **Scanner**. In assenza di altri processi attivi, le risorse del computer verranno utilizzate nel grado massimo.
- ◆ La lista a cascata **Azioni dopo la scansione** imposta l'esecuzione automatica di un'azione subito dopo la fine della scansione:
 - **non fare nulla** – dopo la fine della scansione non eseguire nessuna azione con il computer dell'utente.



- **spegni la postazione** – dopo la fine della scansione spegnere il computer dell'utente. Prima di spegnere il computer, lo **Scanner** applicherà le azioni impostate alle minacce rilevate.
 - **riavvia la postazione** – dopo la fine della scansione riavviare il computer dell'utente. Prima di riavviare il computer, lo **Scanner** applicherà le azioni impostate alle minacce rilevate.
 - **trasferire la postazione nella modalità standby.**
 - **trasferire la postazione nella modalità sleep.**
- ◆ Spuntare il flag **Disattivare rete durante la scansione** per scollegare il computer dalla rete locale e da Internet per il tempo della scansione.
 - ◆ Spuntare il flag **Controlla dischi fissi** per scansionare le unità dischi fissi (hard drive ecc.).
 - ◆ Spuntare il flag **Controlla oggetti nei dispositivi rimovibili** per scansionare tutte le unità dispositivi rimovibili, per esempio unità dischi magnetici (dischetti), dischi CD/DVD, dispositivi flash ecc.
 - ◆ Nel campo **Percorsi da scansionare** impostare una lista dei percorsi da scansionare (il metodo di impostazione è descritto sotto).
 - Per aggiungere una nuova riga alla lista, fare clic sul pulsante e nella riga che si è aperta inserire il percorso richiesto.
 - Per eliminare un elemento dalla lista, fare clic sul pulsante di fronte alla riga corrispondente.
- Se viene spuntato il flag **Percorsi da scansionare**, vengono scansionati soltanto i percorsi indicati. Se il flag è tolto, vengono scansionati tutti i dischi.

6.5.4.2. Azioni



Le impostazioni che non sono supportate per la scansione delle postazioni UNIX e Mac OS X sono contrassegnate con .

Nella sezione **Azioni** viene impostata la reazione dell'**Antivirus** al rilevamento di file infetti o sospetti, di programmi nocivi e di archivi infetti.



Dr.Web Agent Scanner applica automaticamente le azioni impostate per gli oggetti malevoli rilevati.

Sono previste le seguenti azioni da applicare agli oggetti malevoli rilevati:

- ◆ **Cura** – per ripristinare l'oggetto infetto allo stato precedente all'infezione. Se l'oggetto non può essere disinfettato o se il tentativo di disinfezione non è riuscito, viene applicata l'azione impostata per gli oggetti incurabili.

Quest'azione è disponibile solo per gli oggetti infettati da un virus conosciuto curabile, esclusi i trojan e i file infetti all'interno di oggetti complessi (archivi compressi, file di email o container di file).
- ◆ **Rimuovi** – per cancellare gli oggetti infetti.
- ◆ **Sposta in quarantena** – per mettere gli oggetti infetti nella cartella di **Quarantena** su postazione.
- ◆ **Informa** – per inviare nel **Pannello di controllo** un avviso del rilevamento di un virus (per la configurazione della modalità di avvisi v. p. [Configurazione avvisi](#)).
- ◆ **Ignora** – per saltare l'oggetto senza eseguire alcun'azione e senza avvisarne nelle statistiche della scansione.



Tabella6–9. Azioni di Scanner applicate a oggetti malevoli rilevati

Oggetto	Azione				
	Cura	Rimuovi	Sposta in quarantena	Informa	Ignora
Infetti	+/*	+	+		
Sospetti		+	+/*		+
Incurabili		+	+/*		
Container		+	+/*		
Archivi compressi		+	+/*		
File di email			+/*		+
Settori di avvio	+/*			+	
Adware		+	+/*		+
Dialer		+	+/*		+
Joke		+	+/*		+
Riskware		+	+/*		+
Hacktool		+	+/*		+

Leggenda

- | | |
|-----|---|
| + | azione consentita per questo tipo di oggetti |
| +/* | azione predefinita per questo tipo di oggetti |

Per impostare le azioni da applicare a oggetti malevoli rilevati, si utilizzano le seguenti impostazioni:

- ◆ La lista a cascata **Infetti** imposta la reazione di **Scanner** al rilevamento di un file infettato da un virus conosciuto.
- ◆ La lista a cascata **Sospetti** imposta la reazione di **Scanner** al rilevamento di un file presumibilmente infettato da un virus (tale file è stato rilevato tramite l'analisi euristica).



Se nella scansione è inclusa la cartella di installazione del SO, si consiglia di selezionare per i file sospetti la reazione **Informa**.

- ◆ La lista a cascata **Incurabili** imposta la reazione di **Scanner** al rilevamento di un file infettato da un virus conosciuto incurabile, nonché per i casi quando il tentativo di cura non è riuscito.
- ◆ La lista a cascata **Container infetti** imposta la reazione di **Scanner** al rilevamento di un file infettato o sospetto incluso in un container di file.
- ◆ La lista a cascata **Archivi infetti** imposta la reazione di **Scanner** al rilevamento di un file infettato o sospetto incluso in un archivio di file.
- ◆ La lista a cascata **File di email infetti** imposta la reazione di **Scanner** al rilevamento di un file infettato o sospetto nel formato di email.



Se un virus o un codice sospetto vengono rilevati dentro oggetti complessi (archivi compressi, file di email o container di file), le azioni da applicare alle minacce in tali oggetti vengono eseguite con l'intero oggetto e non soltanto con la parte infetta. Di default, in tutti questi casi è prevista l'azione "Informa".

- ◆ La lista a cascata **Settori di avvio infetti** imposta la reazione di **Scanner** al rilevamento di un virus o di un codice sospetto nell'area dei settori di avvio.
- ◆ Le seguenti liste a cascata impostano la reazione di **Scanner** al rilevamento dei corrispondenti tipi di malware:
 - **Adware;**



- **Dialer;**
- **Joke;**
- **Riskware;**
- **Hacktool.**



Se viene impostata l'azione **Ignora**, nessuna azione verrà eseguita: nessun avviso verrà spedito nel **Pannello di controllo** diversamente dal caso quando l'opzione **Informa** è attivata per il rilevamento dei virus.

Spuntare il flag **Riavvia il computer automaticamente** per riavviare il computer dell'utente automaticamente dopo la fine della scansione se durante la scansione sono stati rilevati gli oggetti infetti per cui, per completarne la cura, occorre il riavvio del sistema operativo. Se il flag è deselezionato, il computer dell'utente non verrà riavviato. Nelle statistiche della scansione della postazione, ricevute dal Pannello di controllo, viene segnalata la necessità di riavviare la postazione per completare la cura. Le informazioni sullo stato che richiede il riavvio vengono visualizzate nella tabella [Stati](#). Se necessario, l'amministratore può riavviare la postazione dal **Pannello di controllo** (v. sezione [Rete antivirus](#)).

Spuntare il flag **Mostra il progresso della scansione** per visualizzare nel **Pannello di controllo** l'indicatore e la barra di stato del processo di scansione della postazione.

6.5.4.3. Limitazioni



Le impostazioni che non sono supportate per la scansione delle postazioni UNIX e Mac OS X sono contrassegnate con .

Nella sezione **Limitazioni** sono disponibili le seguenti configurazioni di scansione antivirus:

- ◆ **Tempo massimo di scansione (ms)** – tempo massimo in millisecondi di scansione di un oggetto. Dopo il tempo indicato, la scansione dell'oggetto viene terminata.
- ◆ **Livello di annidamento massimo di un archivio** – numero massimo di archivi nidificati. Se il livello di annidamento dell'archivio eccede il limite indicato, la scansione viene eseguita solo fino al livello di annidamento indicato.
- ◆ **Dimensione massima di un archivio (Kb)** – dimensione massima in kilobyte di un archivio da controllare. Se la dimensione dell'archivio eccede il limite indicato, la decompressione e la scansione non vengono eseguite.
- ◆ **Grado massimo di compressione** – rapporto massimo di compressione di un archivio. Se lo **Scanner** determina che il rapporto di compressione dell'archivio eccede il limite indicato, la decompressione e la scansione non vengono eseguite.
- ◆ **Dimensione massima di un oggetto decompresso (Kb)** – dimensione massima in kilobyte di un file da decomprimere. Se lo **Scanner** determina che dopo la decompressione, la dimensione dei file dell'archivio eccede il limite indicato, la decompressione e la scansione non vengono eseguite.
- ◆ **Valore soglia per il controllo del grado di compressione (Kb)** – dimensione minima in kilobyte di un file all'interno dell'archivio, a partire dalla quale viene controllato il rapporto di compressione.



6.5.4.4. Esclusioni

Nella sezione **Esclusioni** viene impostata una lista delle cartelle e dei file da escludere dalla scansione antivirus.

Per modificare le liste dei percorsi e dei file da escludere:

1. Inserire il percorso del file o della cartella richiesta nella riga **Percorsi e file da escludere**.



2. Per aggiungere una nuova riga alla lista, fare clic sul pulsante  e nella riga che si è aperta inserire il percorso richiesto.
3. Per eliminare un elemento dalla lista, fare clic sul pulsante  di fronte alla riga corrispondente.

La lista degli oggetti esclusi può contenere elementi dei seguenti tipi:

1. Percorso diretto esplicito dell'oggetto da escludere. In questo caso:
 - ◆ Carattere \ o / – viene escluso dalla scansione tutto il disco su cui si trova la cartella di installazione del SO Windows,
 - ◆ Percorso che finisce con il carattere \ – questa cartella viene esclusa dalla scansione,
 - ◆ Percorso che non finisce con il carattere \ – viene esclusa dalla scansione qualsiasi sottocartella, il percorso della quale inizia con la riga indicata.

Per esempio: C:\Windows – non scansionare file della cartella C:\Windows e tutte le sottocartelle.

2. Le maschere di oggetti esclusi dalla scansione. Per impostare le maschere si possono utilizzare i caratteri ? e *.

Per esempio: C:\Windows**.dll – non scansionare tutti i file con l'estensione dll che si trovano in tutte le sottocartelle della cartella C:\Windows.

3. Espressione regolare. I percorsi si possono impostare con le espressioni regolari. Inoltre, qualsiasi file, il cui nome completo (con il percorso) corrisponde a un'espressione regolare, viene escluso dalla scansione.



Prima di avviare il processo di scansione antivirus, consultare le raccomandazioni sull'utilizzo dei programmi antivirus sui computer Windows Server 2003 e Windows XP. L'articolo che contiene le informazioni necessarie si trova all'indirizzo – <http://support.microsoft.com/kb/822158/ru>. Il materiale di questo articolo è progettato per aiutare ad ottimizzare le prestazioni del sistema.

La sintassi delle espressioni regolari utilizzate per trascrivere percorsi esclusi è la seguente:

`qr{espressione}flag`

Spesso come flag si utilizza il carattere `i`, questo flag significa "non prendere in considerazione differenza di maiuscole e minuscole".

Alcuni esempi di trascrizione in espressioni regolari dei percorsi e dei file da escludere sono riportati sotto:

- ◆ `qr{\\pagefile\.sys$}i` – non scansionare file di swap del SO Windows NT,
- ◆ `qr{\\notepad\.exe$}i` – non scansionare file `notepad.exe`,
- ◆ `qr{^C:}i` – non scansionare proprio niente sul disco C,
- ◆ `qr{^.:\\WINNT\\}i` – non scansionare niente nelle cartelle `WINNT` su tutti i dischi,
- ◆ `qr{(^C:)|(^.:\\WINNT\\)}i` – unione di due casi precedenti,
- ◆ `qr{^C:\\dir1\\dir2\\file\.ext$}i` – non scansionare il file `c:\dir1\dir2\file.ext`,
- ◆ `qr{^C:\\dir1\\dir2\\(.+\\)?file\.ext$}i` – non scansionare il file `file.ext` se si trova nella cartella `c:\dir1\dir2` e nelle sottocartelle,
- ◆ `qr{^C:\\dir1\\dir2\\}i` – non scansionare la cartella `c:\dir1\dir2` e le sottocartelle,
- ◆ `qr{dir\\[^\\]+}i` – non scansionare la sottocartella `dir` che si trova in qualsiasi cartella, ma scansionare le sottocartelle,
- ◆ `qr{dir\\}i` – non scansionare la sottocartella `dir` che si trova in qualsiasi cartella e le sottocartelle.

L'utilizzo delle espressioni regolari è descritto in breve nel documento **Allegati**, sezione [Allegato J. Utilizzo di espressioni regolari in Dr.Web Enterprise Security Suite](#).



Nella sottosezione **Controllare i contenuti dei seguenti file**, si può disattivare la scansione di oggetti compositi. Per farlo, togliere i seguenti flag:

- ◆ Il flag **Archivi** comanda allo **Scanner** di cercare virus nei file compressi in archivi di file.
- ◆ Il flag **File di email** comanda di scansionare caselle di email.
- ◆ Il flag **Pacchetti d'installazione** comanda allo **Scanner** di controllare pacchetti di installazione di programmi.

6.6. Visualizzazione delle statistiche della postazione

Tramite il menu di gestione della sezione **Rete antivirus** si possono visualizzare le seguenti informazioni:

- ◆ **Statistiche** - le statistiche del funzionamento di elementi antivirus su postazione, i dati dello stato di postazioni e di elementi antivirus, per visualizzare e salvare i report che includono le statistiche riepilogative o i riassunti di dati selezionati per tipo di tabella.
- ◆ **Grafici** - i grafici con le informazioni su infezioni rilevate su postazione.
- ◆ **Quarantena** - l'accesso su remoto ai contenuti della **Quarantena** su postazione.

6.6.1. Statistiche

Per visualizzare le tabelle:

1. Selezionare la voce **Rete antivirus** del 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 richiesta dalla scheda **Statistiche**.

La sezione di menu **Statistiche** contiene le seguenti voci:

- ◆ **Statistiche complessive** - per ottenere le statistiche riepilogative senza suddividerle per sessioni.
- ◆ **Dati complessivi** - per visualizzare e per salvare i report che contengono tutte le statistiche riepilogative o i riassunti di dati selezionati per tipo di tabella impostato. Non è disponibile nel menu se sono nascoste tutte le altre voci di menu nella sezione **Statistiche**.
- ◆ **Infezioni** - per visualizzare le informazioni sui virus rilevati (l'elenco degli oggetti infetti, il virus, le azioni eseguite dall'antivirus ecc.).
- ◆ **Errori** - per visualizzare una lista degli errori di scansione sulla postazione selezionata per un determinato periodo.
- ◆ **Statistiche di scansione** - per ricavare le statistiche di funzionamento degli elementi antivirus su postazione.
- ◆ **Avvio/Arresto** - per visualizzare una lista dei componenti che erano in esecuzione su postazione.
- ◆ **Virus** - per visualizzare le informazioni sui virus rilevati su postazione, raggruppati per tipo di virus.
- ◆ **Stato** - per visualizzare le informazioni su uno stato insolito delle postazioni che probabilmente richiede l'intervento.
- ◆ **Task** - per visualizzare una lista dei task assegnati alla postazione in un determinato periodo.
- ◆ **Prodotti** - per visualizzare le informazioni sui prodotti installati su postazioni selezionate. "Prodotti" in questo caso si riferisce ai prodotti del **repository** del **Server**.
- ◆ **Database dei virus** - per visualizzare le informazioni circa i database dei virus installati: nome del file di un concreto database dei virus; versione del database dei virus; numero di record nel database dei virus; data di creazione del database dei virus. Questa voce è disponibile solo se vengono selezionate postazioni.



- ◆ **Moduli** - per visualizzare le informazioni dettagliate su tutti i moduli dell'antivirus **Dr.Web**: descrizione del modulo; il suo nome di funzione; il file che determina un modulo separato del prodotto; la versione completa del modulo ecc. Questa voce è disponibile solo se vengono selezionate postazioni.
- ◆ **Tutte le installazioni di rete** - per visualizzare una lista delle installazioni del software **Agent** sulla postazione o su un gruppo di postazioni.
- ◆ **Tutte le disinstallazioni** - per visualizzare una lista delle postazioni da cui il software antivirus **Dr.Web** è stato rimosso.



Per visualizzare le voci nascoste della sezione **Statistiche** selezionare la voce del menu principale **Amministrazione**, nella finestra che si è aperta selezionare la voce del menu di gestione **Configurazione del Server Dr.Web**. Nella scheda **Statistiche** spuntare i flag corrispondenti (v. di seguito), dopodiché premere **Salva** e riavviare il **Server**.

Tabella 6-10. Corrispondenza delle voci della sezione Statistiche e dei flag della sezione Dati statistici

Voci della sezione Statistiche	Flag della sezione Dati statistici
Statistiche complessive	Statistiche della scansione
Infezioni	Infezioni
Errori	Errori di scansione
Statistiche della scansione	Statistiche della scansione
Avvio/Arresto	Informazioni su avvio/arresto dei componenti
Virus	Infezioni
Stato	Monitoraggio dello stato delle postazioni
Task	Log di esecuzione dei task sulla postazione
Database dei virus	Monitoraggio dello stato della postazione Monitoraggio dei database dei virus Log di esecuzione dei task sulla postazione
Moduli	Lista dei moduli delle postazioni
Tutte le installazioni di rete	Informazioni sulle installazioni dell'agent

Le finestre in cui vengono visualizzati i risultati del funzionamento di vari componenti e le statistiche riepilogative della postazione hanno l'interfaccia uguale e le azioni per l'ottenimento delle informazioni dettagliate che loro forniscono sono uguali.

Di seguito vengono riportati alcuni esempi della visualizzazione di statistiche riepilogative tramite il **Pannello di controllo**.



6.6.1.1. Dati riepilogativi

Per visualizzare i dati riepilogativi:

1. Selezionare nella lista gerarchica la postazione richiesta o il gruppo richiesto.
2. Nel [menu di gestione](#) nella sezione **Statistiche** selezionare la voce **Dati complessivi**.
3. Si apre la finestra che contiene i dati di tabella di report. Per includere nel report determinate statistiche, premere il pulsante **Dati complessivi** nella barra degli strumenti e selezionare i tipi richiesti dalla lista a cascata: **Statistiche della scansione, Infezioni, Task, Avvio/Arresto, Errori**. Le statistiche che vengono incluse in queste sezioni del report corrispondono alle statistiche contenute nei punti corrispondenti della sezione **Tabelle**. Per visualizzare il report con le tabelle selezionate, premere il pulsante **Aggiorna**.
4. Per visualizzare le informazioni per un determinato periodo, indicare un periodo relativamente al giorno odierno nella lista a cascata o impostare un intervallo di tempo nella barra degli strumenti. Per impostare un intervallo di tempo, inserire le date richieste o premere sulle icone del calendario accanto ai campi di date. Per visualizzare le informazioni, premere il pulsante **Aggiorna**.
5. Se occorre salvare il report in modo da stamparlo o da elaborarlo in seguito, premere uno dei pulsanti:



Registra le informazioni in file CSV,



Registra le informazioni in file HTML,



Registra le informazioni in file XML,



Registra le informazioni in file PDF.

6.6.1.2. Statistiche della scansione

Per ottenere le statistiche del funzionamento degli elementi antivirus su postazione:





1. Selezionare nella lista gerarchica la postazione richiesta o il gruppo richiesto.



Se è necessario visualizzare le statistiche per diverse postazioni o gruppi, si possono selezionare le postazioni richieste utilizzando i tasti SHIFT o CTRL.

2. Nel [menu di gestione](#) nella sezione **Statistiche** selezionare la voce **Statistiche di scansione**.
3. Si apre la finestra delle statistiche. Di default vengono visualizzate le statistiche per le ultime 24 ore.
4. Per visualizzare le informazioni per un determinato periodo, indicare un periodo relativamente al giorno odierno nella lista a cascata o impostare un intervallo di tempo nella barra degli strumenti. Per impostare un intervallo di tempo, inserire le date richieste o premere sulle icone del calendario accanto ai campi di date. Per visualizzare le informazioni, premere il pulsante **Aggiorna**. Nella finestra verranno caricate le tabelle con i dati statistici.
5. Nella sezione **Statistiche complessive** vengono riportati i dati riepilogativi:
 - ◆ se selezionate postazioni - per le postazioni selezionate;
 - ◆ se selezionati gruppi - per i gruppi selezionati. Se sono stati selezionati diversi gruppi, vengono visualizzati soltanto i gruppi che contengono postazioni;
 - ◆ se selezionate postazioni e gruppi contemporaneamente - separatamente per tutte le postazioni, comprese quelle che fanno parte dei gruppi non vuoti selezionati.
6. Per visualizzare le statistiche dettagliate del funzionamento di elementi antivirus concreti, premere sul nome di postazione nella tabella. Se sono stati selezionati dei gruppi, premere sul nome di gruppo nella tabella delle statistiche generali e quindi sul nome di postazione nella tabella visualizzata. Si apre una finestra (o una sezione della finestra attuale) contenente una tabella con i dati statistici dettagliati.



7. Dalla tabella con le statistiche del funzionamento di elementi antivirus della postazione o del gruppo, si può aprire la finestra di configurazione di un componente antivirus concreto. Per farlo, premere sul nome del relativo componente nella tabella delle statistiche.
8. Per ordinare i dati di una colonna della tabella, premere la freccia corrispondente (ordine decrescente o crescente) nell'intestazione della colonna corrispondente.
9. Se occorre salvare la tabella delle statistiche in modo da stamparla o da elaborarla in seguito, premere uno dei pulsanti:
 -  **Registra le informazioni in file CSV,**
 -  **Registra le informazioni in file HTML,**
 -  **Registra le informazioni in file XML,**
 -  **Registra le informazioni in file PDF.**
10. Per ottenere le statistiche riepilogative senza suddividerle per sessioni, premere la voce **Statistiche complessive** nel menu di gestione. Si apre una finestra con le statistiche complessive.
11. Per visualizzare le statistiche di eventi di virus nel formato dei diagrammi, nel [menu di gestione](#) selezionare la voce **Grafici**. Si apre la finestra di visualizzazione dei diagrammi statistici (per la descrizione dettagliata v. [sotto](#)).

6.6.1.3. Stato

Per visualizzare le informazioni circa lo stato delle postazioni:

1. Selezionare nella lista gerarchica la postazione richiesta o il gruppo richiesto.
2. Nel [menu di gestione](#) nella sezione **Statistiche** selezionare la voce **Stato**.
3. Le informazioni circa lo stato di postazioni vengono visualizzate nella finestra automaticamente in conformità ai parametri indicati nella barra degli strumenti.
4. Per limitare l'elenco dei messaggi di stato ai soli messaggi di una determinata gravità, selezionare il livello di gravità dalla lista a cascata **Gravità** nella barra degli strumenti. Di default, è selezionato il livello di gravità **Minima**, e dunque viene visualizzato l'intero elenco dei messaggi.
5. Nell'elenco vengono incluse anche le postazioni che non si sono connesse al **Server** per un determinato numero di giorni. Indicare questo numero nel campo di input a sinistra dell'elenco **Gravità**. Se questo valore viene superato, la situazione viene considerata critica, e queste informazioni vengono visualizzate nella finestra della sezione **Stato**.
6. Le informazioni di questa tabella possono essere visualizzate ed elaborate nel modo uguale a quello descritto sopra per la tabella delle statistiche della scansione.



Inoltre, si possono visualizzare i risultati del funzionamento e le statistiche di diverse postazioni. Per farlo, occorre selezionare queste postazioni nella lista gerarchica della rete.

6.6.2. Grafici

Grafici delle infezioni

Per visualizzare grafici generali con informazioni sulle infezioni rilevate:

1. Selezionare la voce **Rete antivirus** del 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. Nel [menu di gestione](#) che si è aperto nella sezione **Generali** selezionare la voce **Grafici**.
2. Si apre una finestra che contiene le seguenti informazioni grafici:



- ◆ **Top dieci virus diffusi** - viene riportata una lista di dieci virus che hanno infettato il più grande numero di file. Nel grafico vengono visualizzati i dati numerici sugli oggetti che sono stati infettati dai virus indicati.
 - ◆ **Attività di virus giornaliera** - il periodo di tempo impostato viene suddiviso in periodi di 24 ore. Nel grafico viene visualizzato il numero totale di virus trovati entro ogni 24 ore su tutti gli oggetti della rete selezionati (postazioni e gruppi). Il grafico viene visualizzato se è stato impostato un periodo di tempo più lungo di 24 ore.
 - ◆ **Classi di infezione** - vengono visualizzati i dati numerici sugli oggetti suddivisi a seconda della classificazione di infezioni.
 - ◆ **Per numero di postazioni infette nel gruppo** - vengono visualizzati i dati numerici sul numero di postazioni infette per ciascun gruppo in cui tali postazioni sono inclusi.
 - ◆ **Azioni eseguite** - vengono visualizzati i dati numerici sugli oggetti infetti su cui sono state eseguite le azioni previste dal software antivirus.
3. Per visualizzare le informazioni grafiche per un determinato periodo, selezionare un intervallo di tempo da una lista a cascata nella barra degli strumenti: report per un determinato giorno o mese. Oppure si può impostare un intervallo di tempo, per farlo, inserire le date richieste o premere sulle icone del calendario accanto ai campi di date. Per visualizzare le informazioni, premere il pulsante **Aggiorna**.

Grafici delle statistiche complessive

I dati grafici vengono riportati nella voce **Grafici** della sezione **Generali** ed in alcune voci della sezione **Statistiche** del menu di gestione.

A seconda di ciò qual oggetto (gruppo o postazione) è stato selezionato nella lista gerarchica, vengono visualizzati vari set di grafici. La tabella sottostante riporta una lista dei possibili grafici e le sezioni del menu di gestione in cui questi grafici vengono visualizzati, a seconda dell'oggetto selezionato nella lista gerarchica.

Tabella 6-11Corrispondenza dei grafici
agli elementi selezionati della lista gerarchica e alle sezioni del menu di gestione

Grafici	Per i gruppi	Per postazioni	Sezioni
Top dieci virus diffusi	+	+	Infezioni Virus Grafici
Dieci computer più infetti	+		Infezioni
Tipi di infezione	+	+	Virus
Risultati delle installazioni			Tutte le installazioni di rete
Attività media dell'infezione	+		Statistiche della scansione
Per numero di errori	+	+	Errori
Errori per componente	+	+	Errori
Risultati dell'esecuzione dei task	+	+	Task
Classi di infezione	+	+	Grafici
Azioni eseguite	+	+	Grafici
Attività di virus giornaliera	+	+	Grafici
Per numero di postazioni infette nel gruppo	+		Grafici

- ◆ **Dieci computer più infetti** - viene riportata una lista di dieci postazioni infettate dal maggior numero di oggetti malevoli. Nel grafico vengono visualizzati i dati numerici sugli oggetti malevoli trovati sulle postazioni indicate.



- ◆ **Tipi di infezione** - un diagramma circolare che visualizza il numero di oggetti malevoli trovati per tipo di oggetto malevolo.
- ◆ **Risultati delle installazioni** - un diagramma circolare che visualizza il numero totale di installazioni avviate da questo **Server**, suddivise per il risultato di installazione. In caso di un'installazione non riuscita, viene specificata la causa dell'errore. Il diagramma visualizza tutte le installazioni avviate da questo **Server** a prescindere dall'oggetto selezionato nella lista gerarchica.
- ◆ **Attività media dell'infezione** - visualizza il valore medio di infezione sulle postazioni del gruppo selezionato. Questo valore viene calcolato come la somma del numero totale di oggetti malevoli trovati divisa per il numero di oggetti scansionati su ciascuna postazione.
- ◆ **Per numero di errori** - viene riportata una lista delle postazioni su cui sono stati rilevati errori nel funzionamento dei componenti antivirus installati su queste postazioni. Nel grafico viene visualizzato il numero di errori per postazione.
- ◆ **Errori per componente** - viene riportata una lista dei componenti antivirus installati su postazioni, nel funzionamento dei quali si verificavano degli errori. Nel diagramma circolare viene visualizzato il numero totale di errori di ciascuno dei componenti.
- ◆ **Risultati dell'esecuzione dei task** - viene riportata una lista dei task avviati sugli oggetti selezionati. Nel grafico viene visualizzato il numero di avvii di ciascuno dei task. Inoltre, una tabella che si trova sotto il grafico riporta i risultati dell'esecuzione dei task.

6.6.3. Quarantena

Contenuti di Quarantena

I file possono essere aggiunti a **Quarantena**:

- ◆ da uno dei componenti antivirus, per esempio dallo **Scanner**,
- ◆ manualmente dall'utente tramite la gestione di **Quarantena**.

Quando i file vengono messi in **Quarantena**, essi vengono scansionati nuovamente in automatico. In particolare:

- ◆ viene precisato lo stato dell'infezione - la presenza dell'infezione e il suo tipo (siccome quando i file vengono messi in **Quarantena** manualmente, le informazioni sullo stato di infezione di file non sono disponibili),
- ◆ vengono uniformati i nomi delle infezioni e i loro tipo.

Inoltre, l'utente può da solo scansionare nuovamente i file che si trovano in **Quarantena**, utilizzando il **Pannello di controllo** o la gestione di **Quarantena** su postazione.

Per visualizzare e per modificare i contenuti di Quarantena nel Pannello di controllo:

1. Selezionare la voce **Rete antivirus** del 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. Nel **menu di gestione** nella sezione **Generali** selezionare la voce **Quarantena**.
2. Si apre una finestra che contiene i dati tabulari sullo stato corrente di **Quarantena**.

Se è stata selezionata una postazione, viene visualizzata una tabella con gli oggetti che si trovano in **Quarantena** su questa postazione.

Se sono state selezionate diverse postazioni o un gruppo o diversi gruppi, viene visualizzato un set di tabelle che elencano oggetti in quarantena su ciascuna postazione separatamente.

3. Per visualizzare i file che sono stati messi in **Quarantena** in un determinato periodo di tempo, specificare il periodo richiesto nella barra degli strumenti e premere il pulsante **Aggiorna**.
4. Per gestire i file in **Quarantena**, spuntare il flag che corrisponde a un file, a un gruppo di file o a tutti i file in **Quarantena** (nell'intestazione della tabella). Nella barra degli strumenti selezionare una delle seguenti azioni:








- ◆  **Recupera files** - per ripristinare i file da **Quarantena**.



Utilizzare questa funzione soltanto se si è sicuri che l'oggetto è innocuo.

Dal menu a cascata selezionare una delle opzioni:

- a)  **Recupera files** - per far tornare il file alla sua posizione originale sul computer (ripristinare il file nella cartella dove era prima dello spostamento in **Quarantena**).
 - b)  **Recupera files al percorso indicato** - per trasferire il file nella cartella indicata dall'amministratore.
- ◆  **Rimuovere files** - per rimuovere i file selezionati da **Quarantena** e dal sistema.
 - ◆  **Scansiona files** - per eseguire un'altra scansione dei file selezionati in **Quarantena**.
 - ◆  **Esportazione** - per copiare e per salvare i file selezionati in **Quarantena**.

Dopo che i file sospetti sono stati messi nella **Quarantena** locale sul computer dell'utente, si possono copiare questi file tramite il **Pannello di controllo** e salvarli tramite il browser web, per esempio per il fine di mandarli successivamente per analisi al laboratorio antivirus **Doctor Web**. Per il salvataggio, spuntare i flag di fronte ai file richiesti e premere il pulsante **Esportazione**.

- ◆ Esportare i dati sullo stato di **Quarantena** in un file in uno dei seguenti formati:



Registra le informazioni in file CSV,



Registra le informazioni in file HTML,



Registra le informazioni in file XML,



Registra le informazioni in file PDF.

6.7. Invio dei file d'installazione

Quando viene creato un nuovo account di postazione nel **Pannello di controllo** viene generato un pacchetto d'installazione di **Agent Dr.Web**. Il pacchetto d'installazione 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** (il pacchetto d'installazione e il processo di installazione di **Agent** attraverso di esso vengono descritti nella **Guida all'installazione**, nella sezione **Installazione locale di Agent Dr.Web**).

Dopo aver creato pacchetti d'installazione, per renderne più conveniente la distribuzione, si possono inviare concreti pacchetti d'installazione via email sugli indirizzi degli utenti.

Quando i pacchetti d'installazione vengono inviati via email, i contenuti dell'email vengono formati nel seguente modo:

1. Il sistema operativo della postazione è conosciuto:
 - a) SO Windows: all'email viene allegato il pacchetto d'installazione di **Agent Dr.Web per Windows**.
 - b) SO Linux, SO Mac X, SO Android: all'email viene allegato il file d'installazione di **Agent Dr.Web** per il rispettivo sistema operativo e il file di configurazione con le impostazioni per la connessione al **Server Dr.Web**.
2. Il sistema operativo della postazione non è conosciuto (nuovo account di postazione, l'**Agent** non è ancora installato):



- a) Se sul **Server** non vi sono pacchetti per le postazioni SO Linux, SO Mac X, SO Android (in particolare, sul **Server** non è installato il pacchetto supplementare (extra)): all'email viene allegato il pacchetto d'installazione di **Agent Dr.Web per Windows** e il file di configurazione con le impostazioni per la connessione al **Server Dr.Web** per le postazioni SO Linux, SO Mac X, SO Android.
- b) Se sul **Server** vi è almeno un pacchetto oltre al pacchetto per le postazioni SO Windows: all'email viene allegato il pacchetto d'installazione di **Agent Dr.Web per Windows**, il file di configurazione con le impostazioni per la connessione al **Server Dr.Web** per le postazioni SO Linux, SO Mac X, SO Android, nonché un link al download dei file d'installazione per le postazioni SO Linux, SO Mac X, SO Android.

Per inviare pacchetti d'installazione via email:

1. Selezionare la voce **Rete antivirus** del menu principale del **Pannello di controllo**, nella finestra che si è aperta nella lista gerarchica selezionare i seguenti oggetti:
 - selezionare una postazione per inviare via email il pacchetto d'installazione generato per questa postazione.
 - selezionare un gruppo di postazioni per inviare via email i pacchetti d'installazione generati per le postazioni di questo gruppo.Per selezionare più oggetti alla volta, utilizzare i tasti CTRL o SHIFT.
2. Nella barra degli strumenti premere **★ Generali** → **Invia i file di installazione**.
3. Nella sezione **Invio dei file di installazione** che si è aperta, impostare i seguenti parametri:
 - Nella sezione **E-mail dei destinatari** impostare l'indirizzo email su cui verrà inviato il pacchetto d'installazione. Se si sono selezionate diverse postazioni o gruppi, impostare il rispettivo indirizzo email per l'invio di pacchetto d'installazione per ciascuna postazione separatamente di fronte al nome di questa postazione.
 - Nella sezione **Avanzate** spuntare il flag **Comprimi in archivio zip** per comprimere i file di pacchetti d'installazione in un archivio zip. La compressione in archivio può essere utile se sul lato utente vi sono dei filtri di email che bloccano la trasmissione di file eseguibili in allegati a messaggi email.
 - Nella sezione **Mittente** indicare l'indirizzo email che verrà indicato come il mittente dell'email con i file d'installazione.
 - Nella sezione **Impostazioni del server SMTP** si impostano i parametri del server SMTP che verrà utilizzato per l'invio delle email. Se i parametri sono conosciuti, per esempio sono già stati impostati in precedenza, questa sezione è ridotta e si può espanderla e si possono modificare i parametri impostati, se necessario. Quando i pacchetti d'installazione vengono inviati per la prima volta, nella sezione che si è aperta, è necessario impostare i seguenti parametri:
 - **Indirizzo** – indirizzo del server SMTP che verrà utilizzato per l'invio delle email.
 - **Porta** – porta del server SMTP che verrà utilizzato per l'invio delle email.
 - **Utente, Password** – se necessario, impostare il nome utente e la password dell'utente del server SMTP se il server SMTP richiede l'autenticazione.
 - Spuntare il flag **Crittografia STARTTLS** per utilizzare la crittografia *STARTTLS* per cifrare il traffico quando vengono inviate le email.
 - Spuntare il flag **Crittografia SSL** per utilizzare la crittografia *SSL* per cifrare il traffico quando vengono inviate le email.
 - Spuntare il flag **Utilizza l'autenticazione CRAM-MD5** per utilizzare *l'autenticazione CRAM-MD5* sul mail server.
 - Spuntare il flag **Utilizza l'autenticazione DIGEST-MD5** per utilizzare *l'autenticazione DIGEST-MD5* sul mail server.
 - Spuntare il flag **Utilizza l'autenticazione Plain** per utilizzare *l'autenticazione plain text* sul mail server.
 - Spuntare il flag **Utilizza l'autenticazione LOGIN** per utilizzare *l'autenticazione LOGIN* sul mail server.



- Spuntare il flag **Verifica se il certificato SSL del server è corretto** per controllare la correttezza del certificato SSL del mail server.
- Spuntare il flag **Modalità debug** per ottenere un log dettagliato di sessione SMTP. Premere il pulsante **Invia**.

6.8. Invio di messaggi alle postazioni SO Windows®

L'amministratore di sistema può inviare agli utenti i messaggi informativi di qualsiasi contenuto, che includono:

- ◆ testo del messaggio;
- ◆ link alle risorse Internet;
- ◆ logotipo della società (o qualsiasi immagine grafica);
- ◆ nella testata della finestra inoltre viene indicata la data precisa di ricezione del messaggio.

Tali messaggi vengono visualizzati sul lato utente come finestre pop-up (v. [immagine 6-1](#)).

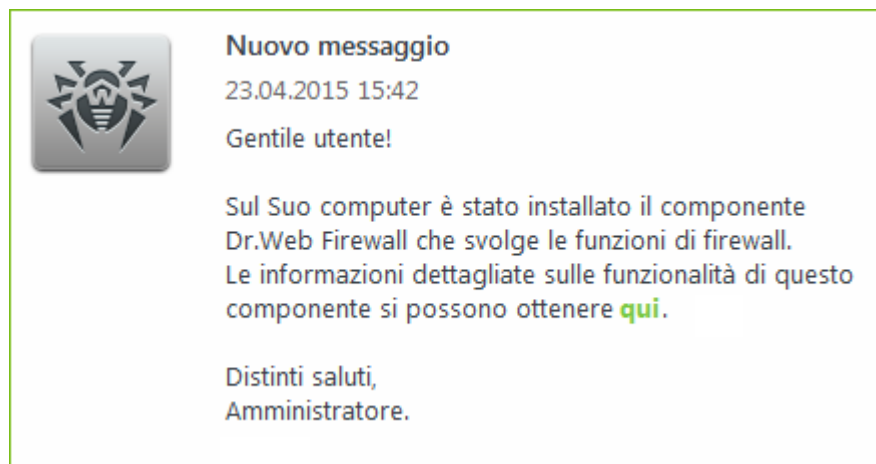



Immagine 6-1. Una finestra di messaggio sul lato utente

Per inviare un messaggio all'utente:

1. Selezionare la voce **Rete antivirus** del menu principale del **Pannello di controllo**.
2. Nella finestra che si è aperta nella lista gerarchica selezionare una postazione o un gruppo e nella barra degli strumenti premere **★ Generali** → **Invia il messaggio alle postazioni**.
3. Nella finestra che si è aperta, riempire i seguenti campi:
 - ◆ **Testo del messaggio** - campo obbligatorio. Contiene il messaggio stesso.
 - ◆ Spuntare il flag **Visualizza il logo nel messaggio** per visualizzare un oggetto grafico nella barra del titolo del messaggio. Impostare i seguenti parametri del logotipo:
 - Spuntare il flag **Utilizza trasparenza** per utilizzare la trasparenza nell'immagine del logo (v. [Formato del file di logo](#), p. 4).
 - Nel campo **URL** si può indicare il link alla pagina web che si apre quando si preme sul logo e sulla testata della finestra.
 - Nel campo **Intestazione del messaggio** si può inserire un'intestazione del messaggio, per esempio il nome della società. Tale testo verrà visualizzato nella testata della finestra del messaggio a destra del logo. Se questo campo rimane vuoto, invece dell'intestazione nella finestra di messaggio verranno visualizzate le informazioni sul messaggio.
 - A destra del campo **File del logo** premere il pulsante  per caricare il file di logo da risorsa locale e selezionare l'oggetto richiesto nel visualizzatore di file system (v. [Formato del file di logo](#)).



Se il logotipo non è impostato, o la dimensione del logotipo supera la dimensione massima ammissibile (v. [Formato del file di logo](#), p. 3), invece di esso nella finestra di messaggio verrà visualizzata l'icona di **Agent Dr.Web**.

- ◆ Spuntare il flag **Mostra link nel messaggio** per includere nel messaggio un link a risorse web.

Per aggiungere un link:

1. Nel campo **URL** impostare un link ad una risorsa Internet.
 2. Nel campo **Testo** indicare il nome del link - testo che verrà visualizzato invece del link nel messaggio.
 3. Nel campo **Testo del messaggio** aggiungere il marcatore `{link}` ovunque è necessario aggiungere il link. Nel messaggio risultante, invece di esso viene inserito il link con i parametri indicati. Il numero di tag `{link}` nel testo non è limitato, però ogni tag ha gli stessi parametri dai campi **URL** e **Testo**.
- ◆ Spuntare il flag **Invia soltanto alle postazioni online** per inviare il messaggio soltanto alle postazioni online. Se il flag è spuntato, il messaggio non verrà inviato alle postazioni offline. Se il flag è tolto, l'invio del messaggio alle postazioni offline verrà rinviato fino al momento della loro connessione.
 - ◆ Spuntare il flag **Mostra lo stato dell'invio** per visualizzare un avviso con lo stato dell'invio del messaggio.
4. Premere il pulsante **Invia**.

Formato del file di logo

Il file con un'immagine grafica (logotipo), che viene incluso nel messaggio, deve soddisfare le seguenti condizioni:

1. Formato di file grafico: BMP, JPG, PNG, GIF, SVG.
2. La dimensione del file di logo non deve eccedere 512 KB.
3. Le dimensioni dell'immagine sono 72x72 pixel. Le immagini di altre dimensioni verranno ridimensionate per l'invio fino alla dimensione predefinita.
4. La profondità di colore (bit depth) è qualsiasi (8 - 24 bit).



Se si vuole utilizzare nel messaggio un logo con lo sfondo trasparente, utilizzare i file nel formato PNG o GIF.

Prima di inviare il messaggio all'utente (soprattutto su molteplici indirizzi), si consiglia di inviarlo preliminarmente a qualsiasi computer con l'**Agent** installato per controllare la correttezza del risultato.

Esempio dell'invio del messaggio

Per avviare il messaggio riportato nell'immagine [6-0](#) sono stati impostati i seguenti parametri:

Testo del messaggio:

```
Gentile utente!
```

```
Sul Suo computer è stato installato il componente Dr.Web Firewall che svolge le funzioni di firewall.
```

```
Le informazioni dettagliate sulle funzionalità di questo componente si possono ottenere {link}.
```

```
Distinti saluti,  
Amministratore.
```



URL: <http://drweb.com/>

Testo: qui



Capitolo 7: Configurazione del Server Dr.Web

In questo capitolo vengono descritte le seguenti funzioni che permettono di gestire parametri di funzionamento della rete antivirus e del **Server Dr.Web**:

- ◆ [Logging](#) - per visualizzare e gestire i log di funzionamento del **Server**, per visualizzare le informazioni statistiche dettagliate sul funzionamento del **Server**;
- ◆ [Configurazione del Server Dr.Web](#) - per configurare i parametri di funzionamento del **Server**;
- ◆ [Configurazione del calendario di Server Dr.Web](#) - per configurare un calendario dei task per la manutenzione del **Server**;
- ◆ [Configurazione del web server](#) - per configurare i parametri di funzionamento del **web server**;
- ◆ [Procedure personalizzate](#) - per attivare e configurare procedure personalizzate;
- ◆ [Configurazione degli avvisi](#) - per configurare il sistema di avviso che notifica l'amministratore su eventi della rete antivirus e fornisce diversi modi per consegnare i messaggi;
- ◆ [Gestione del repository di Server Dr.Web](#) - per configurare il repository per l'aggiornamento di tutti i componenti della rete antivirus da **SAM** e per la successiva distribuzione degli aggiornamenti su postazioni;
- ◆ [Gestione del database](#) - per mantenere il database del **Server**;
- ◆ [Caratteristiche di una rete con diversi Server Dr.Web](#) - per configurare una rete antivirus con diversi server e per configurare le reazioni interserver.

7.1. Log

7.1.1. Log di funzionamento di Server Dr.Web

Il **Server Dr.Web** registra in un log gli eventi relativi al suo funzionamento.



Il log di **Server** viene utilizzato per il debugging e per l'eliminazione di inconvenienti in caso di funzionamento non corretto dei componenti della rete antivirus.

Di default, il file di log si chiama `drwcsd.log` e si trova in:



- ◆ Nei SO **UNIX**:
 - in caso dei SO Linux e Solaris: `/var/opt/drwcs/log/drwcsd.log`;
 - in caso del SO FreeBSD: `/var/drwcs/log/drwcsd.log`.
- ◆ Nei SO **Windows**: nella sottocartella `var` della cartella di installazione del **Server**.

Il file ha il formato di testo semplice (v. il documento **Allegati**, sezione [Allegato K. Formato dei file di log](#)).

Per visualizzare il log di funzionamento di Server tramite il Pannello di controllo:

1. Selezionare la voce **Amministrazione** del menu principale del **Pannello di controllo**.
2. Nella finestra che si è aperta, selezionare la voce del menu di gestione **Log del Server Dr.Web**.
3. Si apre una finestra con l'elenco dei log di funzionamento del **Server**. Secondo le impostazioni della modalità di rotazione, viene utilizzato il seguente formato dei nomi dei file di log di **Server**: `<file_name>.<N>.log` o `<file_name>.<N>.log.gz`, dove `<N>` - un numero progressivo: 1, 2, ecc. Per esempio, se il file ha il nome `drwcsd`, l'elenco dei file di log di funzionamento sarà il seguente:
 - `drwcsd.log` — file corrente (in cui le informazioni vengono registrate al momento),



- drwcsd.1.log.gz — file precedente,
 - drwcsd.2.log.gz e così via, più alto è il numero, più vecchia è la versione del file.
4. Per gestire i file di log, spuntare i flag accanto al file o diversi file richiesti. Per selezionare tutti i file di log, spuntare il flag nell'intestazione della tabella. Nella barra degli strumenti saranno disponibili i seguenti pulsanti:
-  **Esporta i file di log selezionati** - salvare una copia locale dei file di log selezionati. Si può usare il salvataggio di copia di log, per esempio per visualizzare i contenuti del file di log da un computer remoto.
-  **Rimuovi i file di log selezionati** - rimuovere i file di log selezionati senza la possibilità di recupero.






7.2. Configurazione del Server Dr.Web

Per configurare il Server Dr.Web:

1. Selezionare la voce **Amministrazione** del 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**. Si apre la finestra di configurazione di **Server**.



I valori dei campi marcati con il carattere * devono essere impostati obbligatoriamente.

3. Nella barra degli strumenti sono disponibili i seguenti pulsanti per gestire le impostazioni della sezione:
 -  **Riavvia Server Dr.Web** - per riavviare il **Server** al fine di accettare le modifiche apportate in questa sezione. Il pulsante diventa attivo dopo che si sono apportate delle modifiche nelle impostazioni della sezione e si è premuto il pulsante **Salva**.
 -  **Recupera la configurazione da copia di backup** - lista a cascata che include le copie salvate delle impostazioni dell'intera sezione a cui si può ritornare dopo aver apportato delle modifiche. Il pulsante diventa attivo dopo che si sono apportate delle modifiche nelle impostazioni della sezione e si è premuto il pulsante **Salva**.
 -  **Resetta tutti i parametri ai valori iniziali** - per ripristinare tutti i parametri di questa sezione ai valori che avevano prima della modifica corrente (ultimi valori salvati).
 -  **Resetta tutti i parametri ai valori default** - per ripristinare tutti i parametri di questa sezione ai valori di default.
4. Per accettare le modifiche apportate nelle impostazioni della sezione, premere il pulsante **Salva**, dopodiché sarà necessario riavviare il **Server**. Per farlo, premere il pulsante  **Riavvia Server Dr.Web** nella barra degli strumenti di questa sezione.



7.2.1. Generali

Nella scheda **Generali** vengono configurate le seguenti impostazioni del funzionamento di **Server**:

- ◆ Nel campo **Nome di Server Dr.Web** viene definito il nome di questo **Server**. Se il valore del campo non è impostato, viene utilizzato il nome del computer su cui è installato il **Server Dr.Web**.
- ◆ Nel campo **Numero di richieste parallele** viene impostato il numero di thread di elaborazione dei dati che arrivano dagli **Agent**. Questo parametro influisce sulle prestazioni del **Server**. Si consiglia di modificare il valore predefinito soltanto dopo l'approvazione da parte del servizio di supporto tecnico.
- ◆ Nel campo **Numero di connessioni al database** viene impostato il numero di connessioni di **Server** al database. Si consiglia di modificare il valore predefinito soltanto dopo l'approvazione da parte del servizio di supporto tecnico.



A partire dalla versione **10.0**, non viene più fornita la possibilità di modificare il parametro **Coda di autenticazione** attraverso il **Pannello di controllo**.

Di default, quando viene installato il nuovo **Server**, questo parametro viene impostato pari a 50. Se il server viene aggiornato da una versione precedente e viene mantenuto il file di configurazione, il valore di coda di autenticazione viene mantenuto dalla configurazione della versione precedente.

Se è necessario modificare il valore di coda di autenticazione, modificare il valore del seguente parametro nel file di configurazione del **Server**:

```
<!-- Maximun authorization queue length -->  
<maximum-authorization-queue size='50' />
```

- ◆ Spuntare il flag **Limita il volume del traffico dati degli aggiornamenti** per limitare il traffico dati di rete quando gli aggiornamenti vengono trasmessi tra il **Server** e gli **Agent**.

Se il flag è spuntato, inserire nel campo **Velocità di trasmissione massima (KB/s)** un valore della velocità massima di trasmissione degli aggiornamenti. Gli aggiornamenti verranno trasmessi entro la larghezza di banda impostata per il traffico dati cumulativo degli aggiornamenti di tutti gli **Agent**.

Se il flag è tolto, gli aggiornamenti vengono trasmessi agli **Agent** senza la limitazione della larghezza di banda.

Per maggiori informazioni v. p. [Limitazione del traffico dati delle postazioni](#).

- ◆ Nella lista a cascata **Modalità di registrazione dei nuovi arrivi** viene definito il criterio di ammissione delle nuove postazioni (v p. [Criteri di approvazione delle postazioni](#)).
 - La lista a cascata **Gruppo primario predefinito** definisce il gruppo primario in cui le postazioni verranno messe se l'accesso delle postazioni al **Server** viene approvato in maniera automatica.
- ◆ Spuntare il flag **Trasferisci le postazioni non autenticate in nuovi arrivi** per resettare per le postazioni non autenticate i parametri con cui possono ottenere l'accesso a **Server**. Questa opzione potrebbe essere utile in caso di modifica delle impostazioni del **Server** (quali, per esempio, la chiave di cifratura pubblica) o in caso di cambio del database. In tali casi le postazioni non potranno connettersi e dovranno ricevere le nuove impostazioni di accesso al **Server**.
- ◆ Dalla lista a cascata **Crittografia** viene selezionato il criterio di codifica dei dati trasmessi attraverso il canale di comunicazione tra il **Server Dr.Web** e i client connessi: **Agent**, **Server** adiacenti, **Installer di rete**.

Per maggiori informazioni su questi parametri v. p. [Utilizzo di cifratura e di compressione di traffico](#).

- ◆ Dalla lista a cascata **Compressione** viene selezionato il criterio di compressione dei dati trasmessi attraverso il canale di comunicazione tra il **Server Dr.Web** e i client connessi: **Agent**, **Server** adiacenti, **Installer di rete**. Per maggiori informazioni su questi parametri v. p. [Utilizzo di cifratura e di compressione di traffico](#).



- Se vengono selezionati i valori **Sì** e **Possibile** per la compressione del traffico dati, diventa disponibile la lista a cascata **Grado di compressione**. Da questa lista si può selezionare un grado di compressione dei dati da 1 a 9, dove 1 è il grado minimo e 9 è il grado massimo di compressione.
- ◆ Nel campo **Differenza ammissibile tra l'ora del Server e dell'Agent** viene definita la differenza ammissibile in minuti tra l'ora di sistema sul **Server Dr.Web** e sugli **Agent**. Se la differenza è maggiore del valore specificato, ciò verrà segnalato nello stato della postazione sul **Server Dr.Web**. Di default, è ammissibile la differenza di 3 minuti. Il valore 0 significa che il controllo non verrà eseguito.
- ◆ Spuntare il flag **Sostituisci gli indirizzi IP** per sostituire gli indirizzi IP con i nomi DNS dei computer nel file di log di **Server Dr.Web**.
- ◆ Spuntare il flag **Sostituisci i nomi NetBIOS** affinché nella directory rete antivirus del **Pannello di controllo** vengano visualizzati i nomi DNS delle postazioni invece dei nomi NetBIOS (se un nome a dominio non può essere determinato, viene visualizzato l'indirizzo IP).



Di default, entrambi i flag **Sostituisci gli indirizzi IP** e **Sostituisci i nomi NetBIOS** sono deselezionati. In caso di configurazione scorretta del servizio DNS, l'attivazione di queste possibilità potrebbe rallentare notevolmente il funzionamento del **Server**. Se viene attivata una di queste modalità, si consiglia di consentire la memorizzazione dei nomi nella cache su server DNS.



Se il flag **Sostituisci i nomi NetBIOS** è selezionato, e nella rete antivirus viene utilizzato un **Server proxy**, per tutte le postazioni connesse al **Server** attraverso il **Server proxy** nel **Pannello di controllo** come i nomi di postazioni verrà visualizzato il nome del computer su cui è installato il **Server proxy**.

- ◆ Spuntare il flag **Sincronizza le descrizioni delle postazioni** per sincronizzare la descrizione del computer dell'utente con la descrizione della rispettiva postazione nel **Pannello di controllo** (campo **Computer description** sulla pagina **System properties**). Se la descrizione della postazione non è disponibile nel **Pannello di controllo**, in questo campo verrà scritta la descrizione del computer disponibile sul lato utente. Se le descrizioni sono diverse, i dati nel **Pannello di controllo** verranno sostituiti con quelli dell'utente.
- ◆ Spuntare il flag **Tieni d'occhio epidemie** per attivare la modalità di avviso con cui l'amministratore viene notificato su casi di epidemie di virus. Se il flag è tolto, gli avvisi di infezioni di virus vengono spediti in modalità normale. Se il flag è spuntato, si possono inoltre impostare i seguenti parametri di monitoraggio di epidemie di virus:
 - **Periodo (s)** - il periodo in secondi in cui deve arrivare il numero impostato di avvisi di infezione affinché il **Server Dr.Web** mandi all'amministratore un singolo avviso di epidemia racchiudente tutti i casi di infezione.
 - **Numero di avvisi** - il numero di avvisi di infezione che deve arrivare nel periodo impostato affinché il **Server Dr.Web** mandi all'amministratore un singolo avviso di epidemia racchiudente tutti i casi di infezione.
- ◆ Spuntare il flag **Sincronizza la posizione geografica** per attivare la sincronizzazione della posizione geografica delle postazioni tra i **Server Dr.Web**. Se il flag è spuntato, si può inoltre impostare il seguente parametro:
 - **Sincronizzazione iniziale** - numero di postazioni senza coordinate geografiche di cui le informazioni vengono chieste quando viene stabilita una connessione tra i **Server Dr.Web**.

7.2.1.1. Utilizzo di cifratura e di compressione di traffico

La rete antivirus di **Dr.Web Enterprise Security Suite** permette di cifrare il traffico dei dati trasmessi tra il **Server** e le postazioni (**Agent Dr.Web**), tra i **Server Dr.Web** (se la configurazione della rete include diversi server), nonché tra il **Server** e gli **Installer di rete**. Questa modalità viene utilizzata per evitare l'eventuale divulgazione delle chiavi di utenti, nonché delle informazioni su hardware e utenti della rete antivirus nel corso della comunicazione dei componenti.



La rete antivirus **Dr.Web Enterprise Security Suite** utilizza i mezzi di firma digitale e di crittografia forte, basati sul concetto di coppie delle chiavi pubbliche e private.

Il criterio di utilizzo di cifratura viene impostato separatamente su ogni componente della rete antivirus, e le impostazioni di altri componenti devono corrispondere alle impostazioni del **Server**.

Visto che il traffico dei dati trasmessi 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 di criterio di compressione e la compatibilità di queste impostazioni su vari componenti sono uguali alle impostazioni di cifratura.



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 del traffico (per esempio, l'**Antivirus Dr.Web per Android** e l'**Antivirus Dr.Web per Mac OS X** non supportano né la cifratura né la compressione). Non sarà possibile connettere al **Server** tali client se è impostato il valore **Sì** per la cifratura e/o compressione sul lato **Server**.

Per impostare i criteri di compressione e di cifratura per il Server Dr.Web:

1. Selezionare la voce **Amministrazione** del 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 **Generali** selezionare dalle liste a cascata **Crittografia** e **Compressione** una delle varianti:
 - ◆ **Sì** — è obbligatoria la cifratura (o la compressione) del traffico dati scambiati con tutti i componenti (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 dei dati scambiati con i componenti, 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 vengono coordinate le impostazioni di criterio di cifratura e di compressione sul **Server** e su un altro componente (**Agent** o **Installer di rete**), si deve tenere presente che alcune combinazioni di impostazioni non sono ammissibili e la loro scelta porterà all'impossibilità di stabilire una connessione tra il **Server** e il componente.

Nella tabella 7-1 sono riportate le informazioni su ciò con quali impostazioni la connessione tra il **Server** e un componente è cifrata/compressa (+), con quali è non cifrata/non compressa (-), e quali combinazioni non sono ammissibili (**Errore**).

Tabella 7-1. Compatibilità delle impostazioni di criteri di cifratura e di compressione

Impostazioni del componente	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 minime ammissibili per i componenti installati. Se la cifratura di traffico dati non è richiesta per assicurare la sicurezza supplementare, si può rinunciare all'utilizzo di questa modalità. Inoltre, la cifratura di traffico dati non è consigliabile nelle reti grandi (più di 2000 client).



Per disattivare la modalità di cifratura, conviene prima cambiare consecutivamente il **Server** e i componenti nella modalità **Possibile**, non lasciando che vengano create coppie incompatibili **Installer di rete-Server** e **Agent-Server**. Se questa regola non viene osservata, ciò potrebbe portare alla perdita di controllo sul componente e alla necessità di reinstallarlo.

L'utilizzo della compressione diminuisce il traffico dati ma aumenta notevolmente il carico di elaborazione dei dati sui computer, più della cifratura.



Il valore **Possibile**, impostato sul lato **Agent Dr.Web**, significa che di default la cifratura/compressione viene eseguita ma può essere annullata con la modifica delle impostazioni di **Server Dr.Web** senza dover modificare le impostazioni sul lato **Agent**.

7.2.1.2. Limitazione del traffico dati delle postazioni

Nella rete antivirus di **Dr.Web Enterprise Security Suite** c'è la possibilità di limitare la velocità di trasmissione di dati tra il **Server** e gli **Agent**. Le impostazioni sono divise in limitazioni di trasmissione di aggiornamenti e in limitazioni di trasmissione di dati durante le installazioni di **Agent**.

Sono possibili le seguenti varianti di limitazione del traffico:

1. Limitazione della velocità generale di trasmissione di dati su tutte le postazioni.

L'impostazione viene configurata nella sezione di configurazione di **Server**: voce **Amministrazione** del menu principale del **Pannello di controllo** → voce del menu di gestione **Configurazione del Server Dr.Web** → scheda **Traffico** → scheda interna **Aggiornamenti** o **Installazioni** → parametro **Limita traffico**.

2. Limitazione individuale della velocità di trasmissione di dati su concrete postazioni o gruppi di postazioni.

L'impostazione viene configurata nella sezione di configurazione di postazioni: voce **Rete antivirus** del menu principale del **Pannello di controllo** → selezionare una postazione o un gruppo nella lista gerarchica della rete → voce del menu di gestione **Limitazioni di traffico** → scheda interna **Aggiornamenti** o **Installazioni** → parametro **Limita traffico**.

Il traffico dati viene limitato secondo il seguente principio:

1. Se è attivata la limitazione della velocità generale di trasmissione di dati nelle impostazioni del **Server**, la velocità totale di trasmissione di dati dal **Server** su tutte le postazioni non eccede il valore indicato. In particolare:
 - a) A prescindere da differenze nelle capacità di canale tra il **Server** e le postazioni, la velocità di trasmissione di dati viene suddivisa equamente tra tutte le postazioni.
 - b) Se la capacità di canale tra il **Server** e una postazione è inferiore al valore di velocità media per una postazione secondo il punto **a)**, per tale postazione viene impostata la limitazione di trasmissione di dati pari alla larghezza di banda massima fino a questa postazione. Il valore residuo di limitazione, ugualmente al punto **a)**, viene suddiviso equamente tra le altre postazioni.
2. Se è attivata la limitazione individuale della velocità di trasmissione di dati nelle impostazioni di un gruppo o di una concreta postazione, la velocità di trasmissione di dati a questi gruppi o postazione non eccede il valore indicato. La limitazione non si applica a nessun'altra postazione, e i dati vengono trasmessi con la velocità massima.
3. Se sono attivate la limitazione della velocità generale di trasmissione di dati nelle impostazioni del **Server** e la limitazione individuale per un gruppo o una postazione:
 - a) La velocità di trasmissione di dati sui gruppi o sulle postazioni con la limitazione individuale non eccede il valore indicato nelle impostazioni di questi gruppi o postazioni.



- b) Per la trasmissione di dati sulle altre postazioni, la limitazione generale della velocità di trasmissione di dati meno la limitazione della postazione dal p. **a)** viene suddivisa equamente.
- c) Se la capacità di canale tra il **Server** e una postazione senza la limitazione individuale è inferiore al valore di velocità media per una postazione secondo il punto **b)**, per tale postazione viene impostata la limitazione di trasmissione di dati pari alla larghezza di banda massima fino a questa postazione. Il valore residuo di limitazione, ugualmente al punto **b)**, viene suddiviso equamente tra le altre postazioni senza la limitazione individuale.

7.2.2. DNS

Nella scheda **DNS** vengono impostati i parametri delle query inviate al server DNS:

- ◆ **Timeout per query DNS (secondi)** - timeout in secondi per la risoluzione delle query DNS dirette/inverse. Impostare 0 per non limitare il tempo di attesa della fine della risoluzione di una query DNS.
- ◆ **Numero di query DNS ripetute** - numero massimo di query DNS ripetute in caso di mancata risoluzione di una query DNS.
- ◆ Spuntare il flag **Imposta il tempo di conservazione delle risposte del server DNS** per impostare il tempo di conservazione di risposte del server DNS nella cache (TTL).
 - **Per le risposte positive (minuti)** - tempo in minuti per cui le risposte positive del server DNS si conservano nella memoria cache (TTL).
 - **Per le risposte negative (minuti)** - tempo in minuti per cui le risposte negative del server DNS si conservano nella memoria cache (TTL).
- ◆ **Server DNS** - lista dei server DNS che sostituisce la lista di sistema predefinita.
- ◆ **Domini DNS** - lista dei domini DNS che sostituisce la lista di sistema predefinita.

7.2.3. Statistiche

Nella scheda **Statistiche** vengono definite le informazioni statistiche che verranno registrate nel log e salvate nel database del **Server**.

Per registrare e aggiungere al database il rispettivo tipo d'informazione, spuntare i seguenti flag:

- ◆ **Stato della quarantena** - abilita il monitoraggio dello stato della **Quarantena** su postazioni e la registrazione delle informazioni nel database.
- ◆ **Elenco di hardware e software** - abilita il monitoraggio dell'elenco di hardware e software su postazioni e la registrazione delle informazioni nel database.
- ◆ **Elenco di moduli di postazioni** - abilita il monitoraggio della lista dei moduli di **Antivirus** installati su postazioni e la registrazione delle informazioni nel database.
- ◆ **Elenco di componenti installati** - abilita il monitoraggio della lista dei componenti di **Antivirus** (**Scanner, Monitor** ecc.) installati sulla postazione e la registrazione delle informazioni nel database.
- ◆ **Sessioni degli utenti di postazioni** - abilita il monitoraggio delle sessioni degli utenti di postazioni e la registrazione nel database dei nomi utente degli utenti entrati nel sistema da computer con **Agent** installato.
- ◆ **Avvio/arresto dei componenti** - abilita il monitoraggio delle informazioni su avvio e arresto dei componenti di **Antivirus** (**Scanner, Monitor** ecc.) su postazioni e la registrazione delle informazioni nel database.
- ◆ **Minacce alla sicurezza rilevate** - abilita il monitoraggio del rilevamento di infezioni su postazioni e la registrazione delle informazioni nel database.

Se il flag **Minacce alla sicurezza rilevate** è spuntato, è inoltre possibile configurare impostazioni aggiuntive delle statistiche su infezioni.



Per abilitare l'invio delle statistiche su infezioni rilevate alla società **Doctor Web**, spuntare il flag **Invia le statistiche a Doctor Web**. Diventano disponibili i seguenti campi:

- **Intervallo** - intervallo in minuti di invio delle statistiche;
- **Identificatore** - chiave MD5 (si trova nel file di configurazione del **Server**).

È obbligatorio soltanto il campo **Intervallo** di invio delle statistiche.

- ◆ **Errori di scansione** - abilita il monitoraggio del rilevamento di errori di scansione su postazioni e la registrazione delle informazioni nel database.
- ◆ **Statistiche di scansione** - abilita il monitoraggio dei risultati di scansione su postazioni e la registrazione delle informazioni nel database.
- ◆ **Installazioni degli Agent** - abilita il monitoraggio delle informazioni sulle installazioni di **Agent** su postazioni e la registrazione delle informazioni nel database.
- ◆ **Log di esecuzione di task su postazioni** - abilita il monitoraggio dei risultati dell'esecuzione di un task su postazioni e la registrazione delle informazioni nel database.
- ◆ **Stato delle postazioni** - abilita il monitoraggio dei cambiamenti di stato delle postazioni e la registrazione delle informazioni nel database.
 - **Stato dei database dei virus dei virus** - abilita il monitoraggio dello stato (componenti, modifiche) dei database dei virus su postazione e la registrazione delle informazioni nel database. Il flag è disponibile soltanto se è spuntato il flag **Stato delle postazioni**.

Per visualizzare le informazioni statistiche:

1. Selezionare la voce del menu principale **Rete antivirus**.
2. Nella lista gerarchica selezionare una postazione o un gruppo.
3. Aprire la sezione corrispondente del menu di gestione (v. tabella sotto).



La descrizione dettagliata delle informazioni statistiche è riportata nella sezione [Visualizzazione delle statistiche della postazione](#).

Nella tabella sottostante è riportata la corrispondenza dei flag della sezione **Statistiche** nelle impostazioni di **Server** e delle voci del menu di gestione sulla pagina **Rete antivirus**.

Se vengono deselezionati i flag nella scheda **Statistiche**, saranno nascoste le voci corrispondenti nel menu di gestione.

Tabella 7-2 Corrispondenza delle impostazioni del Server e delle voci del menu di gestione

Impostazioni del Server	Voci del menu
Stato della quarantena	Generali → Quarantena Configurazione → Windows → Agent Dr.Web → flag Consenti la gestione remota della quarantena
Elenco di hardware e software	Generali → Hardware e software Generali → Comparazione di hardware e di software
Elenco di moduli di postazioni	Statistiche → Moduli
Elenco di componenti installati	Generali → Componenti installati
Sessioni degli utenti di postazioni	Generali → Sessioni degli utenti
Avvio/arresto dei componenti	Statistiche → Avvio/Arresto
Minacce alla sicurezza rilevate	Statistiche → Infezioni



Impostazioni del Server	Voci del menu
	Statistiche → Virus
Errori di scansione	Statistiche → Errori
Statistiche della scansione	Statistiche → Statistiche di scansione Tabelle → Statistiche riassuntive
Installazioni degli Agent	Statistiche → Tutte le installazioni di rete
Log di esecuzione dei task sulla postazione	Statistiche → Task Statistiche → Database dei virus
Stato delle postazioni	Statistiche → Stato Statistiche → Database dei virus
Stato dei database dei virus	Statistiche → Database dei virus

7.2.4. Sicurezza

Nella scheda **Sicurezza** vengono impostate le limitazioni riguardanti gli indirizzi di rete da cui gli **Agent**, gli installer di rete e gli altri **Server Dr.Web** (adiacenti) possono accedere a questo **Server**.

Il log di verifica del **Server** viene gestito tramite i seguenti flag:

- ◆ **Verifica delle operazioni dell'amministratore** consente di registrare nel log di verifica le informazioni sulle operazioni eseguite dall'amministratore con il **Pannello di controllo** e di registrare il log nel database.
- ◆ **Verifica delle operazioni interne del server** consente di registrare nel log di verifica le informazioni sulle operazioni interne del **Server Dr.Web** e di registrare il log nel database.
- ◆ **Verifica delle operazioni Web API** consente di registrare nel log di verifica le informazioni sulle operazioni tramite XML API e di registrare il log nel database.



Si può visualizzare il log di verifica selezionando nel menu principale **Amministrazione** la voce **Log di verifica**.

Nella scheda **Sicurezza** sono incluse schede supplementari in cui vengono impostate le limitazioni per i tipi di connessione corrispondenti:

- ◆ **Agent** - lista delle limitazioni riguardanti gli indirizzi IP da cui gli **Agent Dr.Web** possono connettersi a questo **Server**.
- ◆ **Installer** - lista delle limitazioni riguardanti gli indirizzi IP da cui gli installer di **Agent Dr.Web** possono connettersi a questo **Server**.
- ◆ **Adiacenti** - lista delle limitazioni riguardanti gli indirizzi IP da cui i **Server Dr.Web** adiacenti possono connettersi a questo **Server**.
- ◆ **Servizio di scoperta** - lista delle limitazioni riguardanti gli indirizzi IP da cui le query di trasmissione vengono accettate dal servizio di scoperta del Server.



Per impostare la limitazione di accesso per qualche tipo di connessione:

1. Passare alla scheda corrispondente (**Agent**, **Installazioni**, **Adiacenti** o **Servizio di scoperta**).
2. Per consentire tutte le connessioni, togliere la spunta dal flag **Usa questa lista di controllo di accesso**.
3. Per impostare liste degli indirizzi consentiti o proibiti, spuntare il flag **Usa questa lista di controllo di accesso**.



4. Per consentire l'accesso da un determinato indirizzo TCP, includerlo nella lista **TCP: Consentito** o **TCPv6: Consentito**.
5. Per proibire qualche indirizzo TCP, includerlo nella lista **TCP: Negato** o **TCPv6: Negato**.

Per modificare una lista degli indirizzi:

1. Inserire l'indirizzo di rete nel campo corrispondente e premere il pulsante **Salva**.
2. Per aggiungere un nuovo campo di indirizzo, premere il pulsante  della sezione corrispondente.
3. Per eliminare un campo, premere il pulsante .

Indirizzo di rete viene definito come: `<indirizzo-IP>/ [<prefisso>]`.



Le liste per inserire gli indirizzi TCPv6 saranno visualizzate solo se sul computer è installata l'interfaccia IPv6.

Esempio di utilizzo del prefisso:

1. Il prefisso 24 sta per la maschera di rete: 255.255.255.0
Contiene 254 indirizzi
Gli indirizzi di host in queste reti sono del tipo: 195.136.12.*
2. Il prefisso 8 sta per la maschera di rete 255.0.0.0
Contiene fino a 16387064 indirizzi (256*256*256)
Gli indirizzi di host in queste reti sono del tipo: 125.*.*.*

Gli indirizzi non inclusi in nessuna lista vengono consentiti o proibiti a seconda della selezione del flag **Priorità di negazione**. Se il flag è selezionato, la lista **Negato** ha la precedenza rispetto alla lista **Consentito**. Gli indirizzi non inclusi in nessuna lista o inclusi in tutte e due vengono proibiti. Vengono consentiti soltanto gli indirizzi che sono inclusi nella lista **Consentito** e non sono inclusi nella lista **Negato**.

7.2.5. Cache

Nella scheda **Cache** vengono configurati i parametri della cancellazione della cache di server:

- ◆ **Periodicità di pulizia della cache** - periodicità della cancellazione completa della cache.
- ◆ **File in quarantena** - periodicità dell'eliminazione di file conservati in **Quarantena** sul lato **Server**.
- ◆ **Pacchetti di installazione** - periodicità dell'eliminazione di pacchetti di installazione individuali.
- ◆ **File del repository** - periodicità dell'eliminazione di file conservati nel repository.

Impostando valori numerici, prestare attenzione alle liste a cascata con le unità di misura di periodicità.

7.2.6. Database

Nella scheda **Database** viene selezionato il DBMS necessario per il funzionamento del **Server Dr.Web**.



Si può ottenere la struttura del database di **Server Dr.Web** sulla base dello script `sql_init.sql` locato nella sottocartella `etc` della cartella di installazione di **Server Dr.Web**.



1. Dalla lista a cascata Database selezionare il tipo di database:
 - ◆ **IntDB** – database incorporato SQLite2 (un componente di **Server Dr.Web**),
 - ◆ **ODBC** – per utilizzare un database esterno tramite la connessione ODBC,
 - ◆ **Oracle** – database esterno per le piattaforme ad eccezione di FreeBSD,



Se viene utilizzato il DBMS esterno **Oracle** tramite la connessione ODBC, è necessario installare l'ultima versione del driver ODBC, fornita insieme a questo DBMS. L'utilizzo del driver ODBC per Oracle, fornito da Microsoft, è fortemente sconsigliato.

- ◆ **PostgreSQL** – database esterno,
 - ◆ **SQLite3** – database incorporato (un componente di **Server Dr.Web**). È la variante consigliata se viene utilizzato il database incorporato.
2. Configurare le impostazioni necessarie di utilizzo del database:
 - ◆ Per i database incorporati, se necessario, inserire nel campo **Nome del filefile** il percorso completo del file di database ed impostare la dimensione della memoria cache e la modalità di registrazione dei dati.
 - ◆ I parametri per i database esterni sono descritti nel documento **Allegati**, nella sezione [Allegato B. Impostazioni necessarie per l'utilizzo di DBMS. Parametri dei driver per DBMS.](#)
 3. Per rendere effettive le impostazioni, fare clic su **Salva**.



Il pacchetto di **Server Dr.Web** contiene client incorporati dei DBMS supportati dunque:

- Se si programma di utilizzare i client del DBMS incorporati, forniti insieme a **Server Dr.Web**, durante l'installazione (l'aggiornamento) di **Server** nelle impostazioni dell'installer selezionare la voce **Installazione personalizzata** e nella finestra successiva controllare che l'installazione del relativo client del DBMS sia consentita nella sezione **Database support**.
- Se si programma di utilizzare database esterni attraverso la connessione ODBC, durante l'installazione (l'aggiornamento) di **Server**, nelle impostazioni dell'installer selezionare la voce **Installazione personalizzata** e nella finestra successiva annullare l'installazione del relativo client del DBMS nella sezione **Database support**.
Altrimenti, l'utilizzo del database attraverso ODBC non sarà possibile per conflitto delle librerie.

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

Di default, è impostato l'utilizzo del DBMS incorporato. La scelta di questa modalità impegna molte risorse di elaborazione di dati del **Server**. Se la rete antivirus è di una dimensione significativa, si consiglia di utilizzare un DBMS esterno. La procedura di cambio del tipo di DBMS viene descritta nel documento **Allegati**, nella sezione [Cambio del tipo di DBMS di Dr.Web Enterprise Security Suite](#).



Il database incorporato può essere utilizzato se al **Server** sono connesse non più di 200-300 postazioni. Se lo permettono la configurazione dell'hardware del computer su cui è installato il **Server Dr.Web** e il carico di altri processi eseguiti su questo computer, è possibile connettere fino a 1000 postazioni.

Altrimenti, si deve utilizzare un database esterno.

Se viene utilizzato un database esterno e se al **Server** sono connesse più di 10000 postazioni, sono consigliabili i seguenti requisiti minimi:

- ◆ processore con velocità 3GHz,
- ◆ memoria operativa a partire dai 4 GB per il **Server Dr.Web**, a partire dai 8 GB per il server del database,
- ◆ SO della famiglia UNIX.



È prevista la possibilità di eseguire le operazioni di pulizia del database utilizzato dal **Server Dr.Web**, in particolare: eliminazione dei record di eventi e delle informazioni su postazioni che non si sono connesse al **Server** per un determinato periodo. Per ripulire il database, passare alla sezione del [calendario del Server](#) e creare un task corrispondente.

7.2.7. Proxy

Nella scheda **Server proxy** vengono impostati i parametri del server proxy.

Spuntare il flag **Utilizza server proxy** per configurare le connessioni di **Server Dr.Web** attraverso il server proxy. In questo caso, diventano disponibili le seguenti impostazioni:

- ◆ **Server proxy** - indirizzo IP o nome DNS del server proxy.
- ◆ Per utilizzare l'autenticazione per l'accesso al server proxy secondo i metodi impostati, spuntare il flag **Utilizza autenticazione** e definire i seguenti parametri:
 - Compilare i campi **Utente del proxy** e **Password dell'utente del proxy**.
 - Selezionare uno dei metodi di autenticazione:

Opzione		Descrizione
Qualsiasi metodo da quelli supportati		Utilizzare qualsiasi metodo di autenticazione supportato dal proxy. Se il proxy supporta più metodi di autenticazione, verrà utilizzato il più affidabile.
Qualsiasi metodo sicuro da quelli supportati		Utilizzare qualsiasi metodo di autenticazione sicuro supportato dal proxy. In questa modalità l'autenticazione Basic non si usa. Se il proxy supporta più metodi di autenticazione, verrà utilizzato il più affidabile.
Metodi elencati sotto:	Autenticazione Basic	Utilizza l'autenticazione Basic. Non è consigliabile utilizzare questo metodo perché il trasferimento di credenziali di autenticazione non viene criptato.
	Autenticazione Digest	Utilizza l'autenticazione Digest. Metodo di autenticazione crittografica.
	Autenticazione NTLM	Utilizza l'autenticazione NTLM. Metodo di autenticazione crittografica. Per l'autenticazione viene utilizzato il protocollo NTLM di Microsoft.
	Autenticazione GSS-Negotiate	Utilizza l'autenticazione GSS-Negotiate. Metodo di autenticazione crittografica.

7.2.8. Trasporto

Nella scheda **Trasporto** si impostano i parametri dei protocolli di trasporto utilizzati dal **Server** per la comunicazione con i client.

Nella sottosezione TCP/IP vengono configurati i parametri delle connessioni con il **Server** attraverso i protocolli TCP/IP:

- ◆ Nei campi **Indirizzo** e **Porta** è necessario indicare rispettivamente l'indirizzo IP e il numero di porta dell'interfaccia di rete a cui viene associato questo protocollo di trasporto. L'interfaccia che ha le impostazioni indicate viene ascoltata dal **Server** per la comunicazione con gli **Agent** installati su postazioni.
- ◆ Nel campo **Nome** viene indicato il nome di **Server Dr.Web**. Se non è indicato, viene utilizzato il nome impostato nella scheda **Generali** (v. sopra, in particolare, se nella scheda non è impostato nessun nome, viene utilizzato il nome di computer). Se per il protocollo è impostato un nome diverso da quello definito nella scheda **Generali**, viene utilizzato il nome definito nella descrizione del protocollo. Questo nome viene utilizzato dal servizio di scoperta per la ricerca del **Server** da parte degli **Agent** ecc.
- ◆ Spuntare il flag **Scoperta** per abilitare il servizio di scoperta del **Server**.



- ◆ Spuntare il flag **Multicasting** per utilizzare la modalità *Multicast over UDP* per il rilevamento del **Server**.
- ◆ Nel campo **Gruppo Multicast** viene impostato l'indirizzo IP del gruppo multicast in cui è registrato il **Server**. Viene utilizzato per la comunicazione con gli **Agent** e gli **Installer di rete** durante la ricerca dei **Server Dr.Web** attivi nella rete. Se il valore di questo campo non è impostato, di default viene utilizzato il gruppo 231.0.0.1.
- ◆ Soltanto nei SO della famiglia UNIX: nel campo **Percorso** viene impostato il percorso del socket, per esempio per la connessione con **Agent**.



Per maggiori informazioni consultare la sezione [Configurazione delle connessioni di rete](#).

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

7.2.9. Moduli

Nella scheda **Moduli** viene configurata la modalità di interazione di **Server Dr.Web** con gli altri componenti di **Dr.Web Enterprise Security Suite**:

- ◆ Spuntare il flag **Estensione del Pannello di controllo della sicurezza Dr.Web** per poter utilizzare l'**Estensione del Pannello di controllo della sicurezza Dr.Web** per gestire il **Server** e la rete antivirus tramite il **Pannello di controllo**,



Se è tolto il flag **Estensione del Pannello di controllo della sicurezza Dr.Web**, dopo il riavvio del **Server Dr.Web** non sarà disponibile il **Pannello di controllo della sicurezza Dr.Web**. In questo caso il **Server** e la rete antivirus possono essere gestiti soltanto tramite l'utility di diagnostica remota, a condizione che sia spuntato il flag **Estensione Dr.Web Server FrontDoor**.

- ◆ Spuntare il flag **Estensione Dr.Web Server FrontDoor** per poter utilizzare l'estensione **Dr.Web Server FrontDoor** che abilita la connessione dell'utility di diagnostica remota di **Server** (v. inoltre p. [Accesso remoto al Server Dr.Web](#)).
- ◆ Spuntare il flag **Protocollo di Agent Dr.Web** per attivare il protocollo di interazione del **Server** con gli **Agent Dr.Web**.
- ◆ Spuntare il flag **Protocollo Microsoft NAP Health Validator** per attivare il protocollo di interazione di **Server** con il componente di verifica di integrità di sistema Microsoft **NAP Validator**.
- ◆ Spuntare il flag **Protocollo di installer di Agent Dr.Web** per attivare il protocollo di interazione del **Server** con gli installer di **Agent Dr.Web**.
- ◆ Spuntare il flag **Protocollo di cluster dei Server Dr.Web** per attivare il protocollo di interazione dei **Server** in un sistema a cluster.
- ◆ Spuntare il flag **Protocollo di Server Dr.Web** per attivare il protocollo di interazione del **Server Dr.Web** con gli altri **Server Dr.Web**. Di default, il protocollo è disattivato. Se viene configurata una rete con diversi server (v. p. [Caratteristiche di una rete con diversi Server Dr.Web](#)), attivare questo protocollo, spuntando il flag **Protocollo di Server Dr.Web**.

7.2.10. Cluster

Nella scheda **Cluster** vengono impostati i parametri di cluster dei **Server Dr.Web** per lo scambio delle informazioni in una configurazione di rete antivirus con diversi server (v. p. [Caratteristiche di una rete con diversi Server Dr.Web](#)).



Per utilizzare il cluster, impostare i seguenti parametri:

- ◆ **Gruppo multicast** - l'indirizzo IP del gruppo multicast attraverso il quale i **Server** si scambieranno le informazioni.
- ◆ **Porta** - il numero di porta dell'interfaccia di rete a cui viene associato il protocollo di trasporto per la trasmissione di informazioni nel gruppo multicast.
- ◆ **Interfaccia** - l'indirizzo IP dell'interfaccia di rete a cui è associato il protocollo di trasporto per la trasmissione delle informazioni nel gruppo multicast.

7.2.11. Posizione

Nella scheda **Posizione** si può indicare le informazioni supplementari circa la posizione fisica del computer su cui è installato il software **Server Dr.Web**.

Inoltre, in questa scheda si può visualizzare la posizione del **Server** su una mappa.

Per visualizzare la posizione della postazione del Server sulla mappa:

1. Nei campi **Latitudine** e **Longitudine** inserire le coordinate geografiche del **Server** nel formato gradi decimali (Decimal Degrees).
2. Premere il pulsante **Salva** per memorizzare i dati immessi nel file di configurazione del **Server**.
Non è necessario riavviare il **Server** per visualizzare la mappa. Tuttavia, sarà necessario riavviare il **Server** per applicare le coordinate geografiche modificate.
3. Nella scheda **Posizione** viene visualizzata l'anteprima della mappa OpenStreetMaps con un'etichetta corrispondente alle coordinate inserite.
Se l'anteprima non può essere caricata, viene visualizzato il testo **Mostra sulla mappa**.
4. Per visualizzare la mappa di grandezza piena, fare clic sull'anteprima o sul testo **Mostra sulla mappa**.

7.2.12. Download

Nella scheda **Download** vengono configurati i parametri del **Server** utilizzati nella generazione dei file di installazione di **Agent** per le postazioni della rete antivirus. In seguito, questi parametri vengono utilizzati quando l'installer di **Agent** si connette al **Server**:

- ◆ **In dirizzo di Server Dr.Web** - indirizzo IP o nome DNS del **Server Dr.Web**.
Se l'indirizzo di **Server** non è impostato, viene utilizzato il nome del computer restituito dal sistema operativo.
- ◆ **Porta** - numero di porta che verrà utilizzato per la connessione dell'installer di **Agent** al **Server**.
Se il numero di porta non è impostato, di default viene utilizzata la porta 2193 (viene configurata nel **Pannello di controllo** nella sezione **Amministrazione** → **Configurazione del del Server Dr.Web** → scheda **Trasporto**).

Le impostazioni della sezione **Download** vengono memorizzate nel file di configurazione `download.conf` (v. documento **Allegati**, p. [G3. File di configurazione download.conf](#)).



7.2.13. Aggiornamenti per gruppi

Nella scheda **Aggiornamenti per gruppi** viene configurata la trasmissione degli aggiornamenti per gruppi alle postazioni attraverso il protocollo multicast.

Per attivare la trasmissione degli aggiornamenti alle postazioni attraverso il protocollo multicast, spuntare il flag **Attiva gli aggiornamenti per gruppi**, in tale caso:

- ◆ Se gli aggiornamenti per gruppi sono disattivati, l'aggiornamento su tutte le postazioni viene eseguito soltanto nel modo regolare, cioè attraverso il protocollo TCP.
- ◆ Se gli aggiornamenti per gruppi sono attivati, su tutte le postazioni connesse a questo **Server** l'aggiornamento si svolgerà in due fasi:
 1. Aggiornamento attraverso il protocollo multicast.
 2. Aggiornamento standard attraverso il protocollo TCP.

Per configurare gli aggiornamenti per gruppi, utilizzare i seguenti parametri:

- ◆ **Dimensione del datagramma UDP (byte)** - dimensione in byte dei datagrammi UDP utilizzati dal protocollo multicast.

L'intervallo ammissibile è 512 - 8192. Per evitare frammentazione, si consiglia di impostare un valore inferiore all'MTU (Maximum Transmission Unit) della rete in uso.

- ◆ **Tempo di trasmissione del file (ms)** - nel periodo definito viene trasmesso un file di aggiornamento, dopo di che il **Server** inizia a trasmettere il file successivo.

Tutti i file che non sono stati trasmessi in fase dell'aggiornamento tramite il protocollo multicast verranno trasmessi durante l'aggiornamento standard tramite il protocollo TCP.

- ◆ **Durata degli aggiornamenti per gruppi (ms)** - durata del processo di aggiornamento attraverso il protocollo multicast.

Tutti i file che non sono stati trasmessi in fase dell'aggiornamento tramite il protocollo multicast verranno trasmessi durante l'aggiornamento standard tramite il protocollo TCP.

- ◆ **Intervallo di trasmissione pacchetti (ms)** - intervallo di trasmissione dei pacchetti a gruppo multicast.

Un valore piccolo di intervallo potrebbe causare notevoli perdite durante la trasmissione dei pacchetti e sovraccaricare la rete. La modificazione di questo parametro è sconsigliabile.

- ◆ **Intervallo tra le query di trasmissione ripetuta (ms)** - con questo intervallo gli **Agent** inviano le query chiedendo di ripetere la trasmissione dei pacchetti persi.

Il **Server Dr.Web** accumula queste query, dopodiché trasmette i blocchi persi.

- ◆ **Intervallo "di silenzio" su linea (ms)** - se la trasmissione di un file è finita prima della scadenza del tempo assegnato e se nel tempo "di silenzio" impostato nessuna query di trasmissione ripetuta di pacchetti persi è arrivata dagli **Agent**, il **Server Dr.Web** ritiene che tutti gli **Agent** abbiano ottenuto con successo i file di aggiornamento e inizia a trasmettere il file successivo.

- ◆ **Intervallo per accumulare query di trasmissione ripetuta (ms)** - durante questo intervallo il **Server** accumula le query degli **Agent** che chiedono di ripetere la trasmissione di pacchetti persi.

Gli **Agent** chiedono l'invio ripetuto dei pacchetti persi. Il **Server** accumula queste query entro il tempo specificato, dopo di che trasmette i blocchi persi.

Per configurare una lista dei gruppi multicast, attraverso i quali l'aggiornamento per gruppi sarà disponibile, impostare i seguenti parametri nella sottosezione **Gruppi multicast**:

- ◆ **Gruppo Multicast** - indirizzo IP del gruppo multicast attraverso il quale le postazioni riceveranno gli aggiornamenti per gruppi.




- ◆ **Porta** - numero di porta dell'interfaccia di rete del **Server Dr.Web** a cui viene legato il protocollo di trasporto multicast per la trasmissione degli aggiornamenti.



Per gli aggiornamenti per gruppi, è necessario impostare qualsiasi porta libera, in particolare, una che è diversa dalla porta assegnata nelle impostazioni al funzionamento del protocollo di trasporto del **Server** stesso.

- ◆ **Interfaccia** - indirizzo IP dell'interfaccia di rete del **Server Dr.Web** a cui viene legato il protocollo di trasporto multicast per la trasmissione degli aggiornamenti.

In ciascuna riga vengono configurate le impostazioni di un gruppo multicast. Per aggiungere un altro gruppo multicast, fare clic su .

Se vengono impostati diversi gruppi multicast, prestare attenzione alle seguenti caratteristiche:

- ◆ Per diversi **Server Dr.Web** che spediranno gli aggiornamenti per gruppi, devono essere impostati diversi gruppi multicast.
- ◆ Per diversi **Server Dr.Web** che spediranno gli aggiornamenti per gruppi, devono essere impostati diversi parametri **Interfaccia** e **Porta**.
- ◆ Se vengono impostati diversi gruppi multicast, i set delle postazioni che rientrano in questi gruppi non devono intersecarsi. Pertanto, ciascuna postazione della rete antivirus può far parte soltanto di un gruppo multicast.

7.2.14. Licenze

Nella scheda **Licenze** viene configurata la distribuzione di licenze tra i **Server Dr.Web**:

- ◆ **Periodo di validità delle licenze rilasciate** - periodo di tempo per cui vengono rilasciate le licenze dalla chiave su questo **Server**. L'impostazione viene utilizzata se questo **Server** rilascia licenze ai **Server** adiacenti.
- ◆ **Periodo per il rinnovo delle licenze ricevute** - periodo fino alla scadenza di una licenza, a partire da cui questo **Server** richiede il rinnovo della licenza ricevuta da un **Server** adiacente. L'impostazione viene utilizzata se questo **Server** riceve licenze dai **Server** adiacenti.
- ◆ **Periodo di sincronizzazione delle licenze** - periodicità di sincronizzazione delle informazioni su licenze rilasciate tra i **Server**.



Per maggiori informazioni su distribuzione di licenze tra i **Server**, consultare la sezione [Gestione licenze](#).

7.3. Accesso remoto al Server Dr.Web



Per connettere l'utility di diagnostica remota del **Server**, è necessario attivare **Dr.Web Server FrontDoor Plug-in**. Per farlo, nella sezione **Configurazione del Server Dr.Web**, nella scheda **Moduli** spuntare il flag **Estensione Dr.Web Server FrontDoor**.

Per connettere l'utility di diagnostica remota del **Server** è necessario che per l'amministratore che si connette attraverso l'utility sia consentito il permesso **Utilizzo delle funzioni aggiuntive**. Altrimenti, sarà negato l'accesso al **Server** attraverso l'utility di diagnostica remota.

Per configurare i parametri di connessione dell'utility di diagnostica remota del Server:

1. Selezionare la voce **Amministrazione** del menu principale del **Pannello di controllo**, nella finestra che si è aperta selezionare la voce del menu di gestione **Accesso remoto al Server Dr.Web**.



2. Configurare le seguenti impostazioni:
 - **Certificato SSL** - il file del certificato SSL che verrà controllato al momento di connessione. Nella lista a cascata sono elencati i certificati disponibili dalla directory di **Server**.
 - **Chiave privata SSL** - il file della chiave privata SSL che verrà controllata al momento di connessione. Nella lista a cascata sono elencate le chiavi private disponibili dalla directory di **Server**.
 - **Indirizzo** - l'indirizzo da cui è consentita la connessione dell'utility di diagnostica remota del **Server**.
 - **Porta** - la porta per la connessione dell'utility di diagnostica remota del **Server**. Di default, si usa la porta 10101.
3. Premere **Salva**.



L'utilizzo della versione console dell'utility di diagnostica remota di **Server** è descritto nel documento **Allegati**, nella sezione [H9. Utility di diagnostica remota del Server Dr.Web](#).

7.4. Configurazione del calendario di Server Dr.Web

Per configurare il calendario di esecuzione dei task di Server Dr.Web:









1. Selezionare la voce **Amministrazione** del menu principale del **Pannello di controllo**, nella finestra che si è aperta selezionare la voce del menu di gestione **Scheduler del Server Dr.Web**. Si apre una lista dei task del **Server**.
2. Per gestire il calendario, vengono utilizzati gli elementi corrispondenti nella barra degli strumenti:
 - a) Gli elementi generali della barra degli strumenti vengono utilizzati per creare nuovi task e per gestire la sezione calendario in generale. Questi strumenti sono sempre disponibili nella barra degli strumenti.
 -  **Crea task** - per aggiungere un nuovo task. Quest'azione viene descritta in dettaglio qui sotto nella sottosezione [Editor dei task](#).
 -  **Esporta impostazioni da questa sezione in file** - per esportare il calendario in un file dell'apposito formato.
 -  **Importa impostazioni in questa sezione da file** - per importare il calendario da un file dell'apposito formato.
 - b) Per gestire i task esistenti, spuntare i flag di fronte ai task richiesti oppure il flag nell'intestazione della tabella se si vogliono selezionare tutti i task nella lista. Con questo diventano disponibili gli elementi della barra degli strumenti utilizzati per la gestione di task selezionati.

Tabella 7-3. Elementi della barra degli strumenti utilizzati per gestire i task selezionati

Impostazione		Azione
Stato	Permetti l'esecuzione	Attivare l'esecuzione dei task selezionati secondo il calendario impostato se erano proibiti.
	Proibisci l'esecuzione	Proibire l'esecuzione dei task selezionati. I task saranno presenti nella lista ma non verranno eseguiti.
 L'azione simile viene eseguita tramite l'editor del task nella scheda Generali con l'ausilio del flag Permetti l'esecuzione .		
Importanza	Rendi critico	Eseguire il task in modo straordinario al successivo avvio di Server Dr.Web se l'esecuzione di questo task è stata omessa nell'ora programmata.



Impostazione	Azione
Rendi non critico	Eeguire il task solo nell'ora programmata, nonostante l'omissione o l'esecuzione del task.
 L'azione simile viene eseguita tramite l'editor del task nella scheda Generali con l'ausilio del flag Task critico .	
 Duplica le impostazioni	Duplicare i task selezionati nella lista del calendario corrente. Tramite l'azione Duplicare le impostazioni vengono creati nuovi task che hanno le impostazioni uguali a quelle dei task selezionati.
 Programma un'altra esecuzione dei task	Per i task per cui è impostata l'esecuzione singola: eseguire il task ancora una volta secondo le impostazioni di ora (cioè come cambiare la frequenza di esecuzione del task è descritto sotto nella sottosezione Editor dei task).
 Rimuovi i task selezionati	Rimuovere dal calendario il task selezionato.

3. Per modificare i parametri di un task, selezionarlo dalla lista dei task. Si apre la finestra **Editor dei task** descritta [sotto](#).
4. Dopo aver finito di modificare il calendario, fare clic su **Salva** per accettare le modifiche.

Editor dei task

Tramite l'editor dei task si possono definire le impostazioni per:

1. Creare un nuovo task.

A questo fine fare clic sul pulsante  **Crea task** nella barra degli strumenti.

2. Modificare un task esistente.

A questo fine fare clic sul nome del task nella lista dei task.

Si apre la finestra di modifica dei parametri dei task. Le impostazioni di task per la modifica di un task esistente sono simili alle impostazioni per la creazione di un task nuovo.



I valori dei campi marcati con il carattere * devono essere impostati obbligatoriamente.

Per modificare i parametri di un task:

1. Nella scheda **Generali** vengono impostati i seguenti parametri:
 - ◆ Nel campo **Nome** viene definito il nome del task sotto cui verrà visualizzato nel calendario.
 - ◆ Per attivare l'esecuzione del task, spuntare il flag **Permetti l'esecuzione**. Se il flag non è selezionato, il task sarà presente nella lista ma non verrà eseguito.



L'azione simile viene eseguita nella finestra principale del calendario tramite l'elemento **Stato** della barra degli strumenti.

- ◆ Il flag spuntato **Task critico** comanda di avviare il task in modo straordinario alla prossima volta che si avvia il **Server Dr.Web** se l'esecuzione di tale task è stata omessa secondo il calendario (il **Server Dr.Web** è disattivato al momento di esecuzione del task). Se in un periodo il task viene omesso più volte, quando si avvia il **Server Dr.Web**, il task viene eseguito una volta.



L'azione simile viene eseguita nella finestra principale del calendario tramite l'elemento **Importanza** della barra degli strumenti.



2. Nella scheda **Azione** selezionare il tipo di task dalla lista a cascata **Azione** e configurare i parametri del task, richiesti per l'esecuzione.




Tabella 7-4. Tipi di task e i loro parametri

Tipo di task	Parametri e descrizione
Esecuzione di procedura	<p>Il task è studiato per eseguire le procedure personalizzate (per maggiori informazioni v. p. Procedure personalizzate).</p> <p>È necessario impostare i seguenti parametri:</p> <ul style="list-style-type: none">• Gruppo di procedure personalizzate - gruppo di procedure personalizzate per cui verrà eseguita la procedura.• Procedura - nome della concreta procedura personalizzata da eseguire dal gruppo selezionato nell'elenco Gruppo di procedure personalizzate.• Spuntare il flag Esegui in tutti i gruppi di procedure personalizzate affinché la procedura personalizzata selezionata venga eseguita in tutti i gruppi di procedure nelle quali è impostata. In questo caso per ciascun gruppo verrà eseguita quella procedura che è impostata proprio per questo gruppo.
Esecuzione dello script	<p>Il task è studiato per eseguire lo script Lua riportato nel campo Script.</p>
Terminazione di Server Dr.Web	<p>Il task è studiato per interrompere il funzionamento di Server.</p> <p>Viene avviato senza parametri supplementari.</p>
Sostituzione della chiave di cifratura	<p>Il task è studiato per la sostituzione periodica delle chiavi di cifratura:</p> <ul style="list-style-type: none">• della chiave privata <code>drwcsd.pri</code> su Server,• della chiave pubblica <code>drwcsd.pub</code> su postazioni. <p>Siccome alcune postazioni potrebbero essere spente al momento di sostituzione, la procedura si articola in due fasi. Devono essere creati due task per l'esecuzione di ciascuna di queste fasi, e si consiglia di eseguire la seconda fase qualche tempo dopo la prima, in cui le postazioni di sicuro si conatteranno al Server.</p> <p>Creando un task, selezionare dalla lista a cascata la fase corrispondente di sostituzione della chiave:</p> <ul style="list-style-type: none">• Aggiunzione della nuova chiave - è la prima fase della procedura in cui viene creata una nuova coppia non attiva di chiavi di cifratura. Le postazioni avranno la nuova chiave pubblica quando si conatteranno al Server.• Rimozione della chiave vecchia e passaggio alla chiave nuova - è la seconda fase in cui le postazioni vengono informate del passaggio alle nuove chiavi di cifratura, dopo di che le chiavi correnti vengono sostituite con quelle nuove: chiavi pubbliche sulle postazioni e chiave privata sul Server. <p>Le postazioni che per qualche ragione non hanno ricevuto la nuova chiave pubblica non potranno connettersi al Server. Per risolvere questo problema, sono possibili le seguenti varianti di azioni:</p> <ul style="list-style-type: none">• Mettere manualmente la nuova chiave pubblica sulla postazione (si può consultare la procedura di sostituzione di chiave su postazione nel documento Allegati, nella sezione Connessione di Agent Dr.Web ad un altro Server Dr.Web).• Consentire agli Agent di essere autenticati sul Server con una chiave pubblica non valida (v. p. Rete nelle impostazioni di Agent).
Registrazione nel file di log	<p>Il task è studiato per registrare la stringa impostata nel file di log di Server.</p> <p>Stringa - testo del messaggio da registrare nel file di log.</p>
Avvio del programma	<p>Il task è studiato per avviare un programma.</p> <p>È necessario impostare i seguenti parametri:</p> <ul style="list-style-type: none">• Nel campo Percorso — nome completo (con il percorso) del file eseguibile del programma che si vuole avviare.




Tipo di task	Parametri e descrizione
	<ul style="list-style-type: none">• Nel campo Argomenti — parametri da riga di comando per il programma da avviare.• Spuntare il flag Esegui in modo sincrono per la sincronizzazione con il Server - per attendere che sia finita l'esecuzione di questo programma prima di eseguire gli altri task del tipo Avvio del programma. Se il flag Esegui in modo sincrono non è spuntato, il Server registra nel log soltanto l'avvio del programma. Se il flag Esegui in modo sincrono è spuntato, il Server registra nel log il suo avvio, il codice di restituzione e l'ora di conclusione del programma.
Promemoria sulla scadenza della licenza	<p>Il task è studiato per visualizzare un avviso di scadenza della licenza del prodotto Dr.Web.</p> <p>È necessario impostare un periodo prima di scadenza a partire dal quale verranno visualizzati gli avvisi promemoria.</p>
Aggiornamento del repository	<p>Le informazioni su questo task sono riportate nella sezione Aggiornamenti programmati.</p>
Invio del messaggio sulla postazione	<p>Il task è studiato per mandare un messaggio personalizzabile agli utenti della postazione o del gruppo di postazioni.</p> <p>Le impostazioni del messaggio sono riportate nella sezione Invio di messaggi alle postazioni SO Windows®.</p>
Pulizia del database	<p>Il task è studiato per raccogliere e cancellare i record non utilizzati nel database del Server tramite l'esecuzione del comando <code>VACUUM</code>.</p> <p>Viene avviato senza parametri supplementari.</p>
Rimozione degli eventi non inviati	<p>Il task è studiato per cancellare dal database gli eventi non inviati.</p> <p>È necessario impostare il tempo di conservazione degli eventi non inviati, dopo il quale saranno cancellati.</p> <p>Qui sono sottintesi gli eventi trasmessi dal Server subordinato al Server principale. Se la trasmissione di un evento non è riuscita, quest'ultimo viene registrato nell'elenco degli eventi non inviati. Il Server subordinato con una periodicità fa i tentativi di trasmissione. Quando viene eseguito il task Rimozione degli eventi non inviati, vengono rimossi tutti gli eventi, di cui la durata di conservazione ha raggiunto o superato il periodo impostato.</p>
Rimozione delle registrazioni vecchie	<p>Il task è studiato per cancellare dal database le informazioni obsolete riguardanti le postazioni.</p> <p>È necessario impostare il numero di giorni dopo cui le informazioni statistiche su postazioni (però non le postazioni stesse) vengono considerate obsolete e vengono cancellate dal Server.</p> <p>Il periodo di rimozione di dati statistici viene impostato separatamente per ciascun tipo di registrazione.</p>
Rimozione delle postazioni vecchie	<p>Il task è studiato per cancellare dal database le postazioni obsolete.</p> <p>È necessario impostare un periodo di tempo (di default è di 90 giorni), e le postazioni che non si collegavano al Server durante tale periodo vengono considerate obsolete e vengono cancellate dal Server.</p>
Riavvio del Server Dr.Web	<p>Il task è studiato per il riavvio del Server.</p> <p>Viene avviato senza parametri supplementari.</p>
Risveglio delle postazioni	<p>Il task è studiato per accendere le postazioni, per esempio, prima di avviare il task di scansione.</p> <p>Le postazioni da accendere vengono impostate tramite i seguenti parametri del task:</p> <ul style="list-style-type: none">• Sveglia tutte le postazioni - devono essere accese tutte le postazioni connesse a questo Server.• Sveglia le postazioni secondo i parametri specificati - devono essere accese soltanto le postazioni che corrispondano ai parametri indicati di seguito:



Tipo di task	Parametri e descrizione
	<ul style="list-style-type: none">○ Indirizzi IP - una lista degli indirizzi IP delle postazioni da accendere. Viene impostato nel formato: 10.3.0.127, 10.4.0.1-10.4.0.5, 10.5.0.1/30. Stendendo la lista degli indirizzi, usare virgola o nuova riga come separatore. Inoltre, gli indirizzi IP possono essere sostituiti con i nomi DNS dei computer.○ Indirizzi MAC - una lista degli indirizzi MAC delle postazioni da accendere. Gli ottetti degli indirizzi MAC vengono separati dal carattere ":". Stendendo la lista degli indirizzi, usare virgola o nuova riga come separatore.○ Identificatori dei gruppi - una lista degli identificatori dei gruppi, di cui le postazioni sono da accendere. Per ogni nuovo identificatore, utilizzare un campo separato. Per aggiungere un nuovo campo fare clic sul pulsante , per eliminare un campo fare clic sul pulsante  di fronte all'identificatore da eliminare. <hr/> <p> Per l'esecuzione di questo task è necessario che sulle postazioni da accendere siano installate le schede di rete con il supporto dell'opzione Wake-on-LAN.</p> <p>Si può controllare la disponibilità del supporto dell'opzione Wake-on-LAN nella documentazione o nelle proprietà della scheda di rete (Control Panel → Network and Internet → Network Connections → Change Adapter Settings → Configure → Advanced).</p>
Backup dei dati critici del server	<p>Il task è studiato per il backup dei seguenti dati critici del Server:</p> <ul style="list-style-type: none">• database,• file della chiave di licenza,• chiave di cifratura privata. <p>È necessario impostare i seguenti parametri:</p> <ul style="list-style-type: none">• Percorso - percorso della cartella in cui verranno salvati i dati (il percorso vuoto significa la cartella predefinita).• Numero massimo di copie – numero massimo di copie di backup (il valore 0 significa l'annullamento di questa limitazione). <p>Per maggiori informazioni v. documento Allegati, p. Allegato H3.5.</p>
Backup del repository	<p>Il task è studiato per il salvataggio periodico delle copie di backup del repository.</p> <p>È necessario impostare i seguenti parametri:</p> <ul style="list-style-type: none">• Percorso - percorso completo della cartella in cui verrà salvata la copia di backup.• Numero massimo di copie - numero massimo di copie di backup del repository che il task salva nella cartella indicata. Quando viene raggiunto il numero massimo di copie del repository, per salvare una nuova copia, viene rimossa la copia più vecchia tra quelle a disposizione.• Area del repository determina quale blocco delle informazioni sul componente antivirus verrà salvato:<ul style="list-style-type: none">○ Tutto il repository - vengono salvate tutte le revisioni dal repository, per i componenti selezionati nella lista sotto.○ Soltanto le revisioni importanti - vengono salvate soltanto le revisioni contrassegnate come importanti, per i componenti selezionati nella lista sotto.○ Soltanto i file di configurazione - vengono salvati soltanto i file di configurazione, per i componenti selezionati nella lista sotto.• Contrassegnare con i flag i componenti le cui aree selezionate verranno salvate.
Sincronizzazione con Active Directory	<p>Il task è studiato per sincronizzare la struttura della rete: i container Active Directory che contengono computer diventano gruppi della rete antivirus in cui vengono messe le postazioni.</p>



Tipo di task	Parametri e descrizione
	<p>Viene avviato senza parametri supplementari.</p> <hr/> <p> Di default, questo task è disattivato. Per attivare l'esecuzione del task, impostare l'opzione Permetti l'esecuzione nelle impostazioni del task o nella barra degli strumenti, come è descritto sopra.</p> <hr/>
Il server adiacente non si collega da molto tempo	<p>Il task è studiato per visualizzare l'avviso su ciò che i Server adiacenti non si collegano a questo Server da molto tempo.</p> <p>La visualizzazione dell'avviso viene configurata nella sezione Configurazione degli avvisi tramite la voce Il server adiacente non si collega da molto tempo.</p> <p>Nei campi Ore e Minuti impostare un periodo, dopo il quale il Server adiacente verrà considerato un server che non si collega da molto tempo.</p>
La postazione non si collega da molto tempo	<p>Il task è studiato per visualizzare l'avviso su ciò che alcune postazioni non si collegano a questo Server da molto tempo.</p> <p>La visualizzazione dell'avviso viene configurata nella sezione Configurazione degli avvisi tramite la voce La postazione non si connette al server da molto tempo.</p> <p>Nel campo Giorni impostare un periodo, dopo il quale la postazione verrà considerata una postazione che non si collega da molto tempo.</p>
Resoconti statistici	<p>Il task è studiato per creare un report con le informazioni statistiche della rete antivirus.</p> <p>Per poter creare un report, è necessario che sia attivo l'avviso Report periodico (v. p. Configurazione degli avvisi). Il report creato viene salvato sul computer su cui è installato il Server. L'ottenimento del report dipende dal tipo di avviso:</p> <ul style="list-style-type: none">• In caso del metodo di invio di messaggio E-mail: sull'indirizzo e-mail impostato nella configurazione dell'avviso viene inviato un messaggio con un link del percorso del report e con il report stesso in allegato.• In caso di ogni altro metodo di invio: viene inviato l'avviso congruo che contiene il link al percorso del report. <p>Per creare il task, nel calendario si devono definire i seguenti parametri:</p> <ul style="list-style-type: none">• Profili di notifiche - nome del gruppo di avvisi secondo le cui impostazioni verrà generato il report. L'intestazione viene definita quando viene creato un nuovo gruppo di avvisi.• Lingua del resoconto - lingua in cui le informazioni sono presentate nel report.• Formato della data - formato in cui vengono presentate le informazioni statistiche con date. Sono disponibili i seguenti formati:<ul style="list-style-type: none">◦ europeo: DD-MM-YYYY HH:MM:SS◦ americano: MM/DD/YYYY HH:MM:SS• Formato del resoconto - formato del documento in cui verrà salvato il report statistico.• Periodo di riferimento - periodo di tempo, per cui le statistiche verranno incluse nel report.• Gruppi - lista dei gruppi di postazioni della rete antivirus, le cui informazioni verranno incluse nel report. Per selezionare più gruppi, utilizzare i tasti CTRL o SHIFT.• Tabelle del resoconto - lista delle tabelle statistiche da cui le informazioni verranno incluse nel report. Per selezionare diverse tabelle, utilizzare i tasti CTRL o SHIFT.• Tempo di conservazione del resoconto - periodo di conservazione del report sul computer su cui è installato il Server, a partire dal momento di creazione del report.
Eliminazione dei messaggi obsoleti	<p>Il task è studiato per cancellare dal database i seguenti messaggi:</p> <ul style="list-style-type: none">• avvisi degli agent,



Tipo di task	Parametri e descrizione
	<ul style="list-style-type: none"> • avvisi per la console web, • report generati secondo il calendario. <p>Vengono rimossi i messaggi contrassegnati come obsoleti, cioè i messaggi di cui è scaduto il periodo di conservazione che può essere configurato:</p> <ul style="list-style-type: none"> • per gli avvisi: durante la creazione degli avvisi per il metodo di invio corrispondente (v. p. Configurazione degli avvisi). • per i report: nel task di generazione dei report. <p>Viene avviato senza parametri supplementari.</p>



Le informazioni vecchie vengono rimosse dal database automaticamente al fine di risparmiare spazio su disco. Di default, per i task **Rimozione delle registrazioni vecchie** e **Rimozione delle postazioni vecchie** il periodo è di 90 giorni. Con la diminuzione di questo parametro, le informazioni statistiche sui componenti di rete antivirus accumulate diventano meno rappresentative. Con l'aumento di questo parametro, potrebbe aumentare notevolmente il volume delle risorse consumate dal **Server**.



L'esecuzione simultanea del tipo di task **Esecuzione dello script** su diversi **Server** che utilizzano l'unico database potrebbe portare agli errori nell'esecuzione di questo task.

3. Nella scheda **Tempo**:


- ◆ Dalla lista a cascata **Periodicità** selezionare la modalità di avvio del task e impostare il tempo secondo la periodicità scelta.

Tabella 7-5. Modalità di avvio e i loro parametri

Modalità di avvio	Parametri e descrizione
Finale	Il task verrà eseguito a terminazione di Server . Viene avviato senza parametri supplementari.
Iniziale	Il task verrà eseguito ad avvio di Server . Viene avviato senza parametri supplementari.
Tra N minuti dopo il task iniziale	Dalla lista a cascata Task iniziale è necessario scegliere il task rispetto al quale viene impostata l'ora di esecuzione del task corrente. Nel campo Minuto impostare o selezionare dalla lista il numero di minuti da aspettare dopo l'esecuzione del task iniziale prima che venga avviato il task corrente.
Ogni giorno	È necessario inserire l'ora e il minuto — il task verrà avviato ogni giorno all'ora indicata.
Ogni mese	È necessario selezionare un giorno (giorno del mese), immettere l'ora e il minuto — il task verrà avviato nel giorno del mese selezionato all'ora indicata.
Ogni settimana	È necessario selezionare un giorno della settimana, immettere l'ora e il minuto — il task verrà avviato nel giorno della settimana selezionato all'ora indicata.
Ogni ora	È necessario immettere un numero dallo 0 ai 59 che indica il minuto di ogni ora in cui il task verrà avviato.
Ogni N minuti	È necessario immettere il valore N per definire l'intervallo di tempo dell'esecuzione del task. Se N è pari ai 60 o superiore, il task verrà avviato ogni N minuti. Se N è inferiore ai 60, il task verrà avviato ogni minuto dell'ora multiplo di N .

- ◆ Spuntare il flag **Proibisci dopo la prima esecuzione** per eseguire il task soltanto una volta secondo l'ora impostata. Se il flag è tolto, il task verrà eseguito molte volte con la periodicità selezionata.



Per ripetere l'esecuzione di un task la cui esecuzione è definita come singola e che è già stato eseguito, utilizzare il pulsante  **Programma un'altra esecuzione dei task** che si trova nella barra degli strumenti della sezione calendario.

4. Finite le modifiche dei parametri del task, fare clic sul pulsante **Salva** per accettare le modifiche dei parametri del task, se veniva modificato un task esistente, oppure per creare un nuovo task con i parametri impostati, se veniva creato un nuovo task.

7.5. Configurazione del web server

Per configurare il web server:


1. Selezionare la voce **Amministrazione** del menu principale del **Pannello di controllo**.
2. Nella finestra che si è aperta, selezionare la voce del menu di gestione **Configurazione del web server**. Si apre la finestra di configurazione di **web server**.





I valori dei campi marcati con il carattere * devono essere impostati obbligatoriamente.


3. Nella barra degli strumenti sono disponibili i seguenti pulsanti per gestire le impostazioni della sezione:

 **Riavvia Server Dr.Web** - per riavviare il **Server** al fine di accettare le modifiche apportate in questa sezione. Il pulsante diventa attivo dopo che si sono apportate delle modifiche nelle impostazioni della sezione e si è premuto il pulsante **Salva**.

 **Recupera la configurazione da copia di backup** - lista a cascata che include le copie salvate delle impostazioni dell'intera sezione a cui si può ritornare dopo aver apportato delle modifiche. Il pulsante diventa attivo dopo che si sono apportate delle modifiche nelle impostazioni della sezione e si è premuto il pulsante **Salva**.

 **Resetta tutti i parametri ai valori iniziali** - per ripristinare tutti i parametri di questa sezione ai valori che avevano prima della modifica corrente (ultimi valori salvati).

 **Resetta tutti i parametri ai valori default** - per ripristinare tutti i parametri di questa sezione ai valori di default.

4. Per accettare le modifiche apportate nelle impostazioni della sezione, premere il pulsante **Salva**, dopodiché sarà necessario riavviare il **Server**. Per farlo, premere il pulsante  **Riavvia Server Dr.Web** nella barra degli strumenti di questa sezione.

7.5.1. Generali

Nella scheda **Generali** vengono configurate le seguenti impostazioni del funzionamento del **server web**:

- ◆ **Server** - nome del **Server Dr.Web**.

Viene impostato nel formato:

<Indirizzo IP o nome DNS del Server> [: <porta>]

Se l'indirizzo del **Server** non è impostato, viene utilizzato il nome di computer restituito dal sistema operativo o l'indirizzo di rete del **Server**: nome DNS, se disponibile, altrimenti l'indirizzo IP.

Se il numero di porta non è impostato, viene utilizzata la porta impostata nella query (per esempio in caso di connessione al **Server** dal **Pannello di controllo** o attraverso **Web API**). In particolare, in caso di connessione dal **Pannello di controllo** - è la porta specificata nella barra degli indirizzi durante la connessione del **Pannello di controllo** al **Server**.



Valore è memorizzato nel parametro `<server-name />` nel file di configurazione `webmin.conf`.

Il valore del parametro viene utilizzato anche quando vengono generati i link per il download del file d'installazione di **Agent** per le postazioni della rete antivirus.

- ◆ **Query parallele** - numero di query parallele elaborate dal **web server**. Questo parametro influisce sulle prestazioni del server. Non è consigliabile modificarne il valore senza necessità.
- ◆ **Threads Input/Output** - numero di flussi che elaborano i dati trasmessi via rete. Questo parametro influisce sulle prestazioni del **Server**. Non è consigliabile modificarne il valore senza necessità.
- ◆ **Time-out (s)** - time-out di una sessione HTTP. In caso di connessioni permanenti, il **Server** interrompe la connessione se nel periodo indicato non arrivano richieste dal client.
- ◆ **Velocità di invio minima (B/s)** - velocità minima dell'invio dei dati. Se la velocità di trasmissione in uscita nella rete è più bassa di questo valore, la connessione sarà rifiutata. Impostare il valore 0 per togliere questa limitazione.
- ◆ **Velocità di ricezione minima (B/s)** - velocità minima della ricezione dei dati. Se la velocità di trasmissione in arrivo nella rete è più bassa di questo valore, la connessione sarà rifiutata. Impostare il valore 0 per togliere questa limitazione.
- ◆ **Dimensione del buffer di invio (KB)** - dimensione dei buffer utilizzati per l'invio dei dati. Questo parametro influisce sulle prestazioni del **Server**. Non è consigliabile modificarne il valore senza necessità.
- ◆ **Dimensione del buffer di ricezione (KB)** - dimensione dei buffer utilizzati per la ricezione dei dati. Questo parametro influisce sulle prestazioni del **Server**. Non è consigliabile modificarne il valore senza necessità.
- ◆ **Lunghezza massima di una query (KB)** - lunghezza massima ammissibile di una query HTTP.
- ◆ **Utilizza compressione** - spuntare il flag per utilizzare la compressione dei dati trasmessi attraverso il canale di comunicazione con il **server web** via HTTP/HTTPS.
 - Se il flag è spuntato, è disponibile la lista a cascata **Grado di compressione**. Da questa lista si può selezionare un grado di compressione dei dati da 1 a 9, dove 1 è il grado minimo e 9 è il grado massimo di compressione.
- ◆ **Sostituisci gli indirizzi IP** - spuntare il flag per sostituire gli indirizzi IP con i nomi DNS dei computer nel file di log del **Server**.
- ◆ **Mantieni attiva la sessione SSL** - spuntare il flag per utilizzare connessione permanente per SSL. Le versioni superate dei browser potrebbero gestire in modo scorretto le connessioni permanenti SSL. In caso di problemi con l'utilizzo del protocollo SSL, disattivare questo parametro.
- ◆ **Certificato SSL** - percorso del file di certificato SSL. Nella lista a cascata sono elencati i certificati disponibili dalla directory di **Server**.
- ◆ **Chiave privata SSL** - percorso del file della chiave privata SSL. Nella lista a cascata sono elencate le chiavi private disponibili dalla directory di **Server**.

7.5.2. Avanzate

Nella scheda **Addizionali** vengono configurate le seguenti impostazioni del funzionamento del **web server**:

- ◆ Spuntare il flag **Mostra errori degli script** per visualizzare errori degli script nel browser. Questo parametro si usa dal servizio di supporto tecnico e dagli sviluppatori. Non è consigliabile modificarne il valore senza necessità.
- ◆ Spuntare il flag **Rintraccia gli script** per attivare il rintracciamento degli script. Questo parametro si usa dal servizio di supporto tecnico e dagli sviluppatori. Non è consigliabile modificarne il valore senza necessità.
- ◆ Spuntare il flag **Consenti l'interruzione degli script** per consentire l'interruzione degli script. Questo parametro si usa dal servizio di supporto tecnico e dagli sviluppatori. Non è consigliabile modificarne il valore senza necessità.



7.5.3. Trasporto

Nella scheda **Trasporto** vengono configurati gli indirizzi di rete "ascoltati" da cui il **web server** accetta le connessioni in entrata, per esempio per la connessione del **Pannello di controllo** o per l'esecuzione di query attraverso Web API:

- ◆ Nella sezione **Indirizzi ascoltati tramite HTTP**, viene configurata una lista delle interfacce che verranno ascoltate per l'accettazione delle connessioni attraverso il protocollo HTTP:

Nei campi **Indirizzo** e **Porta** è necessario indicare rispettivamente l'indirizzo IP e il numero di porta dell'interfaccia di rete da cui è consentito accettare le connessioni attraverso il protocollo HTTP.



Di default, per "l'ascolto" da parte del **web server** vengono impostati:

- **Indirizzo:** 0.0.0.0 - utilizza "tutte le interfacce di rete" per questo computer su cui è installato il **web server**.
 - **Porta:** 9080 - utilizza la porta standard 9080 per il protocollo HTTP.
- ◆ Nella sezione **Indirizzi ascoltati tramite HTTPS**, viene configurata una lista delle interfacce che verranno ascoltate per l'accettazione delle connessioni attraverso il protocollo HTTPS:

Nei campi **Indirizzo** e **Porta** è necessario indicare rispettivamente l'indirizzo IP e il numero di porta dell'interfaccia di rete da cui è consentito accettare le connessioni attraverso il protocollo HTTPS.

Di default, per "l'ascolto" da parte del **web server** vengono impostati:

- **Indirizzo:** 0.0.0.0 - utilizza "tutte le interfacce di rete" per questo computer su cui è installato il **web server**.
- **Porta:** 9081 - utilizza la porta standard 9081 per il protocollo HTTPS.

Per aggiungere un nuovo campo di indirizzo, premere il pulsante  della sezione corrispondente. Per eliminare un campo, premere il pulsante  accanto al campo da eliminare.

7.5.4. Sicurezza

Nella scheda **Sicurezza** vengono impostate le limitazioni riguardanti gli indirizzi di rete da cui il **web server** accetta le richieste HTTP e HTTPS.

Per impostare la limitazione di accesso per qualche tipo di connessione:

1. Per consentire l'accesso attraverso HTTP o HTTPS da determinati indirizzi, includerli nelle liste rispettive **HTTP: Consentito** o **HTTPS: Consentito**.
2. Per vietare l'accesso attraverso HTTP o HTTPS da determinati indirizzi, includerli nelle liste rispettive **HTTP: Negato** o **HTTPS: Negato**.
3. Gli indirizzi non inclusi in nessuna lista vengono consentiti o proibiti a seconda della selezione dei flag **Priorità di negazione per HTTP** e **Priorità di negazione per HTTPS**: se il flag è selezionato, gli indirizzi non inclusi in nessuna lista (o inclusi in tutte e due) vengono proibiti. In caso contrario, tali indirizzi vengono consentiti.



Per modificare una lista degli indirizzi:

1. Inserire l'indirizzo di rete nel campo corrispondente e premere il pulsante **Salva**.
2. Indirizzo di rete viene definito come: `<indirizzo-IP>/ [<prefisso>]`.



Le liste per inserire gli indirizzi TCPv6 saranno visualizzate solo se sul computer è installata l'interfaccia IPv6.



3. Per aggiungere un nuovo campo di indirizzo, premere il pulsante  della sezione corrispondente.
4. Per eliminare un campo, premere il pulsante .

Esempio di utilizzo del prefisso:

1. Il prefisso 24 sta per la maschera di rete: 255.255.255.0
Contiene 254 indirizzi
Gli indirizzi di host in queste reti sono del tipo: 195.136.12.*
2. Il prefisso 8 sta per la maschera di rete 255.0.0.0
Contiene fino a 16387064 indirizzi (256*256*256)
Gli indirizzi di host in queste reti sono del tipo: 125.*.*.*

7.6. Procedure personalizzate

Per semplificare e automatizzare l'esecuzione di determinati task di **Server Dr.Web**, si possono utilizzare delle procedure personalizzate realizzate come script lua.



Le procedure personalizzate si trovano nella seguente sottodirectory della directory d'installazione di **Server**:

- ◆ per il SO Windows: `var\extensions`
- ◆ per il SO FreeBSD: `/var/drwcs/extensions`
- ◆ per i SO Linux e Solaris: `/var/opt/drwcs/extensions`

Dopo l'installazione di **Server**, in questa sottodirectory si trovano le procedure personalizzate predefinite.

Si consiglia di modificare procedure personalizzate attraverso il **Pannello di controllo**.

Per configurare l'esecuzione delle procedure personalizzate:

1. Selezionare la voce **Amministrazione** del menu principale del **Pannello di controllo**.
2. Nella finestra che si è aperta, selezionare la voce del menu di gestione **Procedure personalizzate**. Si apre la finestra di configurazione delle procedure personalizzate.

Albero delle procedure

La lista gerarchica delle procedure riflette una struttura ad albero, i nodi della quale sono i gruppi di procedure e le procedure che ne fanno parte.

Inizialmente l'albero include il gruppo predefinito **Examples of the hooks** che contiene i template di tutte le procedure personalizzate disponibili. Sulla base di questi template, si possono creare le proprie procedure personalizzate.

Gestione delle procedure

Per gestire le procedure personalizzate, si usano i seguenti elementi della barra degli strumenti:







- lista a cascata che serve per aggiungere un elemento all'albero delle procedure:



Aggiungi procedura personalizzata - per aggiungere una procedura personalizzata sulla base di un template a disposizione.






-  **Aggiungi gruppo di procedure personalizzate** - per creare un nuovo gruppo in cui verranno messe le procedure.
-  **Rimuovi gli oggetti segnati** - per rimuovere una procedura personalizzata o un gruppo di procedure, selezionati nell'albero delle procedure.
-  **Consenti l'esecuzione della procedura personalizzata** - l'azione simile viene eseguita tramite l'editor di procedure mediante la selezione del flag **Consenti l'esecuzione della procedura personalizzata**.
-  **Proibisci l'esecuzione della procedura personalizzata** - l'azione simile viene eseguita tramite l'editor di procedure togliendo la spunta alla voce **Consenti l'esecuzione della procedura personalizzata**.

7.7. Configurazione degli avvisi

Dr.Web Enterprise Security Suite supporta la possibilità di inviare gli avvisi su attacchi dei virus, su stato dei componenti della rete antivirus e su altri eventi agli amministratori della rete antivirus **Dr.Web Enterprise Security Suite**.

7.7.1. Configurazione degli avvisi

Per configurare gli avvisi su eventi nella rete antivirus:

1. Selezionare la voce **Amministrazione** del menu principale del **Pannello di controllo**. Nella finestra che si è aperta selezionare la voce del menu di gestione **Configurazione delle notifiche**.
2. Quando si configurano gli avvisi per la prima volta, la lista degli avvisi deve essere vuota. Premere **Aggiungi avviso**.
3. Per abilitare l'invio di avvisi, mettere il controllo a sinistra dell'intestazione di un blocco nella posizione appropriata:
 -  - l'invio di avvisi per questo blocco è abilitato.
 -  - gli avvisi di questo blocco non verranno spediti.
4. In questa sezione, si possono creare alcuni blocchi (profili) degli avvisi, per esempio a seconda di vari modi di invio. Per aggiungere un altro blocco, premere  a destra delle impostazioni del blocco di avvisi. In fondo alla pagina verrà aggiunto un altro blocco di avvisi. Diversi blocchi di avvisi e testi dei template vengono configurati in modo indipendente.
5. Nel campo **Intestazione** impostare il nome del blocco di avvisi aggiunto. Questo nome verrà utilizzato, per esempio nella configurazione del task **Report statistici** nel calendario del **Server**. Per la modifica successiva dell'intestazione, premerla con il tasto sinistro del mouse e digitare il nome richiesto. Se ci sono più di un blocco di avvisi, quando si fa clic sul testo dell'intestazione, viene visualizzata una lista a cascata con le intestazioni dei blocchi di avvisi esistenti.
6. Per configurare l'invio delle notifiche, selezionare il modo di invio richiesto dalla lista a cascata **Metodo di invio notifiche**:
 - ◆ [Console web](#) – per inviare gli avvisi che verranno visualizzati nella [Console web](#).
 - ◆ [Agent Dr.Web](#) – per inviare gli avvisi attraverso il protocollo di **Agent**.
 - ◆ [E-mail](#) – per inviare gli avvisi via posta elettronica.
 - ◆ [SNMP](#) – per inviare gli avvisi attraverso il protocollo SNMP.
 - ◆ [Notifiche push](#) – per inviare gli avvisi push sul **Pannello di controllo della sicurezza mobile Dr.Web**. Questa voce diventa disponibile nella lista a cascata **Metodo di invio notifiche** soltanto dopo che il **Pannello di controllo della sicurezza mobile Dr.Web** viene connesso a questo **Server Dr.Web**.
 - ◆ [Windows Message](#) – per inviare avvisi mediante **Windows Messenger** (solo per i **Server SO Windows**).




Le impostazioni di ciascuno dei tipi di invio di notifiche sono descritte di seguito in questa sezione.

7. Per inviare avvisi, si può utilizzare un set di avvisi predefiniti del **Server**.



Gli avvisi predefiniti e i loro parametri vengono descritti nel documento **Allegati**, in [Allegato D1. Descrizione degli avvisi predefiniti](#).

Per configurare avvisi concreti, è necessario:

- a) Nella lista degli avvisi, spuntare i flag di fronte agli avvisi che verranno inviati in conformità al metodo di invio del blocco di avvisi corrente.
- b) Per modificare le impostazioni, premere  di fronte all'avviso che viene modificato. Si apre il template dell'avviso. Se necessario, modificare il testo dell'avviso che verrà inviato. Nel testo di avviso, si possono utilizzare le variabili di template tra parentesi graffe. Per aggiungere le variabili, si possono utilizzare le liste a cascata nell'intestazione del messaggio. Quando un messaggio viene preparato, il sistema di avviso sostituisce le variabili di template con il testo concreto che dipende dalle sue impostazioni correnti. La lista delle variabili disponibili viene riportata nel documento **Allegati**, in [Allegato D3. Parametri dei template del sistema di avviso](#).
- c) In caso degli avvisi della sottosezione **Postazione**, si può inoltre impostare una lista delle postazioni circa le quali gli avvisi verranno spediti se su queste postazioni si sono verificati degli eventi. Nella finestra di modifica del template, nell'albero **Gruppi di postazioni monitorate** selezionare gruppi di postazioni per cui verranno tracciati eventi e verranno spediti gli avvisi corrispondenti. Per selezionare diversi gruppi, utilizzare i tasti CTRL o SHIFT.



In caso del metodo di invio **SNMP**, i template di avvisi vengono impostati sul lato client SNMP. Tramite il **Pannello di controllo** nella sottosezione **Postazione** si può impostare soltanto una lista delle postazioni per cui gli avvisi verranno spediti se su queste postazioni si sono verificati degli eventi.

8. Dopo aver finito di modificare le impostazioni, premere il pulsante **Salva** per salvare tutte le modifiche apportate.

Avvisi che vengono visualizzati nella Web console

Per gli avvisi che vengono visualizzati nella **Web console**, impostare i seguenti parametri:

- ◆ **Numero di tentativi di invio** – numero di tentativi di invio del messaggio in caso di un invio non riuscito. Il numero predefinito è 10.
- ◆ **Time-out del tentativo di invio** – periodo in secondi, finito il quale viene fatto un tentativo ripetuto di invio dell'avviso. Il time-out predefinito è di 300 secondi.
- ◆ **Tempo di conservazione di una notifica** – tempo per il quale deve essere conservato un avviso dal momento della ricezione. Il tempo predefinito è di 1 giorno. Dopo il tempo specificato, l'avviso viene contrassegnato come obsoleto e viene eliminato secondo il task **Rimozione dei messaggi obsoleti** impostato nel calendario del **Server**.

Per gli avvisi ricevuti tramite questo metodo di invio, si può impostare un tempo illimitato di conservazione nella sezione [Notifiche della web console](#).

- ◆ **Invia un messaggio di test** – per inviare un avviso di test in conformità alle impostazioni del sistema di avviso. Il testo di tale avviso viene specificato nei template di avvisi.

Avvisi attraverso il protocollo di Agent

Per gli avvisi attraverso il protocollo di **Agent** impostare i seguenti parametri:



- ◆ **Numero di tentativi di invio** – numero di tentativi di invio del messaggio in caso di un invio non riuscito. Il numero predefinito è 10.



- ◆ **Time-out del tentativo di invio** – periodo in secondi, finito il quale viene fatto un tentativo ripetuto di invio dell'avviso. Il time-out predefinito è di 300 secondi.
- ◆ **Postazione** – identificatore della postazione sulla quale verranno spediti gli avvisi. L'identificatore della postazione è disponibile nelle [proprietà](#) della postazione.
- ◆ **Tempo di conservazione di una notifica** – tempo per il quale deve essere conservato un avviso dal momento della ricezione. Il tempo predefinito è di 1 giorno. Dopo il tempo specificato, l'avviso viene contrassegnato come obsoleto e viene eliminato secondo il task **Rimozione dei messaggi obsoleti** impostato nel calendario del **Server**.
- ◆ **Invia un messaggio di test** – per inviare un avviso di test in conformità alle impostazioni del sistema di avviso. Il testo di tale avviso viene specificato nei template di avvisi.

Avvisi via email



Per gli avvisi via email, impostare i seguenti parametri:

- ◆ **Numero di tentativi di invio** – numero di tentativi di invio del messaggio in caso di un invio non riuscito. Il numero predefinito è 10.
- ◆ **Time-out del tentativo di invio** – periodo in secondi, finito il quale viene fatto un tentativo ripetuto di invio dell'avviso. Il time-out predefinito è di 300 secondi.
- ◆ **Indirizzo e-mail del mittente** – indirizzo di posta elettronica del mittente degli avvisi.
- ◆ **Indirizzi e-mail dei destinatari** – indirizzi di posta elettronica dei destinatari dei messaggi. In ciascun campo si può inserire soltanto un indirizzo di posta elettronica di destinatario. Per aggiungere un altro campo di destinatario, premere il pulsante . Per rimuovere un campo, premere il pulsante .
- ◆ Nella sezione **Impostazioni del server SMTP**, impostare i seguenti parametri:
 - **Indirizzo** – indirizzo del server SMTP che verrà utilizzato per l'invio delle email.
 - **Porta** – porta del server SMTP che verrà utilizzato per l'invio delle email.
 - **Utente, Password** – se necessario, impostare il nome utente e la password dell'utente del server SMTP se il server SMTP richiede l'autenticazione.
 - Spuntare il flag **Crittografia STARTTLS** per utilizzare la crittografia *STARTTLS* per cifrare il traffico dati quando vengono inviati avvisi via email.
 - Spuntare il flag **Crittografia SSL** per utilizzare la crittografia *SSL* per cifrare il traffico dati quando vengono inviati avvisi via email.
 - Spuntare il flag **Utilizza l'autenticazione CRAM-MD5** per utilizzare *l'autenticazione* CRAM-MD5 sul mail server.
 - Spuntare il flag **Utilizza l'autenticazione DIGEST-MD5** per utilizzare *l'autenticazione* DIGEST-MD5 sul mail server.
 - Spuntare il flag **Utilizza l'autenticazione Plain** per utilizzare *l'autenticazione plain text* sul mail server.
 - Spuntare il flag **Utilizza l'autenticazione LOGIN** per utilizzare *l'autenticazione* LOGIN sul mail server.
 - Spuntare il flag **Verifica se il certificato SSL del server è corretto** per controllare la correttezza del certificato SSL del mail server.
 - Spuntare il flag **Modalità debug** per ottenere un log dettagliato di sessione SMTP. **Invia un messaggio di test** – per inviare un avviso di test in conformità alle impostazioni del sistema di avviso. Il testo di tale avviso viene specificato nei template di avvisi.



Avvisi attraverso il protocollo SNMP

Per gli avvisi attraverso il protocollo SNMP, impostare i seguenti parametri:

- ◆ **Numero di tentativi di invio** – numero di tentativi di invio del messaggio in caso di un invio non riuscito. Il numero predefinito è 10.
- ◆ **Time-out del tentativo di invio** – periodo in secondi, finito il quale viene fatto un tentativo ripetuto di invio dell'avviso. Il time-out predefinito è di 300 secondi.
- ◆ **Destinatario** - entità che riceve una query SNMP. Per esempio, un indirizzo IP o il nome DNS di un computer. In ciascun campo si può inserire soltanto un destinatario. Per aggiungere un altro campo di destinatario, premere il pulsante . Per rimuovere un campo, premere il pulsante .
- ◆ **Mittente** - entità che invia una query SNMP. Di default, è "localhost" per SO Windows e "" per SO della famiglia UNIX.
- ◆ **Community** - community SNMP o contesto. Di default, è `public`.
- ◆ **Invia un messaggio di test** – per inviare un avviso di test in conformità alle impostazioni del sistema di avviso. Il testo di tale avviso viene specificato nei template di avvisi.

Avvisi Push

Per gli avvisi Push che vengono mandati sul **Pannello di controllo mobile**, impostare i seguenti parametri:

- ◆ **Numero di tentativi di invio** – numero di tentativi di invio del messaggio in caso di un invio non riuscito. Il numero predefinito è 10.
- ◆ **Time-out del tentativo di invio** – periodo in secondi, finito il quale viene fatto un tentativo ripetuto di invio dell'avviso. Il time-out predefinito è di 300 secondi.
- ◆ **Invia un messaggio di test** – per inviare un avviso di test in conformità alle impostazioni del sistema di avviso. Il testo di tale avviso viene specificato nei template di avvisi.



Avvisi di rete di Windows



Il sistema di avviso di rete Windows funziona solamente nel SO Windows con il supporto del servizio Windows Messenger (Net Send).

Il SO Windows Vista e superiori non supportano il servizio Windows Messenger.

Per i messaggi di rete di SO Windows, impostare i seguenti parametri:

- ◆ **Numero di tentativi di invio** – numero di tentativi di invio del messaggio in caso di un invio non riuscito. Il numero predefinito è 10.
- ◆ **Time-out del tentativo di invio** – periodo in secondi, finito il quale viene fatto un tentativo ripetuto di invio dell'avviso. Il time-out predefinito è di 300 secondi.
- ◆ **Destinatario** – lista dei nomi dei computer su cui si ricevono i messaggi. In ciascun campo si può inserire soltanto un nome di computer. Per aggiungere un altro campo di destinatario, premere il pulsante . Per rimuovere un campo, premere il pulsante .
- ◆ **Invia un messaggio di test** – per inviare un avviso di test in conformità alle impostazioni del sistema di avviso. Il testo di tale avviso viene specificato nei template di avvisi.



7.7.2. Avvisi nella console web

Tramite il **Pannello di controllo**, è possibile visualizzare e gestire gli avvisi all'amministratore, ricevuti tramite il metodo **Web console** (l'invio di avvisi all'amministratore è descritto nella sezione [Configurazione degli avvisi](#)).

Per visualizzare e gestire gli avvisi:

1. Selezionare la voce **Amministrazione** del menu principale del **Pannello di controllo**. Nella finestra che si è aperta selezionare la voce del menu di gestione **Notifiche della web console**. Si apre un elenco degli avvisi inviati sulla **Web console**.
2. Per visualizzare un avviso, premere la riga corrispondente della tabella. Si apre una finestra con il testo dell'avviso. L'avviso verrà contrassegnato automaticamente come letto.
3. Per gestire la lista degli avvisi, utilizzare i seguenti elementi:
 - a) Gli elementi generali della barra degli strumenti vengono utilizzati per gestire la sezione degli avvisi in generale. Questi strumenti sono sempre disponibili nella barra degli strumenti.

Tabella 7-6. Elementi della barra degli strumenti utilizzati per gestire la sezione degli avvisi nella Web console


Impostazione		Azione
Gravità	Massima	Per visualizzare soltanto gli avvisi con la gravità Massima .
	Alta	Per visualizzare gli avvisi con la gravità da Alta a Massima .
	Media	Per visualizzare gli avvisi con la gravità da Media a Massima .
	Bassa	Per visualizzare gli avvisi con la gravità da Bassa a Massima .
	Minima	Per visualizzare tutti gli avvisi con la gravità da Minima a Massima .
Fonte	Agent	Per visualizzare gli avvisi relativi ad eventi su postazioni
	Server	Per visualizzare gli avvisi relativi ad eventi su Server


Per visualizzare gli avvisi ricevuti entro un determinato intervallo di tempo, utilizzare uno dei seguenti metodi:

- Nella lista a cascata nella barra degli strumenti selezionare uno degli intervalli di tempo predefiniti.
- Nei calendari a cascata selezionare le date di inizio e di fine di un intervallo di tempo.

Dopo aver modificato i valori di queste impostazioni, premere il pulsante **Aggiorna** per visualizzare l'elenco degli avvisi in conformità alle impostazioni definite.

b) Per gestire singoli avvisi, spuntare i flag di fronte agli avvisi richiesti oppure il flag generale nell'intestazione della tabella se si vogliono selezionare tutti gli avvisi nella lista. Con questo diventano disponibili gli elementi della barra degli strumenti utilizzati per la gestione di avvisi selezionati:

 **Elimina avvisi** - per eliminare definitivamente tutti gli avvisi selezionati senza la possibilità di recupero.

 **Contrassegna avvisi come letti** - per contrassegnare come letti tutti gli avvisi selezionati.

c) Spuntare la casella **Conserva il messaggio senza rimozione automatica** nell'elenco degli avvisi di fronte agli avvisi che non devono essere eliminati dopo la fine del periodo di conservazione (il periodo di conservazione viene impostato prima dell'invio di avvisi nella sezione [Configurazione delle notifiche](#) nelle impostazioni del metodo di invio **Console web**). Tali avvisi verranno conservati fino a quando non verranno rimossi manualmente nella sezione **Notifiche della web console** oppure non verrà deselezionata la casella di fronte a questi avvisi.



7.7.3. Avvisi non inviati

Tramite il **Pannello di controllo**, è possibile tracciare e gestire gli avvisi all'amministratore che non sono stati inviati secondo le impostazioni della sezione [Configurazione delle notifiche](#)).

Per visualizzare e gestire gli avvisi non inviati:

1. Selezionare la voce **Amministrazione** del menu principale del **Pannello di controllo**. Nella finestra che si è aperta selezionare la voce del menu di gestione **Notifiche non inviate**. Si apre l'elenco delle notifiche non inviate di questo **Server**.
2. Nell'elenco delle notifiche non inviate vengono elencati gli avvisi di cui l'invio non è riuscito, ma il numero di tentativi di invio, determinato nelle impostazioni di quest'avviso, non si è ancora esaurito.
3. La tabella di avvisi non inviati contiene le seguenti informazioni:
 - **Notifica** - nome dell'avviso dall'elenco degli avvisi predefiniti.
 - **Intestazione** - nome del blocco di avvisi, secondo le cui impostazioni viene inviato quest'avviso.
 - **Tentativi di invio rimanenti** - numero di tentativi rimanenti di invio dell'avviso se l'invio non è riuscito. Il numero iniziale di tentativi di invio ripetuto viene impostato durante la configurazione delle notifiche nella sezione [Configurazione delle notifiche](#). Dopo l'invio di un avviso, non è possibile modificarne il numero di tentativi di invio.
 - **Tempo del successivo tentativo di invio** - data e ora del successivo tentativo di invio dell'avviso. La periodicità con cui si ripetono i tentativi di invio dell'avviso viene impostata durante la configurazione delle notifiche nella sezione [Configurazione delle notifiche](#). Dopo l'invio di un avviso, non è possibile modificarne la periodicità di tentativi di invio.
 - **Destinatario** - indirizzi dei destinatari dell'avviso.
 - **Errore** - errore per cui non è riuscito l'invio della notifica.
4. Per gestire gli avvisi non inviati:
 - a) Spuntare i flag di fronte a concreti avvisi oppure il flag nell'intestazione della tabella per selezionare tutti gli avvisi nella lista.
 - b) Utilizzare i seguenti pulsanti nella barra degli strumenti:
 - ➡ **Rispedisci** - per inviare subito gli avvisi selezionati. Viene fatto un tentativo straordinario di invio di avviso. Se l'invio non è riuscito, il numero di tentativi rimanenti diminuisce di uno, e il tempo del successivo tentativo viene conteggiato dal momento dell'invio corrente con la periodicità impostata nella sezione [Configurazione delle notifiche](#).
 - ✖ **Rimuovi** - per eliminare definitivamente tutti gli avvisi non inviati selezionati senza la possibilità di recupero.
5. Gli avvisi non inviati vengono cancellati dalla lista nei seguenti casi:
 - a) L'avviso è stato mandato con successo al destinatario.
 - b) L'avviso è stato cancellato dall'amministratore manualmente tramite il pulsante ✖ **Rimuovi** nella barra degli strumenti.
 - c) Si è esaurito il numero di tentativi di invio ripetuto e la notifica non è stata inviata.
 - d) Nella sezione [Configurazione delle notifiche](#) è stato eliminato il blocco di avvisi, secondo le cui impostazioni venivano inviati questi avvisi.

7.8. Gestione del repository di Server Dr.Web

Il *repository* di **Server Dr.Web** è studiato per conservare i campioni modello del software e per aggiornarli dai server **SAM**.



Per questo fine, il repository utilizza un set dei file che vengono chiamati *prodotti*. Ciascun prodotto si trova in una sottodirectory separata della directory di `repository` che si trova nella directory `var` che con l'installazione di default è una sottodirectory della directory radice di **Server**. Le funzioni di `repository`, nonché la gestione delle funzioni, vengono effettuate indipendentemente per ciascun prodotto.

Per gestire il repository, si utilizza il concetto *revisione* di un prodotto. Una revisione è lo stato dei file di un prodotto, corretto per un determinato momento (comprende nomi dei file e checksum), essa è caratterizzata da un numero unico.

Il repository sincronizza le revisioni di un prodotto nelle seguenti direzioni:

- a) su **Server Dr.Web** dal sito di aggiornamento del prodotto (via protocollo HTTP),
- b) tra vari **Server Dr.Web** nella configurazione con diversi server (secondo il criterio di scambio impostato),
- c) da **Server Dr.Web** su postazioni.

Il repository permette all'Amministratore della rete antivirus di impostare i seguenti parametri:

- ◆ lista dei siti di aggiornamento nelle operazioni del tipo **a)**;
- ◆ limitare la lista dei prodotti che richiedono la sincronizzazione del tipo **a)** (in questo modo, l'utente ha la possibilità di tracciare solamente le modifiche necessarie di singole categorie di prodotti);
- ◆ limitare la lista delle parti dei prodotti che richiedono la sincronizzazione del tipo **c)** (l'utente può scegliere che cosa concretamente è da installare su postazioni);
- ◆ controllare il passaggio alle revisioni nuove (si possono testare i prodotti per conto proprio prima dell'implementazione);
- ◆ aggiungere propri componenti ai prodotti;
- ◆ creare indipendentemente degli nuovi prodotti per cui anche viene eseguita la sincronizzazione.


Attualmente nella fornitura sono compresi i seguenti prodotti:

- ◆ **Server Dr.Web**,
- ◆ **Agent Dr.Web** (software **Agent**, software antivirus postazione per i sistemi operativi corrispondenti),
- ◆ **Server proxy Dr.Web**,
- ◆ Database dei virus **Dr.Web**,
- ◆ Database di **SpIDer Gate**,
- ◆ Database di **Antispam Dr.Web**,
- ◆ Notizie di **Doctor Web**.



7.8.1. Stato del repository

Per controllare lo stato attuale del repository o per aggiornare i componenti della rete antivirus:

1. Selezionare la voce **Amministrazione** del menu principale del **Pannello di controllo**, nella finestra che si è aperta selezionare la voce del menu di gestione **Stato del repository**.
2. La finestra che si è aperta, visualizza una lista dei prodotti del repository, la data della revisione utilizzata al momento, la data della revisione ultima scaricata e lo stato corrente dei prodotti.
3. Per gestire i contenuti del repository, utilizzare i seguenti pulsanti:
 - Premere il pulsante **Verifica aggiornamenti** per verificare la disponibilità degli aggiornamenti di tutti i prodotti su **SAM** e per scaricare gli aggiornamenti disponibili dai server **SAM**.
 - Premere il pulsante  **Ricarica il repository da disco** per ricaricare la versione corrente del repository da disco.

Quando viene avviato, il **Server** carica i contenuti del repository nella memoria, e se durante l'operazione del **Server** i contenuti del repository sono stati modificati dall'amministratore in un modo diverso da quello fornito dal **Pannello di controllo**, ad esempio, i contenuti del repository sono stati aggiornati tramite un'utilità esterna o manualmente, per cominciare ad utilizzare la versione caricata su disco, è necessario riavviare il repository.

7.8.2. Aggiornamenti differiti

La sezione **Aggiornamenti differiti** contiene una lista dei prodotti per cui gli aggiornamenti di prodotti sono stati vietati temporaneamente nella sezione **Configurazione dettagliata del repository** → *<Prodotto>* → [Aggiornamenti differiti](#). Una revisione differita è considerata *congelata*.

La tabella dei prodotti congelati contiene le seguenti informazioni:

- ◆ **Cartella nel repository** - nome della directory del prodotto congelato nel repository:
 - 10-drwgatedb - database di **SpIDer Gate**,
 - 10-drwspamdb - database di **AntiSpam**,
 - 20-drwagent - **Agent Dr.Web** per Windows,
 - 20-drwandroid - **Agent Dr.Web** per Android,
 - 20-drwcs - **Server Dr.Web**,
 - 20-drwunix - **Agent Dr.Web** per UNIX,
 - 80-drwnews - notizie di **Doctor Web**.
- ◆ **Revisione** - numero della revisione congelata.
- ◆ **Differito fino al** - tempo fino a cui sono stati differiti gli aggiornamenti di questo prodotto.

Quando si fa clic su una riga della tabella dei prodotti congelati, si apre una tabella con le informazioni dettagliate sulla revisione congelata di questo prodotto.

Le funzioni di aggiornamenti differiti possono essere utilizzate se è necessario annullare temporaneamente la distribuzione di ultima revisione di un prodotto su tutte le postazioni della rete antivirus, per esempio se è necessario prima provare questa revisione su un numero limitato di postazioni.

Per utilizzare le funzioni di aggiornamenti differiti, eseguire le azioni descritte nella sezione **Configurazione dettagliata del repository** → [Aggiornamenti differiti](#).



Per gestire gli aggiornamenti differiti:

1. Spuntare il flag di fronte ai prodotti per cui si vuole impostare un'azione da applicare agli aggiornamenti differiti. Per selezionare tutti i prodotti, spuntare il flag nell'intestazione della tabella dei prodotti congelati.
2. Nella barra degli strumenti selezionare l'azione richiesta:
 - ✔ **Esegui subito** - per annullare la congelazione del prodotto e per includere questa revisione nell'elenco delle revisioni per distribuirla su postazioni secondo la [procedura](#) generale.
 - ✘ **Annulla l'aggiornamento** - per annullare la congelazione del prodotto e per vietare questa revisione. Si riprende il processo dell'ottenimento di aggiornamenti dal **SAM**. La revisione scongelata verrà rimossa dall'elenco delle revisioni del prodotto. Quando arriva la prossima revisione, la revisione scongelata verrà rimossa anche dal disco.
 - 🕒 **Cambia il tempo di differimento degli aggiornamenti** - per impostare il tempo per cui la revisione di questo prodotto viene rinviata. Il tempo di inizio di congelazione viene conteggiato dal momento della ricezione della revisione dal **SAM**.
3. Se per un prodotto congelato non è stata impostata un'azione da applicare dopo lo scongelamento, una volta finito il tempo impostato nell'elenco **Tempo di differimento degli aggiornamenti**, la revisione verrà scongelata automaticamente e verrà inclusa nell'elenco delle revisioni per essere distribuita su postazioni secondo la [procedura](#) generale.

7.8.3. Configurazione generale del repository

La sezione **Configurazione generale del repository** consente di impostare i parametri della connessione a **SAM** e dell'aggiornamento del repository per tutti i prodotti.

Per modificare la configurazione del repository:

1. Selezionare la voce **Amministrazione** del menu principale del **Pannello di controllo**.
2. Nella finestra che si è aperta selezionare la voce del menu di gestione **Configurazione generale del repository**.
3. Configurare tutti i parametri necessari dell'aggiornamento da **SAM** descritti [di seguito](#).
4. Se modificando i parametri, si devono annullare tutte le modifiche apportate, utilizzare i seguenti pulsanti nella barra degli strumenti:
 - ⚙️ **Resetta tutti i parametri ai valori iniziali** - per ripristinare tutti i parametri di questa sezione nei valori che avevano prima della modifica corrente (ultimi valori salvati). Per applicare la stessa azione a singoli parametri, utilizzare i pulsanti ↩️ di fronte a ciascun parametro.
 - ⚙️ **Resetta tutti i parametri ai valori default** - per ripristinare tutti i parametri di questa sezione nei valori salvati nel file di configurazione di **Server**. Per applicare la stessa azione a singoli parametri, utilizzare i pulsanti ↩️ di fronte a ciascun parametro.
5. Fare clic su uno dei pulsanti nella barra degli strumenti:
 - **Salva e sincronizza di nuovo** - per salvare tutte le modifiche apportate e per eseguire un aggiornamento del repository da **SAM** secondo le nuove impostazioni.
 - **Salva e ricarica da disco** - per salvare tutte le modifiche apportate senza l'aggiornamento del repository da **SAM**. In questo caso la versione di repository corrente viene ricaricata da disco (v. inoltre la sezione [Stato del repository](#)).

Configurazione su SAM Dr.Web



Nella scheda **SAM Dr.Web** vengono configurati i parametri della connessione al **Sistema di aggiornamento mondiale Dr.Web**.



Per modificare i parametri della connessione a SAM, si utilizzano le seguenti impostazioni:

- ◆ **URI di base** - la directory sui server di aggiornamenti che contiene gli aggiornamenti dei prodotti **Dr.Web**.
- ◆ Spuntare il flag **Utilizza CDN** per consentire l'utilizzo di Content Delivery Network per il caricamento del repository.
- ◆ Spuntare il flag **Utilizza SSL** per caricare il repository attraverso la connessione sicura SLL.

In questo caso dalla lista a cascata **Certificati validi** selezionare il tipo di certificati SSL da accettare automaticamente.

- ◆ Se necessario, modificare la lista dei server **SAM** da cui viene aggiornato il repository, nella sezione **Lista dei server del Sistema di aggiornamento mondiale Dr.Web**:
 - Per aggiungere un server **SAM** alla lista dei server utilizzati per l'aggiornamento, premere il pulsante  ed inserire l'indirizzo del server **SAM** nel campo aggiunto.
 - Per cancellare un server **SAM** dalla lista dei server utilizzati, premere il pulsante  di fronte al server che si vuole cancellare.
 - L'ordine dei server **SAM** nella lista determina l'ordine di connessione del **Server Dr.Web** durante l'aggiornamento del repository. Per modificare l'ordine dei server **SAM** trascinare il server richiesto, tenendo premuto la riga del server alla matrice a sinistra.

Quando viene installato il **Server Dr.Web**, la lista contiene soltanto i server di aggiornamenti della società **Doctor Web**. Se necessario, si possono configurare le proprie zone di aggiornamenti ed inserirle nella lista dei server per la ricezione di aggiornamenti.

Configurazione degli aggiornamenti di Agent Dr.Web

L'aggiornamento di repository per il software **Agent** e per il pacchetto antivirus viene configurato separatamente per le varie versioni dei SO su cui verrà installato tale software:

- ◆ Nella scheda **Agent Dr.Web per Windows** nel gruppo di pulsanti di scelta, indicare se è necessario aggiornare tutti i componenti installati su postazioni SO Windows o soltanto i database dei virus.
- ◆ Nella scheda **Agent Dr.Web per UNIX** indicare per quali SO della famiglia UNIX è necessario aggiornare i componenti installati su postazioni.



Per disattivare completamente la ricezione di aggiornamenti da **SAM** per **Agent per UNIX**, passare alla sezione **Configurazione dettagliata del repository**, voce **Agent Dr.Web per UNIX**, e nella scheda **Sincronizzazione** spuntare il flag **Disattiva l'aggiornamento del prodotto**.

Configurazione degli aggiornamenti di Server Dr.Web

Nella scheda **Server Dr.Web** indicare per quali SO verrà eseguito l'aggiornamento dei file di **Server**:

- ◆ Per ricevere gli aggiornamenti per i **Server** sotto tutti i SO supportati, spuntare il flag **Aggiorna tutte le piattaforme disponibili in SAM**.
- ◆ Per ricevere gli aggiornamenti per i **Server** soltanto sotto alcuni dei SO supportati, spuntare i flag solo accanto a questi SO.



Per disattivare completamente la ricezione di aggiornamenti da **SAM** per **Server**, passare alla sezione **Configurazione dettagliata del repository**, voce **Server Dr.Web**, e nella scheda **Sincronizzazione** spuntare il flag **Disattiva l'aggiornamento del prodotto**.



Notizie di Doctor Web

Nella scheda **Notizie della società Doctor Web** impostare una lista delle lingue in cui verranno scaricate le notizie.

L'iscrizione alle sezioni di notizie viene configurata nella sezione [Impostazioni](#) → **Abbonamento**.

Si possono leggere le notizie di **Doctor Web** nella sezione del menu principale del **Pannello di controllo**  **Guida** → **Notizie**.

Lingue di Agent Dr.Web per Windows

Nella scheda **Lingue di Agent Dr.Web per Windows** impostare una lista delle lingue dell'interfaccia di **Agent** e di pacchetto antivirus per SO Windows che verranno scaricate da **SAM**.

7.8.4. Configurazione dettagliata del repository

La sezione **Configurazione dettagliata del repository** consente di configurare le revisioni separatamente per ogni prodotto nel repository.




Per modificare la configurazione del repository:

1. Selezionare la voce **Amministrazione** del menu principale del **Pannello di controllo**.
2. Nella finestra che si è aperta nella sottosezione del menu di gestione **Configurazione dettagliata del repository** selezionare la voce che corrisponde al prodotto che si vuole modificare.
3. Configurare tutti i parametri di repository necessari del prodotto selezionato, che vengono descritti [di seguito](#).
4. Nella barra degli strumenti premere il pulsante **Salva e ricarica da disco** per salvare tutte le modifiche apportate. In questo caso la versione di repository corrente viene ricaricata da disco (v. inoltre la sezione [Stato del repository](#)).









Lista delle revisioni

Nella scheda **Lista delle revisioni** vengono riportate le informazioni su tutte le revisioni di questo prodotto disponibili su questo **Server**.

La tabella delle revisioni contiene le seguenti colonne:

Nome di colonna	Descrizione dei contenuti
Distribuita	<p>Il marcatore automatico in questa colonna definisce lo stato delle revisioni del prodotto. Nella colonna possono esserci due tipi di marcatore:</p> <p> - <i>Revisione distribuita</i>. La revisione viene utilizzata per aggiornare gli Agent e il software antivirus su postazioni.</p> <p>La revisione da distribuire viene selezionata nel seguente modo:</p> <ol style="list-style-type: none">1. Viene distribuita la revisione che è contrassegnata dal marcatore  nella colonna Corrente. Può essere contrassegnata soltanto una revisione. Per il prodotto Agent Dr.Web per Windows non esiste la possibilità di contrassegnare dal marcatore una revisione che è stata ricevuta prima della revisione che viene distribuita al momento.2. Se nella colonna Corrente nessuna revisione è contrassegnata, viene distribuita l'ultima revisione contrassegnata dal marcatore  nella colonna Conservata.



Nome di colonna	Descrizione dei contenuti
	<p>3. Se nelle colonne Corrente e Conservata non è contrassegnata alcuna revisione, viene distribuita la revisione più recente.</p> <p>Il marcatore automatico sempre indica la revisione che viene distribuita.</p> <p>  - <i>Revisione congelata</i>. Questa revisione non viene distribuita su postazioni, le nuove revisioni non vengono scaricate dal Server. Per le azioni applicabili in caso di congelazione, consultare la sottosezione Aggiornamenti differiti.</p> <p>Se c'è una revisione congelata, la revisione da distribuire viene selezionata nel seguente modo:</p> <ol style="list-style-type: none">1. Se è impostato il marcatore  nella colonna Corrente, su postazioni viene distribuita la revisione corrente.2. Se non è impostato il marcatore  nella colonna Corrente, su postazioni viene distribuita la revisione precedente a quella congelata.
Corrente	<p>Impostare il marcatore  per indicare la revisione di prodotto da utilizzare per l'aggiornamento degli Agent e del software antivirus su postazioni.</p> <p>Può essere impostata soltanto una revisione corrente.</p> <p>Il marcatore che indica la revisione corrente può anche essere non impostato.</p>
Conservata	<p>Impostare il marcatore  per conservare questa revisione quando il repository viene cancellato in automatico.</p> <p>Il marcatore può essere impostato per più revisioni alla volta.</p> <p>Il marcatore può anche essere non impostato.</p> <p>Il Server conserva su disco un determinato numero di revisioni di prodotto, che viene impostato nella scheda Sincronizzazione. Quando viene raggiunto il numero massimo di revisioni conservate temporaneamente, per salvare una nuova revisione scaricata da SAM, la revisione più vecchia conservata temporaneamente viene rimossa.</p> <p>Quando il repository viene cancellato in automatico, non vengono rimosse le seguenti revisioni:</p> <ul style="list-style-type: none">• Le revisioni contrassegnate dal marcatore  nella colonna Conservata.• La revisione contrassegnata dal marcatore  nella colonna Corrente. <p>Se una revisione di prodotto funziona in modo stabile, si può contrassegnarla come conservata, e qualora da SAM arrivi una revisione non stabile, si può eseguire il rollback a quella precedente.</p>
Revisione	<p>Data di ricezione della revisione di prodotto.</p> <p>Se la revisione è congelata, in questa colonna inoltre viene visualizzato lo stato del blocco.</p>

Sincronizzazione

Nella scheda **Sincronizzazione** vengono configurati i parametri dell'aggiornamento del repository di **Server** da **SAM**:

- ◆ Nella lista a cascata **Numero di revisioni conservate** si imposta il numero di revisioni di prodotto che sono conservate temporaneamente su disco, senza contare le revisioni contrassegnate in almeno una delle colonne nella scheda **Lista delle revisioni**. Qualora arrivi una revisione nuova e il numero di revisioni di prodotto abbia già raggiunto il massimo impostato, viene eliminata la revisione più vecchia. Le revisioni contrassegnate come **Corrente**, **Conservata** e **Distribuita** non possono essere eliminate.
- ◆ Spuntare il flag **Disattiva l'aggiornamento del prodotto** per disattivare la ricezione degli aggiornamenti di questo prodotto dai server **SAM**. Gli **Agent** verranno aggiornati alla revisione corrente sul **Server** (o secondo la [procedura della scelta della](#) revisione da distribuire).



Per alcuni prodotti sono inoltre disponibili le seguenti impostazioni:

- ◆ Spuntare il flag **Aggiorna soltanto i seguenti file** per ricevere gli aggiornamenti da **SAM** soltanto per i file indicati di seguito.
- ◆ Spuntare il flag **Non aggiornare soltanto i seguenti file** per disattivare l'aggiornamento da **SAM** soltanto per i file indicati di seguito.

Le liste dei file vengono impostate nel formato di espressioni regolari.

Se sono spuntati entrambi i flag, i file vengono selezionati nel seguente modo:

1. Dalla lista completa dei file di prodotto, vengono selezionati i file secondo le liste **Aggiorna soltanto i seguenti file**.
2. Dalla lista ottenuta al passo 1, vengono cancellati i file secondo le liste **Non aggiornare soltanto i seguenti file**.
3. Da **SAM** vengono aggiornati soltanto i file selezionati al passo 2.

Avvisi

Nella scheda **Notifiche** vengono configurati le notifiche sugli aggiornamenti del repository:

- ◆ Spuntare il flag **Non notificare soltanto dei seguenti file**, per disattivare l'invio delle notifiche soltanto degli eventi relativi ai file indicati nella lista di seguito.
- ◆ Spuntare il flag **Notifica soltanto dei seguenti file** per inviare le notifiche soltanto degli eventi relativi ai file indicati nella lista di seguito.

Le liste dei file vengono impostate nel formato di espressioni regolari.

Se le liste di eccezioni non sono impostate, verranno inviate tutte le notifiche attivate sulla pagina [Configurazione delle notifiche](#).

Le notifiche su aggiornamenti di repository vengono configurate sulla pagina di configurazione di notifiche nella sottosezione **Repository**.

Aggiornamenti differiti

Nella scheda **Aggiornamenti differiti** è possibile rinviare la distribuzione di aggiornamenti su postazioni per un determinato periodo. Una revisione differita è considerata *congelata*.

Queste funzioni possono essere utilizzate se è necessario annullare temporaneamente la distribuzione di ultima revisione di un prodotto su tutte le postazioni della rete antivirus, per esempio se è necessario prima provare questa revisione su un numero limitato di postazioni.

Per utilizzare le funzioni di aggiornamenti differiti, eseguire le seguenti azioni:

1. Per il prodotto da congelare, impostare gli aggiornamenti differiti come viene descritto [di seguito](#).
2. Per annullare la distribuzione dell'ultima revisione, impostare come corrente una delle revisioni precedenti nella scheda [Lista delle revisioni](#).
3. Per il gruppo di postazioni su cui verrà distribuita la revisione più recente, spuntare il flag **Ricevi tutti gli aggiornamenti recenti** nella sezione **Rete antivirus** → [Limitazione degli aggiornamenti delle postazioni](#). Sulle altre postazioni verrà distribuita la revisione che è stata contrassegnata come corrente nel passo 2.
4. La prossima revisione scaricata da **SAM**, che soddisfa le condizioni dell'opzione **Differisci solo gli aggiornamenti dei seguenti file**, verrà congelata e differita per il tempo selezionato nella lista **Tempo di differimento degli aggiornamenti**.





Per configurare gli aggiornamenti differiti:

1. Spuntare il flag **Differisci gli aggiornamenti** per annullare temporaneamente il caricamento degli aggiornamenti di questo prodotto ricevuti dai server **SAM**.
2. Nella lista a cascata **Tempo di differimento degli aggiornamenti** selezionare il tempo per il quale il caricamento degli aggiornamenti viene differito contando dal momento della loro ricezione dai server **SAM**.
3. Se necessario, spuntare il flag **Differisci solo gli aggiornamenti dei seguenti file** per rinviare la distribuzione degli aggiornamenti che contengono i file che corrispondono alle maschere wildcard specificate nella lista sotto. La lista delle maschere viene impostata nel formato di espressioni regolari.

Se il flag non è spuntato, verranno congelati tutti gli aggiornamenti che arrivano da **SAM**.

Per annullare la congelazione:

- ◆ Nella scheda **Lista delle revisioni** premere  **Esegui subito** per annullare la congelazione del prodotto e per includere questa revisione nell'elenco delle revisioni per distribuirla su postazioni secondo la [procedura](#) generale.
- ◆ Nella scheda **Lista delle revisioni** premere  **Annulla l'aggiornamento** per annullare la congelazione del prodotto e per vietare questa revisione. Si riprende il processo dell'ottenimento di aggiornamenti da **SAM**. La revisione scongelata verrà rimossa dall'elenco delle revisioni del prodotto. Quando arriva la prossima revisione, la revisione scongelata verrà rimossa anche dal disco.
- ◆ Una volta finito il tempo impostato nell'elenco **Tempo di differimento degli aggiornamenti**, la revisione verrà scongelata automaticamente e verrà inclusa nell'elenco delle revisioni per essere distribuita su postazioni secondo la [procedura](#) generale.

Le revisioni congelate di tutti i prodotti vengono gestite nella sezione [Aggiornamenti differiti](#).

7.8.5. Contenuti del repository

La sezione **Contenuti del repository** consente di visualizzare e gestire i contenuti correnti del repository a livello di directory e di file del repository.

La finestra principale della sezione **Contenuti del repository** contiene l'albero gerarchico dei contenuti del repository, che riflette tutte le directory e file nella versione corrente del repository con l'elenco di tutte le revisioni disponibili di ogni prodotto.

Visualizzazione delle informazioni sul repository

Per visualizzare le informazioni sugli oggetti del repository, nell'albero gerarchico dei contenuti del repository selezionare un oggetto. Si apre il pannello delle proprietà con le seguenti informazioni:

- Nella sottosezione **Oggetti selezionati** vengono riportate le informazioni dettagliate sull'oggetto selezionato nell'albero dei contenuti del repository: **Tipo**, **Dimensione** (solo per file separati), **Data di creazione** e **Data di modifica**.
- Nella sottosezione **Stato del repository** vengono riportate le informazioni generali su tutti gli oggetti del repository: la lista corrente degli oggetti e la data dell'ultimo aggiornamento.

Gestione del repository

Per gestire i contenuti del repository, utilizzare i seguenti pulsanti nella barra degli strumenti:

 [Esporta i file del repository in archivio,](#)

 [Importa archivio con i file del repository,](#)



✘ Rimuovi gli oggetti selezionati - per rimuovere gli oggetti selezionati nell'albero dei contenuti del repository, senza la possibilità di recupero.



Dopo aver modificato i contenuti del repository, per esempio dopo aver rimosso o importato oggetti del repository, affinché il **Server** possa utilizzare i dati modificati, è necessario riavviare il repository.

V. sezione [Stato del repository](#).

Esportazione del repository

Per salvare i file del repository in un archivio .zip, eseguire le seguenti azioni:

1. Nell'albero gerarchico dei contenuti del repository, selezionare un prodotto, una revisione separata di un prodotto o l'intero repository. L'intero repository verrà esportato se nulla è selezionato nell'albero oppure è selezionata l'intestazione dell'albero - **Repository**. Per selezionare diversi oggetti, utilizzare i tasti della tastiera CTRL o SHIFT.

Quando si esegue l'esportazione di oggetti del repository, prestare attenzione ai tipi principali di oggetto da esportare:

- a) Archivi Zip dei prodotti del repository. Tali archivi contengono uno dei seguenti tipi di oggetto del repository:
 - L'intero repository.
 - L'intero prodotto.
 - L'intera revisione separata di un prodotto.

Gli archivi in cui vengono esportati questi oggetti possono essere [importati](#) tramite la sezione **Contenuti del repository**. Il nome di tali archivi include il prefisso `repository_`.

- b) Archivi Zip di file separati del repository.

Gli archivi in cui vengono esportati file e directory separate che si trovano nell'albero gerarchico più in basso degli oggetti dal p. **a)**, non possono essere importati tramite la sezione **Contenuti del repository**. Il nome di tali archivi include il prefisso `files_`.

Si possono utilizzare tali archivi come backup di file per la sostituzione manuale. Tuttavia, non è consigliato sostituire file del repository manualmente, non utilizzando la sezione **Contenuti del repository**.

2. Premere il pulsante **Esporta i file del repository in archivio** nella barra degli strumenti.
3. Il percorso per il salvataggio dell'archivio .zip con l'oggetto selezionato nel repository viene impostato in conformità alle impostazioni del browser web in cui è aperto il **Pannello di controllo**.

Importazione del repository

Per caricare i file del repository da un archivio .zip, eseguire le seguenti azioni:

1. Premere il pulsante **Importa archivio con i file del repository** nella barra degli strumenti.
2. Nella finestra che si è aperta nella sezione **Selezionare un file** selezionare un archivio .zip con i file del repository. Per selezionare file, si può utilizzare il pulsante .

Possono essere importati soltanto gli archivi .zip in cui è stato esportato uno dei seguenti tipi di oggetti del repository:

- L'intero repository.
- L'intero prodotto.
- L'intera revisione separata di un prodotto.

I nomi di tali archivi ad esportazione includono il prefisso `repository_`.



3. Nella sezione **Parametri dell'importazione**, impostare i seguenti parametri:
 - **Aggiungi soltanto le revisioni mancanti** - in questa modalità di importazione, vengono aggiunte soltanto le revisioni del repository che mancano nella versione corrente. Le altre revisioni rimangono invariate.
 - **Sostituisci l'intero repository** - in questa modalità di importazione, il repository viene sostituito per intero con quello importato.
 - Spuntare il flag **Importa i file di configurazione** per importare i file di configurazione insieme all'importazione del repository.
4. Premere il pulsante **Importa** per iniziare il processo di importazione.

7.9. Possibilità aggiuntive

7.9.1. Gestione del database

La sezione **Gestione del database** consente di mantenere il database con cui interagisce il **Server Dr.Web**.




La sezione **Generali** contiene i seguenti parametri:

- ◆ Il campo **Ultima manutenzione della base di dati** - la data dell'ultima esecuzione dei comandi di manutenzione di database da questa sezione.
- ◆ Una lista dei comandi per la manutenzione del database, che include:
 - Comandi analoghi ai task dal [calendario di Server Dr.Web](#). I nomi dei comandi corrispondono ai nomi dei task dalla sezione **Azioni** nel calendario di **Server** (i task corrispondenti del calendario vengono descritti nella tabella [Tipi di task e i loro parametri](#)).
 - Il comando **Analisi della base di dati**. È studiato per ottimizzare il database di **Server** attraverso l'esecuzione del comando `analyse`.

Per eseguire i comandi di manutenzione di database:

1. Nella lista dei comandi spuntare i flag per i comandi che si desidera eseguire.
Se necessario, modificare i periodi di tempo per i comandi di pulizia di database, trascorsi i quali le informazioni conservate vengono ritenute obsolete e devono essere rimosse dal **Server**.
2. Premere il pulsante **Applica adesso**. Tutti i comandi selezionati verranno eseguiti immediatamente.
Per un'esecuzione differita e/o periodica automatica di questi comandi (eccetto il comando **Analisi della base di dati**) utilizzare lo [Scheduler del Server](#).

Per gestire il database, utilizzare i seguenti pulsanti nella barra degli strumenti:

-  [Importazione](#),
-  [Esportazione](#),
-  [Copia di backup](#).

Esportazione del database

Per salvare le informazioni dal database in un file, eseguire le seguenti azioni:

1. Premere il pulsante  **Esportazione** nella barra degli strumenti.



2. Nella finestra di configurazione dell'esportazione selezionare una delle opzioni:
 - ◆ **Esporta l'intero database** per salvare tutte le informazioni dal database in un archivio gz. Il file XML, ottenuto durante l'esportazione, è analogo al file di esportazione di database che viene ottenuto quando si avvia il file eseguibile di **Server** dalla riga di comando con l'opzione `xmlexportdb`. Questo file di esportazione può essere importato quando si avvia il file eseguibile di **Server** dalla riga di comando con l'opzione `xmlimportdb`.
Una descrizione dettagliata di questi comandi è riportata nel documento **Allegati**, nella sezione [H3.3. Comandi di gestione del database](#)).
 - ◆ **Esporta le informazioni circa le workstation e i gruppi** per salvare le informazioni su oggetti della rete antivirus in un archivio zip. Come risultato dell'esecuzione di quest'operazione, in un file di un apposito formato vengono salvate tutte le informazioni sui gruppi di postazioni e sugli account di postazioni della rete antivirus servita da questo **Server**. Il file di esportazione include le seguenti informazioni su postazioni: proprietà, configurazione dei componenti, permessi, impostazioni delle limitazioni di aggiornamenti, calendario, lista dei componenti da installare, statistiche, informazioni su postazioni rimosse; su gruppi: proprietà, configurazione dei componenti, permessi, impostazioni delle limitazioni di aggiornamenti, calendario, lista dei componenti da installare, identificatore del gruppo padre.
In seguito il file di esportazione può essere [importato](#) attraverso la sezione **Gestione del database**.
3. Premere il pulsante **Esporta**.
4. Il percorso per il salvataggio dell'archivio con il database viene impostato in conformità con le impostazioni del browser web in cui è aperto il **Pannello di controllo**.



Importazione del database

L'importazione del file di database con le informazioni su oggetti della rete antivirus può essere utilizzata per trasferire le informazioni sia su un **Server** nuovo che su un **Server** che già funziona nella rete antivirus, in particolare per unire le liste delle postazioni servite da due **Server**.



Al **Server** su cui viene fatta l'importazione potranno connettersi tutte le postazioni, le informazioni su cui vengono importate. Quando si fa l'importazione, prestare attenzione che sul server deve esserci il numero corrispondente di licenze disponibili per connettere le postazioni trasferite. Per esempio, se necessario, nella sezione [Gestione licenze](#) aggiungere una chiave di licenza dal **Server** da cui sono state trasferite le informazioni circa le postazioni.

Per caricare il database da file, eseguire le seguenti azioni:

1. Premere il pulsante  **Importazione** nella barra degli strumenti.
2. Nella finestra di importazione impostare un archivio zip con il file di database. Per selezionare file, si può utilizzare il pulsante .

Possono essere importati soltanto gli archivi .zip che sono stati ottenuti attraverso l'esportazione di database per la variante **Esporta le informazioni circa le workstation e i gruppi**.

3. Premere il pulsante **Importa** per iniziare il processo di importazione.
4. Se durante l'importazione vengono scoperte postazioni e/o gruppi con identificatori uguali che fanno parte sia delle informazioni importate che del database del **Server** corrente, si apre la sezione **Collisioni** per impostare le azioni con gli oggetti duplicati.

Le liste dei gruppi e delle postazioni vengono riportate in tabelle separate.

Per la rispettiva tabella di oggetti dalla lista a cascata **Modalità di importazione dei gruppi** o **Modalità di importazione delle postazioni** selezionare una variante per risolvere la collisione:


- **Mantieni i dati dell'importazione per tutti** - per cancellare tutte le informazioni sugli oggetti duplicati dal database del **Server** corrente e sovrascriverle con le informazioni dal database che viene importata. L'azione viene applicata contemporaneamente a tutti gli oggetti duplicati in questa tabella.



- **Mantieni i dati correnti per tutti** - per mantenere tutte le informazioni sugli oggetti duplicati dal database del **Server** corrente. Le informazioni dal database che viene importata verranno ignorate. L'azione viene applicata contemporaneamente a tutti gli oggetti duplicati in questa tabella.
- **Seleziona manualmente** - per impostare manualmente un'azione a ciascun oggetto duplicato separatamente. In questa modalità la lista degli oggetti duplicati sarà disponibile per la modifica. Impostare le opzioni di fronte agli oggetti che verranno mantenuti.

Premere **Salva**.

Copiatura di backup

Per creare una copia di backup dei dati critici del **Server**, premere il pulsante  **Copiatura di backup** nella barra degli strumenti. I dati verranno salvati in un archivio gz. I file ottenuti come risultato della copiatura di backup sono analoghi ai file ottenuti quando si avvia il file eseguibile di **Server** dalla riga di comando con l'opzione `backup`.

Questo comando è descritto in più dettagli nel documento **Allegati**, nella sezione [H3.5. Creazione di copie di riserva dei dati critici del Server Dr.Web](#).

7.9.2. Statistiche di Server Dr.Web

Tramite il **Pannello di controllo** è possibile visualizzare le statistiche di funzionamento di **Server Dr.Web**, che specificano il consumo delle risorse di sistema del computer su cui è installato il **Server Dr.Web** e l'interazione via rete con i componenti della rete antivirus e con risorse esterne, in particolare con **SAM**.

Per visualizzare le statistiche di funzionamento di Server Dr.Web:

1. Selezionare la voce **Amministrazione** del menu principale del **Pannello di controllo**.
2. Nella finestra che si è aperta, selezionare la voce del menu di gestione **Statistiche del Server Dr.Web**.
3. Nella finestra che si è aperta sono riportate le seguenti sezioni delle informazioni statistiche:
 - **Attività dei client** - informazioni sul numero di client connessi a questo **Server: Agent Dr.Web, Server Dr.Web** adiacenti e installer di **Agent Dr.Web**.
 - **Traffico di rete** - parametri di traffico di rete in entrata e uscita durante lo scambio di dati con il **Server**.
 - **Utilizzo delle risorse di sistema** - parametri di consumo di risorse di sistema del computer su cui è installato il **Server**.
 - **Microsoft NAP** - parametri di funzionamento di [Dr.Web NAP Validator](#).
 - **Utilizzo del database** - parametri di utilizzo del database del **Server**.
 - **Utilizzo della cache di file** - parametri di utilizzo della cache di file del computer su cui è installato il **Server**.
 - **Utilizzo della cache DNS** - parametri di utilizzo della cache, che conserva query inviate a server DNS, sul computer su cui è installato il **Server**.
 - **Avvisi** - parametri di funzionamento del sottosistema che invia [notifiche](#) all'amministratore.
 - **Repository** - parametri di scambio di dati del repository del **Server** con i server **SAM**.
 - **Statistiche web** - parametri di connessione al **Web server**.
 - **Cluster** - parametri di connessione attraverso il protocollo di sincronizzazione interserver se viene utilizzato un cluster di **Server** nella configurazione di una rete multi-server.
4. Per visualizzare le statistiche di una sezione, premere il nome della sezione richiesta.
5. Nell'elenco che si è aperto sono riportate i parametri della sezione con contatori dinamici dei valori.



6. Contemporaneamente con l'apertura della sezione statistica, si attiva la rappresentazione grafica delle modifiche per ciascuno dei parametri. In particolare:
 - Per disattivare la rappresentazione grafica, premere il nome della sezione richiesta. Se la rappresentazione grafica viene disattivata, il valore numerico dei parametri continua ad aggiornarsi in maniera dinamica.
 - Per riattivare la rappresentazione grafica dei dati, premere ancora una volta il nome della sezione richiesta.
 - I nomi delle sezioni e i rispettivi parametri, per cui è attivata la rappresentazione grafica, sono evidenziati in grassetto.
7. Per modificare la frequenza dell'aggiornamento dei parametri, servirsi dei seguenti strumenti nella barra di gestione:
 - Dalla lista a cascata **Frequenza dell'aggiornamento** selezionare il periodo richiesto di aggiornamento di dati. Quando cambia il valore dalla lista a cascata, viene applicato automaticamente il periodo di aggiornamento dei dati numerici e grafici.
 - Premere il pulsante **Aggiorna** per aggiornare una volta tutti i valori delle informazioni statistiche nello stesso tempo.
8. Quando il puntatore del mouse passa sopra i dati grafici, viene visualizzato il valore numerico del punto selezionato nella forma:
 - **Abs** - il valore assoluto del parametro.
 - **Delta** - aumento del valore del parametro rispetto al valore precedente secondo la frequenza di aggiornamento di dati.
9. Per nascondere i parametri della sezione, premere la freccia a sinistra del nome della sezione. Quando i parametri della sezione vengono nascosti, la rappresentazione grafica viene cancellata, e quando i parametri vengono riaperti, il rendering inizia di nuovo.

7.9.3. Copie di backup

La sezione **Copie di backup** consente di visualizzare a livello di directory e file e salvare localmente i contenuti delle copie di backup dei dati critici del **Server**.

Con il backup vengono salvati i seguenti oggetti: le impostazioni di repository, i file di configurazione, le chiavi di cifratura, i certificati, una copia di backup del database interno.

I backup dei dati critici del **Server** vengono salvati nei seguenti casi:


- ◆ Come risultato dell'esecuzione del task **Backup dei dati critici del Server** secondo il [calendario di Server](#).
- ◆ Come risultato della copiatura di backup eseguita quando si avvia il file eseguibile di **Server** dalla riga di comando con l'opzione `backup`. Questo comando è descritto in più dettagli nel documento **Allegati**, nella sezione [H3.5. Creazione di copie di riserva dei dati critici del Server Dr.Web](#).

Visualizzazione delle informazioni sulle copie di backup

Per visualizzare le informazioni su una copia di backup, selezionare un oggetto nella lista gerarchica delle copie di backup. Si apre un pannello di proprietà con le informazioni sull'oggetto: **Tipo**, **Dimensione** (solo per singoli file), **Data di creazione** e **Data di modificazione**.

Gestione delle copie di backup

Per gestire le copie di backup, utilizzare i seguenti pulsanti nella barra degli strumenti:


 **Esporta** - consente di salvare una copia di backup dell'oggetto selezionato, sul computer su cui è aperto il **Pannello di controllo**.



✘ **Rimuovi gli oggetti selezionati** - per rimuovere gli oggetti selezionati nell'albero, senza la possibilità di recupero.

Esportazione di una copia di backup

Per salvare una copia di backup localmente, eseguire le seguenti azioni:

1. Nell'albero gerarchico selezionare le copie di backup desiderate (per selezionare una copia di backup interamente, basta selezionare nell'albero la directory che corrisponde a questa copia di backup) o file separati da copie di backup. Per selezionare più oggetti, utilizzare i pulsanti CTRL o MAIUSCOLO. Quando si esegue l'esportazione, prestare attenzione ai tipi principali di oggetto da esportare:
 - a) Gli archivi Zip di copie di backup vengono salvati per i seguenti oggetti selezionati:
 - Una o più copie di backup interamente (in caso di selezione di directory che corrispondono alle copie di backup).
 - Diversi file singoli da copie di backup.
 - b) File singoli da copie di backup. Se solo un file è stato selezionato per l'esportazione, viene salvato nella forma originale, senza compressione in archivio.
2. Premere il pulsante  **Esporta** nella barra degli strumenti.
3. Il percorso per il salvataggio degli oggetti selezionati viene impostato in conformità con le impostazioni del browser web in cui è aperto il **Pannello di controllo**.

7.10. Caratteristiche di una rete con diversi Server Dr.Web

Dr.Web Enterprise Security Suite consente di creare una rete antivirus che includa diversi **Server Dr.Web**. In questo caso, ciascuna postazione viene registrata su un determinato **Server** e questo consente di distribuire il carico tra i server.

Le relazioni tra i **Server** possono avere una struttura gerarchica e questo consente di distribuire in modo ottimale il carico sui **Server**.

Per lo scambio di informazioni tra i **Server** viene utilizzato un apposito *protocollo di sincronizzazione interserver*.

Possibilità fornite dal protocollo di sincronizzazione interserver:

- ◆ Distribuzione degli aggiornamenti tra i **Server** all'interno della rete antivirus.
- ◆ Trasferimento veloce degli aggiornamenti ricevuti dai server **SAM Dr.Web**.
- ◆ Tra i **Server** associati vengono trasferite le informazioni sullo stato di postazioni protette.
- ◆ Trasferimento delle licenze per postazioni protette tra i **Server** adiacenti.

7.10.1. Struttura di una rete con diversi Server Dr.Web

In una rete antivirus è possibile installare diversi **Server Dr.Web**. In questo caso ogni **Agent Dr.Web** si connette a uno dei **Server**. Ogni **Server** insieme alle postazioni antivirus connesse funziona come una rete antivirus separata, come descritto nelle sezioni precedenti.

Dr.Web Enterprise Security Suite permette di connettere tali reti antivirus, organizzando la trasmissione di informazioni tra i **Server Dr.Web**.

Un Server Dr.Web può trasmettere su un altro Server Dr.Web:

- ◆ aggiornamenti del software e dei database dei virus. In questo caso solo uno di essi riceve gli aggiornamenti da **SAM Dr.Web**;

- ◆ informazioni su eventi dei virus, statistiche di operazione ecc.;
- ◆ licenze per postazioni protette (il trasferimento di licenza tra i **Server** viene configurato in [Gestione licenze](#)).

Dr.Web Enterprise Security Suite distingue due tipi di relazione tra i Server Dr.Web:

- ◆ *relazione del tipo principale-subordinato*, in cui il server principale trasmette a quello subordinato gli aggiornamenti e riceve da esso le informazioni su eventi,
- ◆ *relazione tra server paritari*, in cui le direzioni di trasmissione di informazioni e i tipi di informazione vengono configurati in maniera personalizzata.

In [immagine 7-1](#) è rappresentata un esempio della struttura della rete con diversi **Server**.

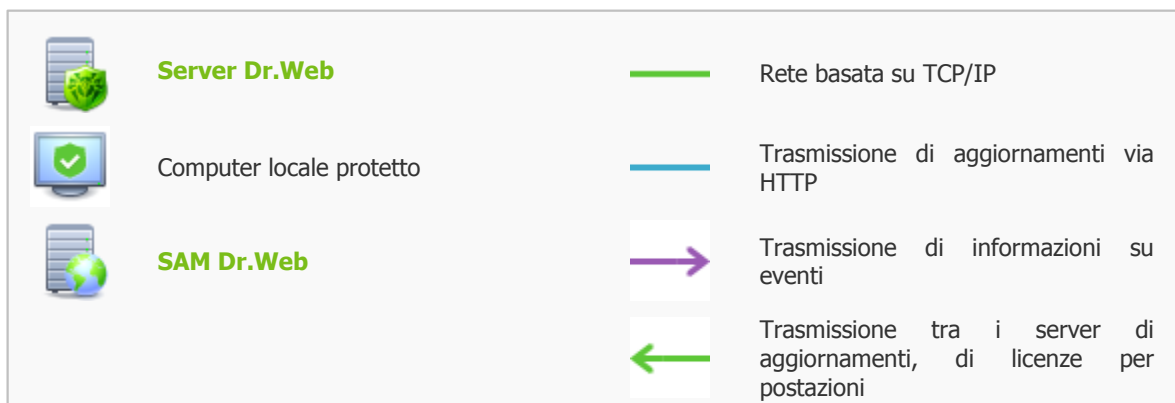
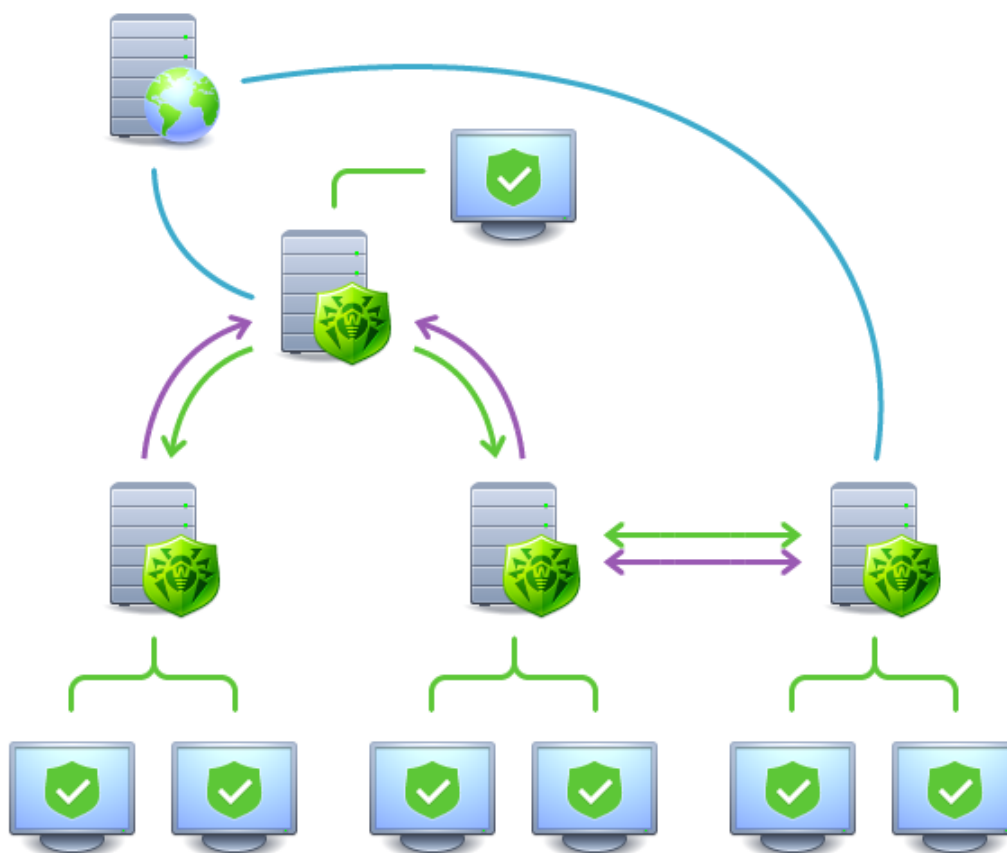


Immagine 7-1. Rete con diversi Server



Alcuni vantaggi di una rete antivirus con diversi Server Dr.Web:

1. Possibilità di ricevere aggiornamenti dai server **SAM Dr.Web** attraverso un **Server Dr.Web** con la successiva trasmissione sugli altri **Server** direttamente attraverso intermediari.



I **Server** che ricevono aggiornamenti da un **Server** principale non ricevono aggiornamenti da **SAM**, anche se tale task è disponibile nel loro calendario.

Tuttavia, per il caso in cui il **Server** principale sia temporaneamente non disponibile, si consiglia di lasciare nel calendario del **Server** subordinato il task di aggiornamento dai server **SAM**. Questo permetterà agli **Agent** connessi al **Server** subordinato di ottenere gli aggiornamenti dei database dei virus e dei moduli di programma (v. anche [Configurazione generale del repository](#)).



Nel task di aggiornamento da **SAM** sul **Server** principale che distribuisce gli aggiornamenti, è necessario configurare la ricezione degli aggiornamenti del software server per tutti i sistemi operativi installati su tutti i **Server** subordinati che ricevono gli aggiornamenti da questo **Server** principale (v. p. [Configurazione generale del repository](#)).

2. Possibilità di distribuire le postazioni tra diversi **Server** diminuendo il carico su ognuno di essi.
3. Unione delle informazioni da diversi **Server** su uno di essi; possibilità di ottenere le informazioni in forma consolidata in una sessione del **Pannello di controllo** su questo **Server**.



Dr.Web Enterprise Security Suite traccia e blocca autonomamente percorsi ciclici di trasmissione delle informazioni.

4. Possibilità di trasferire licenze libere per postazioni su un **Server** adiacente. In questo caso, la chiave di licenza stessa rimane a disposizione del **Server** che la distribuisce, le licenze libere vengono rilasciate al **Server** adiacente per un determinato periodo di tempo, scaduto il quale vengono prese indietro.

7.10.2. Configurazione delle relazioni tra i Server Dr.Web

Per avvalersi le possibilità di utilizzo di diversi **Server**, si deve configurare le relazioni tra di essi.

Si consiglia di progettare prima la struttura della rete antivirus, contrassegnando tutti i flussi d'informazione progettati e prendendo la decisione quali relazioni saranno "tra i paritari" e quali saranno del tipo "principale-subordinato". Dopo questo per ogni **Server** che fa parte della rete antivirus, occorre configurare le relazioni con i **Server** adiacenti (i **Server** adiacenti sono collegati da almeno un flusso d'informazione).

Un esempio della configurazione della comunicazione dei Server Dr.Web principale e subordinato:



I valori dei campi marcati con il carattere * devono essere impostati obbligatoriamente.

1. Assicurarsi che tutti e due **Server Dr.Web** operano correttamente.
2. A ciascuno dei **Server Dr.Web** dare un nome "parlante" per non sbagliare quando si configura la connessione tra i **Server Dr.Web** e quando successivamente si gestiscono i server. Si può farlo nel menu del **Pannello di controllo Amministrazione** → **Configurazione del Server Dr.Web** nella scheda **Generali** nel campo **Nome**. In quest'esempio chiamiamo il **Server** principale **MAIN** e quello subordinato – **AUXILIARY**.



3. Su entrambi i **Server Dr.Web** abilitare il protocollo server. Per farlo, nel menu del **Pannello di controllo Amministrazione** → **Configurazione del Server Dr.Web** nella scheda **Moduli** spuntare il flag **Protocollo di Server Dr.Web** (v. p. [Moduli](#)).



Se il protocollo server non è attivo, quando viene creata una nuova relazione nel **Pannello di controllo** viene visualizzato un avviso di necessità di attivazione di tale protocollo e viene indicato il link alla sezione corrispondente del **Pannello di controllo**.

4. Riavviare entrambi i **Server Dr.Web**.
5. Tramite il **Pannello di controllo** del **Server** subordinato (**AUXILIARY**), aggiungere il **Server principale** (**MAIN**) all'elenco dei **Server** adiacenti. Per farlo, selezionare la voce **Relazioni** dal menu principale. Si apre una finestra che contiene la lista gerarchica dei **Server** della rete antivirus che sono adiacenti a questo **Server**. Per aggiungere un **Server** a questa lista, premere il pulsante **Crea relazione** nella barra degli strumenti.

Si apre una finestra di descrizione delle relazioni tra il **Server** attuale e quello che viene aggiunto. Impostare i seguenti parametri:

- ◆ **Tipo di relazione - Principale.**
- ◆ **Nome** - nome del **Server** principale (**MAIN**).
- ◆ **Password*** - una password di accesso al **Server** principale.
- ◆ **Proprie chiavi del Server Dr.Web** - una lista delle chiavi di cifratura pubbliche del **Server** che viene configurato. Premere il pulsante e selezionare la chiave `drwcsd.pub` che corrisponde al **Server** attuale. Per aggiungere un'altra chiave, premere e aggiungere una chiave nel nuovo campo.
- ◆ **Chiavi del Server Dr.Web adiacente*** - una lista delle chiavi di cifratura pubbliche del **Server** principale che viene collegato. Premere il pulsante e selezionare la chiave `drwcsd.pub` che corrisponde al **Server** principale. Per aggiungere un'altra chiave, premere e aggiungere una chiave nel nuovo campo.
- ◆ **Indirizzo*** - indirizzo di rete del **Server** principale e la porta per la connessione. Viene impostato nel formato `<indirizzo_di_Server>:<porta>`.

Si può ricercare la lista dei **Server** disponibili in rete. Per farlo:

- a) Premere la freccia a destra del campo **Indirizzo**.
 - b) Nella finestra che si è aperta, indicare la lista delle reti nel formato: separate da trattino (per esempio, `10.4.0.1-10.4.0.10`), separate da virgola e spazio (per esempio, `10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90`), utilizzando il prefisso di rete (per esempio, `10.4.0.0/24`).
 - c) Premere il pulsante . Inizia una ricerca nella rete dei **Server** disponibili.
 - d) Selezionare un **Server** nella lista dei **Server** disponibili. Il suo indirizzo verrà scritto nel campo **Indirizzo** per la creazione di una relazione.
- ◆ **Indirizzo del Pannello di controllo della sicurezza Dr.Web** - si può indicare l'indirizzo della pagina iniziale del **Pannello di controllo** del **Server** principale (v. p. [Pannello di controllo della sicurezza Dr.Web](#)).
 - ◆ Nella lista a cascata **Parametri della connessione** viene impostato il principio di connessione dei **Server** della relazione che viene creata.
 - ◆ Nelle liste a cascata **Crittografia** e **Compressione** impostare i parametri di cifratura e di compressione di traffico dati tra i **Server** che vengono collegati (v. p. [Utilizzo di cifratura e di compressione di traffico](#)).
 - ◆ **Periodo di validità delle licenze rilasciate** - periodo per cui vengono rilasciate le licenze dalla chiave sul **Server** principale. L'impostazione viene utilizzata se il **Server** principale rilascerà licenze al **Server** attuale.



- ◆ **Periodo per il rinnovo delle licenze ricevute** - l'impostazione non viene utilizzata se viene creata una relazione a **Server** principale.
- ◆ **Periodo di sincronizzazione delle licenze** - periodicità di sincronizzazione delle informazioni su licenze rilasciate tra i **Server**.
- ◆ I flag nelle sezioni **Licenze**, **Aggiornamenti** e **Eventi** sono spuntati in conformità alla relazione *principale-subordinato* e non possono essere modificati:
 - il **Server** principale invia aggiornamenti sul **Server** subordinato;
 - il **Server** principale invia aggiornamenti sul **Server** subordinato;
 - il **Server** principale riceve le informazioni su eventi dal **Server** subordinato.
- ◆ Nella sezione **Limitazioni degli aggiornamenti** > **Eventi** si può impostare un calendario di trasmissione di eventi dal **Server** attuale su quello principale (le modalità di trasmissione di eventi vengono modificate nel modo uguale alla modifica di modalità di aggiornamenti nella sezione [Limitazione degli aggiornamenti delle postazioni](#)).

Premere il pulsante **Salva**.

Come risultato, il **Server** principale (MAIN) viene incluso nelle cartelle **Principali** e **Offline** (v. [immagine 7-2](#)).

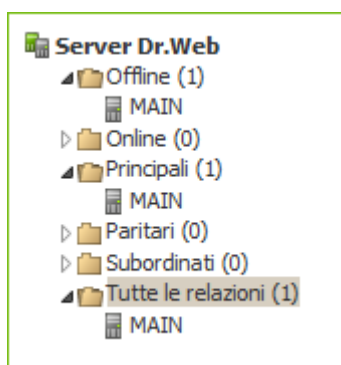


Immagine 7-2.

6. Aprire il **Pannello di controllo** del **Server** principale (MAIN) e aggiungere il **Server** subordinato (AUXILIARY) all'elenco dei **Server** adiacenti. Per farlo, selezionare la voce **Relazioni** dal menu principale. Si apre una finestra che contiene la lista gerarchica dei **Server** della rete antivirus che sono adiacenti a questo Server. Per aggiungere un **Server** a questa lista, premere il pulsante **Crea relazione** nella barra degli strumenti.

Si apre una finestra di descrizione delle relazioni tra il **Server** attuale e quello che viene aggiunto. Impostare i seguenti parametri:

- ◆ **Tipo di relazione** - **Subordinato**.
- ◆ **Nome** - nome del **Server** subordinato (AUXILIARY).
- ◆ **Password*** - inserire la stessa password di quella indicata nella voce **5**.
- ◆ **Proprie chiavi del Server Dr.Web** - una lista delle chiavi di cifratura pubbliche del **Server** che viene configurato. Premere il pulsante e selezionare la chiave `drwcsd.pub` che corrisponde al **Server** attuale. Per aggiungere un'altra chiave, premere e aggiungere una chiave nel nuovo campo.
- ◆ **Chiavi del Server Dr.Web adiacente*** - una lista delle chiavi di cifratura pubbliche del **Server** subordinato che viene collegato. Premere il pulsante e selezionare la chiave `drwcsd.pub` che corrisponde al **Server** subordinato. Per aggiungere un'altra chiave, premere e aggiungere una chiave nel nuovo campo.
- ◆ **Indirizzo del Pannello di controllo della sicurezza Dr.Web** - si può indicare l'indirizzo della pagina iniziale del **Pannello di controllo** del **Server** subordinato (v. p. [Pannello di controllo della sicurezza Dr.Web](#)).



- ◆ Nella lista a cascata **Parametri della connessione** viene impostato il principio di connessione dei **Server** della relazione che viene creata.
- ◆ Nelle liste a cascata **Crittografia** e **Compressione** impostare i parametri di cifratura e di compressione di traffico dati tra i **Server** che vengono collegati (v. p. [Utilizzo di cifratura e di compressione di traffico](#)).
- ◆ **Periodo di validità delle licenze rilasciate** - l'impostazione non viene utilizzata se viene creata una relazione a **Server** subordinato.
- ◆ **Periodo per il rinnovo delle licenze ricevute** - periodo fino alla scadenza di una licenza, a partire da cui il **Server** subordinato richiede il rinnovo della licenza ricevuta dal **Server** attuale. L'impostazione viene utilizzata se il **Server** subordinato riceverà licenze dal **Server** attuale.
- ◆ **Periodo di sincronizzazione delle licenze** - periodicità di sincronizzazione delle informazioni su licenze rilasciate tra i **Server**.
- ◆ I flag nelle sezioni **Licenze**, **Aggiornamenti** e **Eventi** sono spuntati in conformità alla relazione *principale-subordinato* e non possono essere modificati:
 - il **Server** subordinato riceve licenze dal **Server** principale;
 - il **Server** subordinato riceve aggiornamenti dal **Server** principale;
 - il **Server** subordinato invia le informazioni su eventi sul **Server** principale.
- ◆ Nella sezione **Limitazioni degli aggiornamenti > Aggiornamenti** si può impostare un calendario di trasmissione di aggiornamenti dal **Server** attuale su quello subordinato (le modalità di trasmissione di aggiornamenti vengono modificate nel modo uguale alla modifica di modalità di aggiornamenti nella sezione [Limitazione degli aggiornamenti delle postazioni](#)).

Premere il pulsante **Salva**.

Come risultato, il **Server** subordinato (AUXILIARY) viene incluso nelle cartelle **Subordinati** e **Offline** (v. [immagine 7-3](#)).

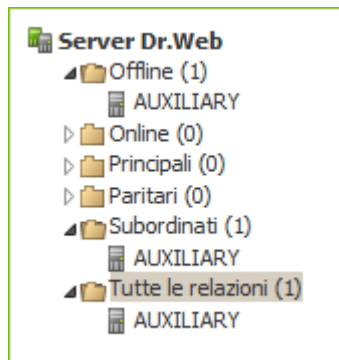


Immagine 7-3.

7. Attendere che viene stabilita una connessione tra i **Server** (di solito ci vuole meno di un minuto). Per il controllo, aggiornare periodicamente la lista dei **Server** tramite il tasto F5. Dopo che è stata stabilita la connessione, il **Server** subordinato (AUXILIARY) viene trasferito dalla cartella **Offline** nella cartella **Online** (v. [immagine 7-4](#)).

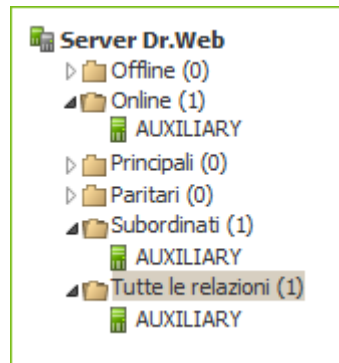


Immagine 7-4.

8. Aprire il **Pannello di controllo** del **Server** subordinato (AUXILIARY) e assicurarsi che il **Server** principale (MAIN) sia connesso a quello subordinato (AUXILIARY) (v. [immagine 7-5](#)).

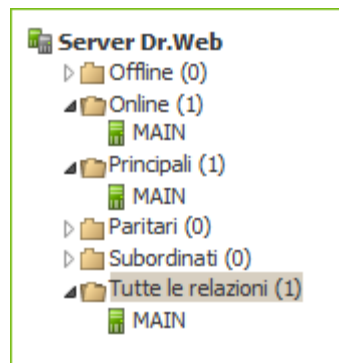


Immagine 7-5.



Non è possibile creare una relazione tra diversi **Server** con la stessa copia dei parametri: password e chiave di cifratura pubblica `drwcsd.pub`.



Quando viene creata una relazione paritaria tra **Server**, si consiglia di indicare l'indirizzo del **Server** che viene connesso soltanto nelle impostazioni di uno di essi.

Questo non influisce su interazione tra i **Server**, però permette di evitare record del tipo `Link with the same key id is already activated` nel log di funzionamento dei **Server**.

Non è possibile stabilire una connessione tra i Server Dr.Web nei seguenti casi:

- ◆ Problemi di connessioni di rete.
- ◆ Quando veniva configurata la relazione, è stato impostato un indirizzo sbagliato del **Server** principale.
- ◆ Sono state impostate chiavi di cifratura pubbliche `drwcsd.pub` non valide su uno dei **Server**.
- ◆ È stata impostata una password di accesso non valida su uno dei **Server** (sono state impostate le password che non coincidono sui **Server** che vengono collegati).

7.10.3. Utilizzo di una rete antivirus con diversi Server Dr.Web

Una caratteristica della rete con diversi **Server** è che dai server **SAM Dr.Web** gli aggiornamenti vengono ricevuti attraverso una parte dei **Server Dr.Web** (di regola, da uno o più **Server** principali). In questo caso solo su questi **Server** si deve impostare un calendario con il task di aggiornamento (v. p. [Configurazione del calendario di Server Dr.Web](#)). Qualsiasi **Server** che abbia ottenuto gli aggiornamenti dai server **SAM Dr.Web** oppure da un altro **Server** li trasmette immediatamente su



tutti i **Server** per cui tale possibilità è configurata su questo server (cioè su tutti i server subordinati e anche su quelli dei server paritari per cui la possibilità di ricezione di aggiornamenti è impostata in modo esplicito).



Dr.Web Enterprise Security Suite traccia automaticamente le situazioni quando, per l'incorretta programmazione della topologia della rete e per l'incorretta configurazione dei **Server**, un aggiornamento, già ottenuto da un'altra fonte, arriva di nuovo sullo stesso **Server**, e tale aggiornamento ripetuto non viene eseguito.

L'amministratore può inoltre ottenere le informazioni consuntive sugli eventi dei virus più importanti nei segmenti della rete connessi a qualche **Server**, attraverso le relazioni interserver (per esempio, nella configurazione descritta sopra "un server principale, altri server subordinati" queste informazioni vengono consolidate sul **Server** principale).

Per visualizzare le informazioni su eventi dei virus su tutti i Server Dr.Web associati a questo Server:

1. Selezionare la voce **Relazioni** del menu principale del **Pannello di controllo**.
2. Nella finestra che si è aperta nella sezione **Tabelle** del menu di gestione, selezionare la voce **Report di riepilogo** per visualizzare le informazioni sul totale record di eventi sui **Server** adiacenti. Nella tabella con le statistiche dei **Server** adiacenti vengono visualizzate le informazioni nelle seguenti sezioni:
 - ◆ **Infezioni** - infezioni rilevate sulle postazioni connesse ai **Server** adiacenti.
 - ◆ **Errori** - errori di scansione.
 - ◆ **Statistiche** - statistiche delle infezioni rilevate.
 - ◆ **Avvio/terminazione** - avvio e completamento dei task di scansione su postazioni.
 - ◆ **Stato** - stato del software antivirus sulle postazioni.
 - ◆ **Tutte le installazioni di rete** - installazioni di rete di **Agent**.
3. Per passare alla pagina con la tabella delle informazioni dettagliate su eventi sui **Server** adiacenti, nella tabella della sezione **Report di riepilogo** premere la cifra del numero di record relativi all'evento richiesto.
4. Inoltre, per passare alla tabella delle informazioni su eventi dei **Server** adiacenti, selezionare la voce corrispondente (v. passo 2) della sezione **Tabelle** del menu di gestione.
5. Per visualizzare le informazioni per un determinato periodo, indicare un periodo relativamente al giorno odierno nella lista a cascata o impostare un intervallo di tempo nella barra degli strumenti. Per impostare un intervallo di tempo, inserire le date richieste o premere sulle icone del calendario accanto ai campi di date. Per visualizzare le informazioni, premere il pulsante **Aggiorna**.
6. Se occorre salvare la tabella in modo da stamparla o da elaborarla in seguito, premere nella barra degli strumenti



Registra le informazioni in file CSV,



Registra le informazioni in file HTML,



Registra le informazioni in file XML,



Registra le informazioni in file PDF.



7.10.4. Utilizzo di un database unico da parte di diversi Server Dr.Web



Per poter utilizzare un database unico, tutti i **Server Dr.Web** devono essere della stessa versione.

Conviene aggiornare i **Server** all'interno di un cluster soltanto da pacchetti d'installazione. In questo caso, occorre arrestare tutti i **Server** e aggiornarli uno dopo l'altro. Non si deve utilizzare l'aggiornamento tramite il **Pannello di controllo** (passaggio ad una nuova revisione), in quanto in caso di utilizzo di database comune dopo l'aggiornamento del primo **Server** tutti gli altri **Server** non potranno continuare a funzionare e ad aggiornarsi.

Quando viene creata una rete antivirus con diversi **Server Dr.Web** e con un database unico, è necessario soddisfare i seguenti requisiti:

1. Su tutti i **Server** devono essere uguali le chiavi di cifratura `drwcsd.pub`, `drwcsd.pri`, i certificati `certificate.pem`, `private-key.pem` e la chiave di agent `agent.key`.
2. Nel file di configurazione del **Pannello di controllo** `webmin.conf` per tutti i **Server** deve essere impostato lo stesso nome DNS di **Server** nel parametro `ServerName`.
3. Sul server DNS in rete viene registrato il nome comune di cluster per ogni singolo **Server** e viene impostato il metodo di bilanciamento del carico.
4. Nei file di configurazione dei **Server** `drwcsd.conf` per tutti i **Server** deve essere definito un database esterno.
5. Nel calendario di server, i task **Purge Old Data**, **Prepare and send fiscal report periodic job**, **Backup sensitive data**, **Purge old stations**, **Purge expired stations**, **Purge unsent IS events** devono essere impostati solo su uno dei **Server** (su quello con maggiori prestazioni, se le configurazioni sono diverse).



Capitolo 8: Aggiornamento dei componenti di Dr.Web Enterprise Security Suite



Prima di cominciare ad aggiornare **Dr.Web Enterprise Security Suite** e singoli componenti, si consiglia vivamente di controllare se le impostazioni di accesso ad Internet del protocollo TCP/IP sono corrette. In particolare, il servizio DNS deve essere attivo ed avere le impostazioni corrette.

Si possono aggiornare i database dei virus e il software sia manualmente che attraverso il calendario di task del **Server** e dell'**Agent**.



Prima di aggiornare il software, si consiglia di configurare il repository, compreso l'accesso a **SAM Dr.Web** (v. p. [Configurazione generale del repository](#)).

8.1. Aggiornamento di Server Dr.Web e ripristino da copia di backup

Il **Pannello di controllo** fornisce le seguenti possibilità per la gestione del software **Server Dr.Web**:

- L'aggiornamento del software **Server** ad una delle versioni disponibili, caricate da **SAM** e memorizzate nel repository del **Server**. Le impostazioni dell'aggiornamento di repository da **SAM** sono descritte nella sezione [Gestione del repository di Server Dr.Web](#).
- Il rollback del software **Server** ad una copia di backup salvata. Le copie di backup del **Server** vengono create automaticamente quando si passa ad una versione nuova nella sezione **Aggiornamenti di Server Dr.Web** (passo 4 della procedura sottostante).



L'aggiornamento di **Server** all'interno della versione **10** inoltre può essere eseguito tramite il pacchetto di **Server**. La procedura viene descritta nella **Guida all'installazione**, nella sezione [Aggiornamento di Server Dr.Web per SO Windows®](#) o [Aggiornamento di Server Dr.Web per SO della famiglia UNIX®](#).

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

Quando il **Server** sotto un SO della famiglia UNIX viene aggiornato tramite il **Pannello di controllo**, la versione di **Server** in gestione pacchetti del SO non cambia.

Per gestire il software Server Dr.Web:

1. Selezionare la voce **Amministrazione** del menu principale del **Pannello di controllo**, nella finestra che si è aperta selezionare la voce del menu di gestione **Server Dr.Web**.
2. Per andare alla lista delle versioni di **Server**, eseguire una delle seguenti azioni:
 - Premere la versione corrente di **Server** nella finestra principale.
 - Premere il pulsante **Elenco delle versioni**.
3. Si apre la sezione **Aggiornamenti di Server Dr.Web** con un elenco degli aggiornamenti e dei backup di **Server** disponibili. In particolare:
 - Nella lista **Versione corrente** è indicata la versione di **Server** che viene utilizzata al momento. Nella sezione **Lista delle modifiche** è riportato un breve elenco di nuove funzioni e un elenco degli errori corretti in questa versione rispetto alla versione precedente dell'aggiornamento.



- Nella lista **Tutte le versioni** è riportata una lista degli aggiornamenti per questo **Server**, caricati da **SAM**. Nella sezione **Lista delle modifiche** è riportato un breve elenco di nuove funzioni e di errori corretti per ciascuno degli aggiornamenti.

Per la versione che corrisponde all'installazione iniziale di **Server** da pacchetto d'installazione, la sezione **Lista delle modifiche** è vuota.

- Nella lista **Copie di backup** è riportata una lista delle copie di backup salvate per questo **Server**. Nella sezione **Data** sono disponibili le informazioni sulla data del backup.
4. Per aggiornare il software **Server**, selezionare la casella di controllo di fronte alla versione di **Server** richiesta nella lista **Tutte le versioni** e premere il pulsante **Salva**.



Il software di **Server** può essere aggiornato soltanto ad una versione più recente rispetto a quella utilizzata al momento.

Nel corso dell'aggiornamento del **Server**, la versione corrente viene salvata come backup (viene messa nella sezione **Copie di backup**) e la versione a cui si aggiorna viene trasferita dalla sezione **Tutte le versioni** nella sezione **Versione corrente**.

I backup vengono salvati nella seguente cartella:

```
var → update_backup_<vecchia_versione>_<nuova_versione>.
```

Nel corso dell'aggiornamento viene creato o completato il file di log `var → dwupdater.log`.

5. Per eseguire il rollback del software **Server** ad una copia di backup salvata, selezionare la casella di controllo di fronte alla versione di **Server** richiesta nella lista **Copie di backup** e premere il pulsante **Salva**.

Nel corso del rollback del software **Server**, la copia di backup a cui si passa viene messa nella sezione **Versione corrente**.



8.2. Aggiornamento manuale dei componenti di Dr.Web Enterprise Security Suite




Controllo della disponibilità di aggiornamenti in SAM

Per controllare la disponibilità di aggiornamenti di prodotti Dr.Web Enterprise Security Suite sul server di aggiornamento:

1. Selezionare la voce **Amministrazione** del menu principale del **Pannello di controllo**, nella finestra che si è aperta selezionare la voce del menu di gestione **Stato del repository**.
2. Nella finestra che si è aperta vengono visualizzate le informazioni su tutti i componenti e inoltre la data dell'ultima revisione e lo stato corrente. Per controllare la disponibilità di aggiornamenti sul server **SAM**, premere il pulsante **Verifica aggiornamenti**.
3. Se il componente che viene verificato è obsoleto, verrà aggiornato automaticamente nel corso della verifica. L'aggiornamento avviene secondo le impostazioni del repository (v. p. [Gestione del repository di Server Dr.Web](#)).

Avvio del processo dell'aggiornamento del software postazione

Per avviare il processo dell'aggiornamento del software postazione:

1. Selezionare la voce **Rete antivirus** del 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. Nella barra degli strumenti premere il pulsante  **Gestione dei componenti**. Nel sottomenu selezionare la voce:
 - ◆  **Aggiorna i componenti falliti** per aggiornare soltanto i componenti di cui l'ultimo aggiornamento è terminato con errore e per resettare lo stato di errore,
 - ◆  **Aggiorna tutti i componenti** per avviare l'aggiornamento forzato di tutti i componenti, compresi quelli di cui l'ultima versione è già installata.




In caso della sincronizzazione forzata di tutti i componenti, sarà necessario riavviare la postazione. Seguire le indicazioni dell'**Agent**.

8.3. Aggiornamenti programmati

È possibile configurare un calendario di esecuzione di task sul **Server** per aggiornare il software a cadenze regolari (per maggiori informazioni sul calendario dei task consultare il p. [Configurazione del calendario di Server Dr.Web](#)).

Per configurare il calendario di esecuzione di un task di aggiornamento sul Server Dr.Web:

1. Selezionare la voce **Amministrazione** del menu principale del **Pannello di controllo**, nella finestra che si è aperta selezionare la voce del menu di gestione **Scheduler del Server Dr.Web**. Si apre una lista attuale dei task del **Server**.
2. Per aggiungere un task alla lista, nella barra degli strumenti premere il pulsante  **Crea task** Si apre la finestra di modifica del task.
3. Inserire nel campo **Nome** il nome del task sotto cui verrà visualizzato nel calendario.
4. Passare alla scheda **Azione** e selezionare dalla lista a cascata il tipo di task **Aggiornamento del repository**.



5. Nella lista che si è aperta, spuntare i flag di fronte ai componenti da aggiornare secondo questo task.
6. Passare alla scheda **Tempo** e selezionare dalla lista a cascata la periodicità dell'esecuzione del task, dopodiché configurare il tempo secondo la periodicità selezionata.
7. Per salvare le modifiche, premere il pulsante **Salva**.

8.4. Aggiornamento del repository di Server Dr.Web, non connesso a Internet

8.4.1. Copiatura del repository di un altro Server Dr.Web

Se un **Server** Dr.Web non è connesso a Internet, si può aggiornare il suo repository manualmente, copiando il repository di un altro **Server Dr.Web** aggiornato.



Questo metodo non è adatto per il passaggio a un'altra versione.

Per l'ottenimento di aggiornamenti del software antivirus, si consiglia la seguente sequenza di azioni:

1. Installare il software **Server Dr.Web** su un computer che ha l'accesso a Internet, come è descritto nella **Guida all'installazione**, p. [Installazione di Server Dr.Web](#).
2. Terminare entrambi i **Server Dr.Web**.
3. Per ottenere gli aggiornamenti del software antivirus, eseguire il **Server**, connesso a Internet, con la chiave `syncrepository`.

Esempio per il SO **Windows**:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Server" syncrepository
```

4. Sostituire completamente i contenuti della directory di repository del **Server** principale (operativo) con i contenuti dell'analogia directory di repository del **Server** connesso a Internet. Di solito è:
 - ◆ `var\repository` nel SO **Windows**,
 - ◆ `/var/drwcs/repository` nel SO **FreeBSD**,
 - ◆ `/var/opt/drwcs/repository` nel SO **Linux** e nel SO **Solaris**.



Se sul computer con il **Server Dr.Web** è installato un **Agent** con il componente di auto-protezione **Dr.Web Self-protection** attivata, prima di aggiornare il repository, è necessario disattivare questo componente attraverso le impostazioni di **Agent**.

5. Se il **Server** principale funziona sotto un SO della famiglia UNIX, sul repository copiato è necessario impostare permessi dell'utente creato/selezionato nel corso dell'installazione di questo **Server**.
6. Eseguire sul **Server** principale il comando:

```
drwcsd rerepository
```

Nel SO **Windows** il comando può essere eseguito sia da *riga di comando*:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Server" rerepository
```



che dal menu Start → Programmi → Server Dr.Web → Gestione del server → Ricarica il repository.

7. Avviare il **Server** principale.



Se durante l'aggiornamento del repository è stato disattivato il componente di autoprotezione **Dr.Web Self-protection**, si consiglia di ripristinare il funzionamento di questo componente.

8.4.2. Caricamento del repository da SAM

Se un **Server Dr.Web** non è connesso a Internet, si può aggiornare il suo repository manualmente, importando un repository caricato da **SAM**.

Per il caricamento del repository di **Server Dr.Web** da **SAM** viene fornita un'utility standard **Loader di repository Dr.Web**.

Caratteristiche dell'utilizzo

- ◆ Per caricare il repository da **SAM**, occorre la chiave di licenza di **Dr.Web Enterprise Security Suite** o il suo hash MD5 che può essere visualizzato nel **Pannello di controllo**, nella sezione **Amministrazione** → **Gestione licenze**.
- ◆ **Il Loader di repository Dr.Web** è disponibile nelle seguenti versioni:
 - [versione dell'utility con interfaccia grafica](#) (soltanto nella versione per il SO Windows),
 - [versione console](#) dell'utility.
- ◆ Per il caricamento del repository da **SAM**, è possibile utilizzare un server proxy.



8.4.2.1. Utility con interfaccia grafica

La versione con interfaccia grafica dell'utility **Loader di repository Dr.Web** può essere scaricata tramite il **Pannello di controllo**, nella sezione **Amministrazione** → **Utility**. Questa versione dell'utility può essere eseguita su ogni computer SO Windows che ha l'accesso a Internet. Il file eseguibile è `drwreploder-gui-<versione>.exe`.

Per caricare il repository tramite la versione con interfaccia grafica di Loader di repository Dr.Web:

1. Avviare la versione con interfaccia grafica di **Loader di repository Dr.Web**.
2. Nella finestra principale dell'utility, impostare i seguenti parametri:
 - a) **Chiave di licenza o MD5 della chiave** - specificare il file della chiave di licenza **Dr.Web**. Per farlo, premere **Sfoglia** e selezionare il file della chiave di licenza attuale. Invece del file della chiave di licenza, si può indicare soltanto il suo hash MD5 che può essere visualizzato nel **Pannello di controllo**, nella sezione **Amministrazione** → **Gestione licenze**.
 - b) **Cartella per il download** - impostare la directory in cui viene caricato il repository.
 - c) Dalla lista **Modalità** selezionare una delle modalità di caricamento degli aggiornamenti:
 - **Carica repository** - il repository viene caricato nel formato di repository di **Server**. I file caricati possono essere importati direttamente tramite il **Pannello di controllo** come gli aggiornamenti di repository di **Server**.
 - **Sincronizza mirror degli aggiornamenti** - il repository viene caricato nel formato della zona degli aggiornamenti di **SAM**. I file caricati possono essere memorizzati sul mirror degli aggiornamenti nella rete locale. In seguito i **Server** possono essere configurati per ricevere aggiornamenti direttamente da questo mirror degli aggiornamenti, che contiene l'ultima versione del repository, invece di riceverli dai server di **SAM**.
 - d) Spuntare il flag **Archivia il repository** affinché il repository venga automaticamente compresso in un archivio .zip. Questa opzione permette di ottenere un file di archivio pronto per la successiva importazione del repository sul **Server** tramite il **Pannello di controllo**, dalla sezione **Amministrazione** → **Contenuti del repository**.
3. Se si vogliono modificare le impostazioni avanzate di connessione a **SAM** e di caricamento di aggiornamenti, premere **Avanzate**. Nella finestra di configurazione che si è aperta, sono disponibili le seguenti schede:
 - a) Nella scheda **Prodotti** si può modificare la lista dei prodotti da caricare. Nella finestra delle impostazioni che si è aperta, viene riportata la lista di tutti i prodotti di repository disponibili per il caricamento da **SAM**:
 - Per aggiornare la lista dei prodotti disponibili attualmente in **SAM**, premere il pulsante **Aggiorna**.
 - Spuntare i flag di fronte ai prodotti che si vogliono caricare da **SAM** oppure il flag nell'intestazione della tabella per selezionare tutti i prodotti nella lista.
 - b) Nella scheda **SAM Dr.Web**, è possibile configurare parametri dei server di aggiornamento:
 - L'ordine dei server **SAM** nella lista determina l'ordine in cui l'utility si connette ad essi per il caricamento del repository. Per modificare l'ordine dei server **SAM**, utilizzare i pulsanti **In alto** e **In basso**.
 - Per aggiungere un server **SAM** alla lista dei server utilizzati per il caricamento, inserire l'indirizzo del server **SAM** nel campo sopra la lista dei server e premere il pulsante **Aggiungi**.
 - Per cancellare un server **SAM** dalla lista dei server utilizzati, selezionare dalla lista il server da cancellare e premere il pulsante **Rimuovi**.
 - Nel campo **URI di base** viene indicata la directory sui server **SAM** che contiene gli aggiornamenti dei prodotti **Dr.Web**.



- Dalla lista a cascata **Protocollo** selezionare il tipo di protocollo per la ricezione degli aggiornamenti dai server di aggiornamenti. Per tutti i protocolli il caricamento degli aggiornamenti viene eseguito secondo le impostazioni della lista dei server di **SAM**.
 - Dalla lista a cascata **Certificati validi** selezionare il tipo di certificato SSL che verrà accettato automaticamente. Questa impostazione si usa solo per i protocolli sicuri che supportano crittografia.
 - **Nome utente e Password** - le credenziali dell'utente per l'autenticazione sul server degli aggiornamenti, se il server richiede l'autenticazione.
 - Spuntare il flag **Utilizza CDN** per consentire l'utilizzo di Content Delivery Network per il caricamento del repository.
- c) Nella scheda **Proxy** è possibile configurare le impostazioni di connessione a **SAM** attraverso un server proxy:
- **Indirizzo del server proxy e Porta** - rispettivamente l'indirizzo di rete e il numero di porta del server proxy in uso.
 - **Nome utente e Password** - parametri per l'autenticazione sul server proxy, se il server proxy in uso richiede l'autenticazione.
- d) Nella scheda **Scheduler** è possibile configurare un calendario di aggiornamenti periodici. Per eseguire il calendario, si usa lo scheduler di task del SO Windows. In questo caso non c'è la necessità di avviare l'utility manualmente, anzi il repository verrà caricato automaticamente tra gli intervalli di tempo impostati.
- e) Nella scheda **Log** si possono configurare i parametri di registrazione del log del caricamento degli aggiornamenti.
- Premere **OK** per accettare le modifiche fatte e per tornare alla finestra principale di **Loader di repository Dr.Web**.
4. Dopo aver configurato tutti i parametri, premere il pulsante **Carica** nella finestra principale di **Loader di repository Dr.Web** per avviare la connessione a **SAM** e il caricamento del repository.

8.4.2.2. Versione console dell'utility

La versione console dell'utility **Loader di repository Dr.Web** si trova nella sottodirectory `bin` della directory di installazione di **Server Dr.Web**. Questa versione dell'utility può essere eseguita soltanto da questa directory di **Server**. Il file eseguibile è `drwreploder`.

Possibili varianti dell'utilizzo

Procedura consigliata

1. Caricare da **SAM** il repository di **Server** attraverso l'utility **Loader di repository Dr.Web**. Per il caricamento, utilizzare l'opzione `--archive` per creare un archivio di repository.
2. Importare il repository sul **Server** tramite il **Pannello di controllo**, dalla sezione **Amministrazione** → [Contenuti del repository](#).

Procedura con l'importazione manuale

1. Caricare da **SAM** il repository di **Server** attraverso l'utility **Loader di repository Dr.Web** senza utilizzare la chiave `--archive`. Per il caricamento, utilizzare l'opzione `--path <argomento>` per caricare il repository nella directory specificata.
2. Per importare il repository, copiare i suoi contenuti, che si trovano nella directory specificata nel parametro `<argomento>`, nella directory `/repository` della directory d'installazione di **Server**, sostituendo i file.
3. Ricaricare il repository dal **Pannello di controllo**, dalla sezione **Amministrazione** → [Stato del repository](#).



Opzioni valide

- ◆ `--help` – visualizza la guida sulle opzioni.
- ◆ `--show-products` – mostra l'elenco dei prodotti in **SAM**.
- ◆ `--path <argomento>` – carica il repository da **SAM** nella directory specificata nel parametro `<argomento>`.
- ◆ `--etc <argomento>` – percorso della directory `etc` di **Server** (si usa per cercare certificati radice e per aggiornare chiavi pubbliche).
- ◆ `--archive` – comprimi il repository in archivio.
- ◆ `--key <argomento>` – percorso del file della chiave di licenza (va specificata la chiave o il suo hash MD5).
- ◆ `--key-md5 <argomento>` – hash MD5 della chiave di licenza (va specificata la chiave o il suo hash MD5).
- ◆ `--product <argomento>` – il prodotto che viene aggiornato. Di default, viene caricato l'intero repository.
- ◆ `--only-bases` – carica soltanto i database dei virus.
- ◆ `--update-url <argomento>` – la directory sui server **SAM** che contiene gli aggiornamenti dei prodotti **Dr.Web** (è consigliabile lasciare il valore predefinito).
- ◆ `--servers <argomento>` – gli indirizzi dei server **SAM** (è consigliabile lasciare il valore predefinito).
- ◆ `--prohibit-cdn` – proibisci l'utilizzo di CDN per il caricamento degli aggiornamenti (di default l'opzione è disattivata, cioè l'utilizzo di CDN è consentito).
- ◆ `--prohibit-ssl` – utilizza il protocollo non sicuro HTTP invece di HTTPS (di default l'opzione è disattivata, cioè viene utilizzato HTTPS).
- ◆ `--cert-mode [<argomento>]` – accetta automaticamente certificati HTTPS.

`<argomento>` può essere uno dei valori:

- `any` – accetta tutti i certificati,
- `valid` – accetta soltanto i certificati verificati,
- `drweb` – accetta soltanto i certificati **Dr.Web**.

Di default, viene utilizzato il valore `drweb`.

- ◆ `--proxy-host <argomento>` – server proxy nel formato `<server>[:<porta>]`.
- ◆ `--proxy-auth <argomento>` – informazioni per l'autenticazione sul server proxy: nome utente e password nel formato `<utente>[:<password>]`.
- ◆ `--strict` – interrompi il caricamento se si verifica un errore.
- ◆ `--log <argomento>` – crea un log di caricamento del repository nel formato dei log di **Server** e salvalo nella directory specificata nel parametro `<argomento>`.

Esempi di utilizzo

1. Crea un archivio da importare con tutti i prodotti:

```
drwreloader.exe --path=C:\Temp\repository.zip --archive --key "C:\Program Files
\DrWeb Server\etc\agent.key" --etc "C:\Program Files\DrWeb Server\etc"
```

2. Crea un archivio da importare con i database dei virus:

```
drwreloader.exe --path=C:\Temp\repository.zip --archive --key "C:\Program Files
\DrWeb Server\etc\agent.key" --only-bases --etc "C:\Program Files\DrWeb Server
\etc"
```



3. Crea un archivio da importare soltanto con il **Server**:

```
drwreploder.exe --path=C:\Temp\repository.zip --archive --key "C:\Program Files
\DrWeb Server\etc\agent.key" --product=20-drwcs --etc "C:\Program Files\DrWeb
Server\etc"
```

8.5. Limitazione degli aggiornamenti delle postazioni

Tramite il **Pannello di controllo**, è possibile configurare la modalità dell'aggiornamento dei componenti di **Dr.Web Enterprise Security Suite** su postazioni protette per determinati intervalli di tempo.

Per configurare la modalità dell'aggiornamento delle postazioni, eseguire le seguenti azioni:

1. Selezionare la voce **Rete antivirus** del menu principale, nella finestra che si è aperta, nella lista gerarchica fare clic sul nome di una postazione o di un gruppo. Nel [menu di gestione](#) selezionare la voce **Limitazioni degli aggiornamenti**.
2. Dalla lista a cascata **Limitazione degli aggiornamenti** selezionare la modalità di limitazione:
 - **Senza limitazioni** - per non porre restrizioni sulla distribuzione degli aggiornamenti su postazioni.
 - **Proibisci ogni aggiornamento** - per proibire la distribuzione di tutti gli aggiornamenti su postazioni negli intervalli di tempo definiti più in basso nella tabella **Calendario dell'aggiornamento delle postazioni**.
 - **Aggiorna soltanto i database** - per proibire la distribuzione soltanto degli aggiornamenti dei moduli di programma negli intervalli di tempo definiti più in basso nella tabella **Calendario dell'aggiornamento delle postazioni**. I database dei virus verranno aggiornati come di solito in modalità normale.
3. Spuntare il flag **Limita il traffico dati degli aggiornamenti** per limitare l'entità di traffico dati durante la trasmissione di aggiornamenti tra il **Server** e gli **Agent**. Nel campo **Velocità di trasmissione massima (KB/s)** impostare un valore della velocità massima di trasmissione di aggiornamenti.

Per maggiori informazioni v. p. [Limitazione del traffico dati degli aggiornamenti](#).

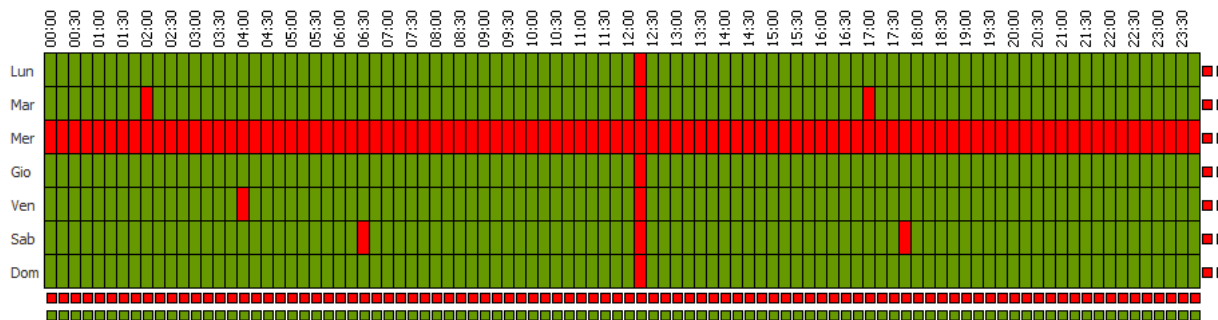
4. Spuntare il flag **Ricevi tutti gli aggiornamenti recenti** affinché la postazione riceva tutti gli aggiornamenti dei componenti a prescindere dalle limitazioni impostate nella sezione [Configurazione dettagliata del repository](#).

Se il flag è tolto, la postazione riceverà soltanto gli aggiornamenti marcati come gli aggiornamenti attuali da distribuire.

5. Nella tabella **Calendario dell'aggiornamento delle postazioni** la modalità di aggiornamento viene configurata con la seguente classificazione di colore:

- colore verde - l'aggiornamento è consentito;
- colore rosso - l'aggiornamento è proibito.


La limitazione viene configurata separatamente per ogni 15 minuti di ogni giorno della settimana.





Per modificare la modalità di aggiornamento, fare clic sul relativo blocco della tabella:

- Per modificare la modalità di una riga intera (un giorno intero), fare clic sul marcatore del colore appropriato a destra della riga richiesta della tabella.
 - Per modificare la modalità di una colonna intera (un intervallo di 15 minuti per tutti i giorni della settimana), fare clic sul marcatore del colore appropriato sotto la colonna richiesta della tabella.
6. Dopo aver apportato delle modifiche, premere il pulsante **Salva** per accettare le modifiche apportate.


Nella barra degli strumenti sono disponibili le seguenti opzioni:

 **Resetta tutti i parametri ai valori iniziali** - per ripristinare tutti i parametri di questa sezione ai valori che avevano prima della modifica corrente (ultimi valori salvati).


 **Resetta tutti i parametri ai valori default** - per ripristinare tutti i parametri di questa sezione ai valori di default.

 **Propaga queste impostazioni verso un altro oggetto** - per copiare le impostazioni da questa sezione nelle impostazioni di un'altra postazione, di un gruppo o di diversi gruppi e postazioni.

 **Imposta l'ereditarietà delle impostazioni dal gruppo primario** - per eliminare le impostazioni individuali delle postazioni e per impostare l'ereditarietà delle impostazioni di questa sezione dal gruppo primario.

 **Copia le impostazioni dal gruppo primario e impostale come individuali** - per copiare le impostazioni di questa sezione dal gruppo primario e per assegnarle alle postazioni selezionate. In questo caso, l'ereditarietà non viene impostata e le impostazioni della postazione vengono considerate individuali.

 **Esporta le impostazioni da questa sezione in file** - per salvare tutte le impostazioni da questa sezione in un file di apposito formato.

 **Importa le impostazioni in questa sezione da file** - per sostituire tutte le impostazioni in questa sezione con le impostazioni salvate in un file dell'apposito formato.

8.6. Aggiornamento di Agent Dr.Web mobile

Se il computer, notebook o dispositivo mobile dell'utente non avrà la connessione con il **Server Dr.Web** per lungo tempo, per la ricezione tempestiva di aggiornamenti dai server **SAM Dr.Web**, si consiglia di impostare la modalità di funzionamento mobile dell'**Agent Dr.Web** sulla postazione.

Nella modalità mobile l'**Agent** cerca di connettersi al **Server**, fa tre tentativi e se non è riuscito, esegue l'aggiornamento HTTP. I tentativi di ricerca del **Server** si susseguono ininterrottamente a intervallo di circa un minuto.



L'attivazione della modalità mobile sarà disponibile nelle impostazioni di **Agent** a condizione che nei permessi della postazione sia consentita la modalità mobile dell'utilizzo di **SAM Dr.Web** (v. p. [Configurazione dei permessi degli utenti](#)).



Mentre l'**Agent** funziona nella modalità mobile, l'**Agent** non è connesso al **Server Dr.Web**. Tutte le modifiche impostate sul **Server** per tale postazione entreranno in vigore non appena la modalità mobile di **Agent** verrà disattivata e l'**Agent** si riconnetterà al **Server**.

Nella modalità mobile vengono aggiornati soltanto i database dei virus.

Le impostazioni della modalità mobile di funzionamento sul lato **Agent** sono descritte nel **Manuale dell'utente**.



Capitolo 9: Configurazione dei componenti aggiuntivi

9.1. Server proxy

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

L'obiettivo principale del **Server proxy** è di assicurare la comunicazione del **Server Dr.Web** e degli **Agent Dr.Web** nel caso non sia possibile organizzare l'accesso diretto (per esempio, se il **Server Dr.Web** e gli **Agent Dr.Web** si trovano in reti diverse senza l'instradamento dei pacchetti tra di esse).



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

Funzioni principali

Il server proxy svolge le seguenti funzioni:

1. È in ascolto e accetta connessioni secondo le impostazioni di protocollo e porta.
2. Traslazione dei protocolli (sono supportati i protocolli TCP/IP).
3. Trasmissione dei dati tra il **Server Dr.Web** e gli **Agent Dr.Web** secondo le impostazioni del **Server proxy**.
4. Memorizzazione nella cache degli aggiornamenti dell'**Agent** e del pacchetto antivirus, trasmessi dal **Server**. Se gli aggiornamenti vengono rilasciati dalla cache del **Server proxy**, questo permette di:
 - ◆ diminuire il traffico di rete,
 - ◆ diminuire il tempo di ricevimento degli aggiornamenti da parte degli **Agent**.



È possibile creare una gerarchia dei **server proxy**.

Uno schema generale di rete antivirus con utilizzo di **server proxy** è riportato in [immagine 9-1](#).

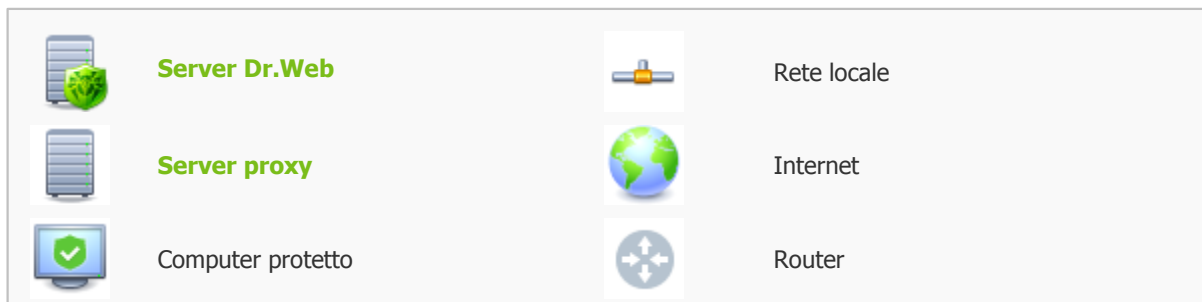
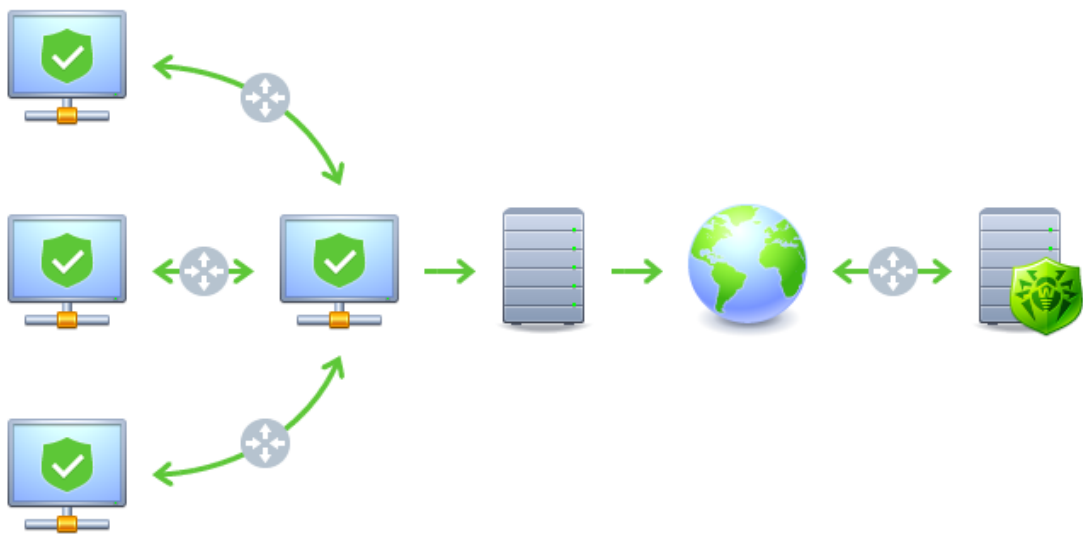


Immagine 9-1. Schema della rete antivirus con utilizzo del Server proxy

Principio di funzionamento

In caso di utilizzo del Server proxy, viene eseguita la seguente sequenza di azioni:

1. Se nell'**Agent** non è definito l'indirizzo del **Server**, l'**Agent** spedisce una richiesta multicast in conformità con il protocollo della rete in cui si trova.
2. Se il **Server proxy** è configurato per la traslazione di connessioni (il parametro `discovery="yes"`), all'**Agent** viene inviato un avviso di disponibilità di un **Server proxy** operativo.
3. L'**Agent** imposta i parametri del **Server proxy** ottenuti come i parametri del **Server Dr.Web**. La comunicazione successiva avviene in un modo trasparente per l'**Agent**.
4. Secondo i parametri del file di configurazione, il **Server proxy** è in ascolto sulle porte impostate per le connessioni in ingresso attraverso i protocolli indicati.
5. Per ciascuna connessione in ingresso da un **Agent**, il **Proxy** stabilisce una connessione con il **Server Dr.Web**.

Algoritmo di reindirizzamento se è disponibile una lista dei Server Dr.Web:

1. Il **Server proxy** carica nella memoria operativa una lista dei **Server Dr.Web** dal file di configurazione `drwcsd-proxy.xml` (v. documento **Allegati**, [Allegato G4](#)).
2. L'**Agent Dr.Web** si connette al **Server proxy**.
3. Il **Server proxy** reindirizza l'**Agent Dr.Web** sul primo **Server Dr.Web** dalla lista nella memoria operativa.



- Il **Server proxy** volta la lista caricata nella memoria operativa e sposta questo **Server Dr.Web** dal primo elemento della lista alla fine della lista.



Il **Server proxy** non memorizza nel suo file di configurazione la sequenza modificata dei **Server**. Quando il **Server proxy** viene riavviato, la lista dei **Server Dr.Web** viene caricata nella memoria operativa nella sua versione originale, conservata nel file di configurazione.

- Quando un altro **Agent** si connette al **Server proxy**, la procedura si ripete dal passo 2.
- Se un **Server Dr.Web** si sconnette dalla rete antivirus (per esempio, in caso di spegnimento o negazione del servizio), l'**Agent** si riconnette al **Server proxy** e la procedura si ripete dal passo 2.



Uno **scanner di rete**, avviato su un computer di una rete esterna relativamente agli **Agent**, non può rilevare gli **Agent** installati.



Se il flag **Sostituisci i nomi NetBIOS** è selezionato, e nella rete antivirus viene utilizzato un **Server proxy**, per tutte le postazioni connesse al **Server** attraverso il **Server proxy** nel **Pannello di controllo** come i nomi di postazioni verrà visualizzato il nome del computer su cui è installato il **Server proxy**.

Cifratura e compressione del traffico dati

Il **Server proxy** supporta la compressione del traffico dati. Le informazioni trasmesse vengono processate a prescindere da quello se il traffico è compresso o meno.

Il **Server proxy** non supporta la cifratura. Analizza le informazioni inviate e se il traffico dati tra il **Server Dr.Web** e l'**Agent** è cifrato, il **Server proxy** passa alla modalità trasparente, cioè trasmette tutto il traffico dati tra il **Server** e l'**Agent** senza alcuna analisi dei dati.



Se è attivata la modalità della cifratura dei dati trasmessi tra l'**Agent** e il **Server**, gli aggiornamenti non vengono salvati nella cache di **Server proxy**.

Memorizzazione nella cache

Il **Server proxy** supporta la memorizzazione del traffico dati nella cache.

I prodotti vengono memorizzati nella cache per revisione. Ciascuna revisione si trova in una directory separata. Nella directory per ciascuna revisione successiva sono disponibili gli *hard link* (*hard links*) ai file esistenti delle revisioni precedenti e le versioni originali dei file modificati. In questo modo, i file per ciascuna versione vengono conservati sul disco rigido in una copia unica, in tutte le directory di revisioni successive vengono riportati soltanto i link ai file invariati.

I parametri che vengono impostati nel file di configurazione permettono di configurare le seguenti azioni per la memorizzazione nella cache:

- Eliminare periodicamente le revisioni obsolete. Di default, una volta all'ora.
- Conservare soltanto le revisioni recenti. Tutte le altre revisioni, in quanto precedenti, sono considerate obsolete e vengono eliminate. Di default, vengono conservate le ultime tre revisioni.
- Scaricare periodicamente dalla memoria i file *memory mapped* non utilizzati. Di default, ogni 10 minuti.



Impostazioni

Il **Server proxy** non ha l'interfaccia grafica. Le impostazioni vengono definite tramite il file di configurazione. Il formato del file di configurazione del **Server proxy** è riportato in documento **Allegati**, p. [Allegato G4](#).



La gestione delle impostazioni (modifica del file di configurazione) del **Server proxy** può essere effettuata soltanto da un utente con i permessi dell'amministratore di tale computer.

Affinché il **Server proxy** funzioni in modo corretto sotto i SO della famiglia Linux, dopo il riavvio del computer occorre eseguire la configurazione di sistema della rete senza utilizzare Network Manager.

Avvio e arresto

Nel SO Windows il **Server proxy** viene eseguito e terminato tramite gli strumenti standard attraverso il **Pannello di controllo** → **Amministrazione** → **Servizi** → nella lista dei servizi fare doppio clic su **drwcsd-proxy** e nella finestra che si è aperta selezionare l'azione necessaria.

Sotto i SO della famiglia UNIX, il **Server proxy** viene eseguito e terminato tramite i comandi `start` e `stop` applicati agli script creati nel corso dell'installazione del **Server proxy** (v. **Guida all'installazione**, p. [Installazione del Server proxy](#)).

Inoltre per avviare il **Server proxy** nei SO Windows e nei SO della famiglia UNIX, si può avviare il file eseguibile `drwcsd-proxy` con i parametri corrispondenti (v. [Allegato H8. Server proxy](#)).

9.2. NAP Validator

Informazioni generali

Microsoft® Network Access Protection (NAP) è una piattaforma di criteri, incorporata nei sistemi operativi Windows, che provvede a una maggiore sicurezza della rete. La sicurezza è dovuta al fatto che vengono soddisfatti i requisiti di operatività dei sistemi della rete.

Utilizzando la tecnologia NAP, si possono creare criteri di operatività personalizzati per valutare lo stato di un computer. Le valutazioni ottenute vengono analizzate nei seguenti casi:

- ◆ prima di consentire l'accesso o l'interazione,
- ◆ per aggiornare in automatico computer che corrispondono ai requisiti per provvedere alla loro compatibilità continua,
- ◆ per portare alla conformità computer che non corrispondono ai requisiti per farli corrispondere ai requisiti stabiliti.

Una descrizione dettagliata della tecnologia NAP è disponibile sul [sito di Microsoft](#).

Utilizzo di NAP in Dr.Web Enterprise Security Suite

Dr.Web Enterprise Security Suite permette di utilizzare la tecnologia NAP per controllare l'operatività del software antivirus di postazioni protette. Il componente utilizzato per questo fine è **Dr.Web NAP Validator**.

Per controllare l'operatività, vengono utilizzati i seguenti strumenti:

- ◆ Server NAP di controllo di operatività installato e configurato.



- ◆ **Dr.Web NAP Validator** è uno strumento per valutare l'operatività del software antivirus del sistema protetto (System Health Validator - SHV) sulla base dei criteri personalizzati **Dr.Web**. Viene installato sul computer insieme al server NAP.
- ◆ Agent di operatività del sistema (System Health Agent - SHA). Viene installato automaticamente insieme al software **Agent Dr.Web** su postazione.
- ◆ **Server Dr.Web** funge da un server di correzioni che provvede all'operatività del software antivirus di postazioni.

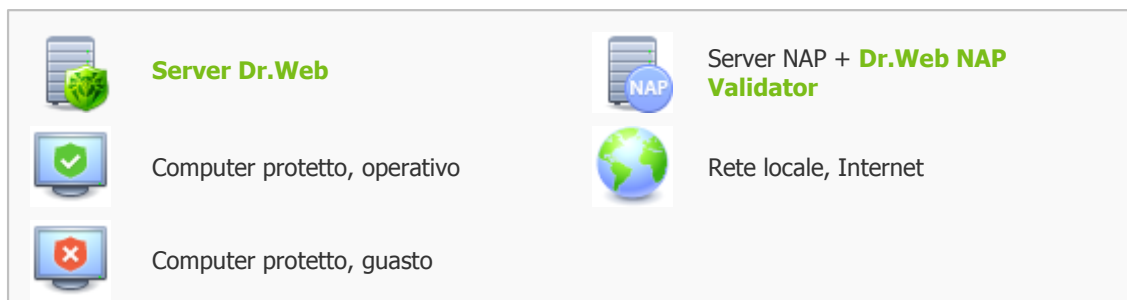


Immagine 9-2. Schema della rete antivirus con utilizzo di NAP

La procedura di controllo viene eseguita nel seguente modo:

1. Il processo di controllo viene attivato quando vengono impostate le configurazioni corrispondenti di **Agent** (v. p. [Configurazione di Agent Dr.Web](#)).
2. SHA su postazione si connette al componente **Dr.Web NAP Validator** installato sul server NAP.
3. **Dr.Web NAP Validator** controlla i criteri di operatività (v. [sotto](#)). Il controllo dei criteri è un processo in cui **NAP Validator** valuta gli strumenti antivirus dal punto di vista della conformità alle regole stabilite da esso e determina la categoria dello stato attuale del sistema:
 - ◆ le postazioni, che hanno superato il controllo della conformità agli elementi dei criteri, vengono considerate operative e vengono ammesse all'operazione a piena funzionalità nella rete.



- ◆ le postazioni, che non soddisfano almeno uno degli elementi dei criteri, vengono considerate non operative. Tali postazioni possono accedere soltanto al **Server Dr.Web** e vengono isolate dal resto della rete. L'operatività della postazione viene ripristinata tramite il **Server**, dopodiché la procedura di controllo per la postazione viene rifatta.

Requisiti di operatività:

1. Stato operativo dell'agent (è avviato e funziona).
2. Database dei virus aggiornati (i database coincidono con i database sul server).

Configurazione di NAP Validator

Dopo l'installazione di **Dr.Web NAP Validator** (v. **Guida all'installazione**, p. [Installazione di NAP Validator](#)), è necessario eseguire le seguenti azioni sul computer su cui è installato il server NAP:

1. Aprire il componente di configurazione del server NAP (comando `nps.msc`).
2. Nella sezione **Policies** selezionare la sottovoce **Health Policies**.
3. Nella finestra che si è aperta, selezionare le proprietà di elementi:
 - ◆ **NAP DHCP Compliant**. Nella finestra delle impostazioni, spuntare il flag **Dr.Web System Health Validator** che comanda l'utilizzo dei criteri del componente **Dr.Web NAP Validator**. Dalla lista a cascata selezionare la voce **Client passed all SHV checks** affinché venga riconosciuta operativa una postazione se corrisponde a tutti gli elementi del criterio impostato.
 - ◆ **NAP DHCP Noncompliant**. Nella finestra delle impostazioni, spuntare il flag **Dr.Web System Health Validator** che comanda l'utilizzo dei criteri del componente **Dr.Web NAP Validator**. Dalla lista a cascata selezionare la voce **Client fail one or more SHV checks** affinché venga riconosciuta non operativa una postazione se non corrisponde almeno ad uno degli elementi del criterio impostato.



Indice analitico

A

- account 68
- Agent
 - aggiornamento 195
 - funzioni 29
 - impostazioni 104
 - interfaccia 29
 - modalità mobile 195
- aggiornamento
 - Agent 195
 - Dr.Web Enterprise Security Suite 186
 - forzato 188
 - limitazione 194
 - manuale 188
 - modalità mobile 195
 - rete antivirus 183
 - secondo il calendario 188
- aggiornamento forzato 188
- aggiornamento manuale 188
- amministratori
 - permessi 68
- approvazione delle postazioni 86
- autenticazione automatica 42
- autenticazione, Pannello di controllo 42
- avvio
 - Server Dr.Web 26, 28
- avvisi
 - impostazioni 158

C

- calendario
 - degli aggiornamenti 188
 - server 147
- cartella di server, contenuti 24
- chiavi 21
 - demo 22
 - ottenimento 21
 - vedi anche registrazione 21
- chiavi demo 22
- cifratura
 - traffico 134
- componenti
 - rete antivirus 54
 - sincronizzazione 188
- compressione traffico 134

- concessione delle licenze 21
- configurazione
 - Agent 104
 - server antivirus 132
- contenuti del pacchetto 20
- creazione
 - gruppi 78

D

- database
 - impostazioni 140
- directory di server, contenuti 26

F

- funzioni
 - Agent 29
 - Server Dr.Web 23

G

- gruppi 75
 - aggiunzione di postazioni 80
 - impostazioni 82
 - impostazioni, copiatura 85
 - impostazioni, ereditarietà 83
 - primari 83
 - rimozione di postazioni 80
- gruppi predefiniti 75
- gruppi primari 83

I

- icone
 - lista gerarchica 36
 - scanner di rete 46
- impostazioni
 - Agent 104
 - copiatura 85
 - server antivirus 132
- interfaccia
 - server antivirus 24, 26

L

- limitazione degli aggiornamenti 194
- lingua
 - Pannello di controllo 40, 70
- loader di repository 190
- log del Server 23



Indice analitico

M

- messaggi
 - formato del logotipo 129
 - invio all'utente 128
- modalità mobile dell'Agent 195

N

- NAP Validator 200
 - impostazioni 202
- nuovo arrivo 86, 104

P

- pacchetto 20
- pacchetto principale di Server Dr.Web
 - contenuti 20
- pacchetto supplementare di Server Dr.Web
 - contenuti 20
- Pannello di controllo
 - barra degli strumenti 36
 - barra delle proprietà 39
 - barra di ricerca 32
 - descrizione 30
 - lista gerarchica 35
 - menu principale 31
- permessi
 - amministratori 68
- postazione
 - aggiunzione a gruppo 80
 - approvazione 86
 - gestione 86
 - impostazioni, copiatura 85
 - impostazioni, ereditarietà 83
 - non confermata 86
 - nuovo arrivo 86
 - rimozione 87
 - rimozione da gruppo 80
 - ripristino 87
 - scansione 96, 111
 - statistiche 120
- postazioni non confermate 86
- privilegi
 - amministratori 68

Q

- quarantena 125

R

- recupero della postazione 87
- registrazione
 - delle postazioni sul server 86
 - di prodotto Dr.Web 21
- relazioni tra i server
 - impostazioni 179
 - tipi 177
- repository
 - editor semplificato 166
 - parametri generali 165
- requisiti di sistema 16
- rete antivirus 177
 - aggiornamenti 183
 - componenti 54
 - configurazione delle relazioni 179
 - eventi dei virus 183
 - struttura 54, 177
- rimozione
 - della postazione 87
 - gruppi 78
 - postazione, da gruppo 80

S

- SAM
 - v. inoltre aggiornamento manuale 188
- scanner
 - antivirus 111
 - di rete 44
- scanner antivirus 111
- scansione
 - automatica 96
 - manuale 111
- scansione antivirus 111
- Scheduler
 - Server 147
- server antivirus
 - avvio 26, 28
 - calendario 147
 - configurazione delle relazioni 179
 - contenuti di cartella 24
 - contenuti di directory 26
 - impostazioni 132
 - interfaccia 24, 26
 - log 23



Indice analitico

- server antivirus
 - tipi di relazioni 177
- Server Dr.Web
 - avvio 26, 28
 - calendario 147
 - configurazione delle relazioni 179
 - contenuti di cartella 24
 - contenuti di directory 26
 - impostazioni 132
 - interfaccia 24, 26
 - log 23
 - task 23
 - tipi di relazioni 177
- server proxy
 - avvio, arresto 200
 - funzioni 197
- sincronizzazione, componenti 188
- statistiche
 - della postazione 120

T

- traffico
 - cifratura 134
 - compressione 134
 - contenuti 56

