



Dr.WEB

Enterprise Security Suite

Manuale dell'amministratore



© Doctor Web, 2024. Tutti i diritti riservati

Il presente documento ha carattere puramente informativo e indicativo nei confronti del software della famiglia Dr.Web in esso specificato. Il presente documento non costituisce una base per conclusioni esaustive sulla presenza o assenza di qualsiasi parametro funzionale e/o tecnico nel software della famiglia Dr.Web e non può essere utilizzato per determinare la conformità del software della famiglia Dr.Web a qualsiasi requisito, specifica tecnica e/o parametro, nonché ad altri documenti di terze parti.

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

Marchi

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

Disclaimer

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

Dr.Web Enterprise Security Suite
Versione 13.0
Manuale dell'amministratore
07/03/2024

Doctor Web, Sede centrale in Russia

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

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

Telefono +7 (495) 789-45-87

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

Doctor Web

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

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

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

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

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



Sommario

Capitolo 1: Introduzione	9
1.1. Scopo del documento	9
1.2. Segni convenzionali e abbreviazioni	10
Capitolo 2: Dr.Web Enterprise Security Suite	12
2.1. Sul prodotto	12
2.2. Contenuto del pacchetto	22
Capitolo 3: Concessione delle licenze	25
3.1. Caratteristiche delle licenze	26
3.2. Distribuzione delle licenze attraverso le relazioni tra i server	27
3.3. Aggiornamento automatico delle licenze	30
Capitolo 4: Introduzione all'uso	34
4.1. Creazione della rete antivirus	34
4.2. Configurazione delle connessioni di rete	38
4.2.1. Connessioni dirette	39
4.2.2. Servizio di rilevamento di Server Dr.Web	40
4.2.3. Utilizzo del protocollo SRV	41
4.3. Connessione sicura	41
4.3.1. Cifratura e compressione del traffico dati	41
4.3.2. Strumenti per la connessione sicura	48
4.3.3. Connessione dei client al Server Dr.Web	50
4.4. Integrazione di Dr.Web Enterprise Security Suite con Active Directory	52
Capitolo 5: Componenti della rete antivirus e la loro interfaccia	54
5.1. Server Dr.Web	54
5.1.1. Gestione di Server Dr.Web sotto SO Windows	56
5.1.2. Gestione di Server Dr.Web sotto SO della famiglia UNIX	60
5.2. Protezione delle postazioni	63
5.3. Pannello di controllo della sicurezza Dr.Web	65
5.3.1. Amministrazione	68
5.3.2. Rete antivirus	71
5.3.3. Preferiti	81
5.3.4. Barra di ricerca	83
5.3.5. Eventi	83
5.3.6. Impostazioni	85



5.3.7. Aiuto	90
5.4. Componenti del Pannello di controllo della sicurezza Dr.Web	91
5.4.1. Scanner di rete	91
5.5. Schema interazione dei componenti della rete antivirus	95
Capitolo 6: Amministratori della rete antivirus	99
6.1. Autenticazione degli amministratori	99
6.1.1. Autenticazione degli amministratori dal database del Server Dr.Web	100
6.1.2. Autenticazione con utilizzo di LDAP/AD	101
6.1.3. Autenticazione con utilizzo di RADIUS	101
6.1.4. Autenticazione con utilizzo di PAM	103
6.1.5. Autenticazione con utilizzo di Active Directory	105
6.1.6. Autenticazione con utilizzo di LDAP	106
6.2. Amministratori e gruppi di amministratori	108
6.2.1. Lista gerarchica degli amministratori	108
6.2.2. Permessi degli amministratori	110
6.3. Gestione degli account amministratori e dei gruppi di amministratori	113
6.3.1. Creazione ed eliminazione degli account amministratori e dei gruppi	113
6.3.2. Ripristino della password amministratore	116
6.3.3. Modifica degli account amministratori e dei gruppi	117
Capitolo 7: Gestione integrata delle postazioni	120
7.1. Ereditarietà della configurazione della postazione	121
7.2. Gruppi	124
7.2.1. Gruppi di sistema e custom	124
7.2.2. Gestione dei gruppi	128
7.2.3. Inserimento delle postazioni in gruppi	131
7.2.4. Confronto delle postazioni e dei gruppi	136
7.2.5. Copiatura delle impostazioni in altri gruppi/postazioni	137
7.3. Criteri	138
7.3.1. Gestione dei criteri	139
7.3.2. Assegnazione di un criterio alle postazioni	140
7.4. Profili	141
7.4.1. Creazione e assegnazione di profili	142
7.4.2. Configurazione dei profili	144
Capitolo 8: Gestione delle postazioni	153
8.1. Gestione degli account di postazioni	153
8.1.1. Criteri di approvazione delle postazioni	153



8.1.2. Rimozione e recupero della postazione	155
8.1.3. Unione delle postazioni	156
8.2. Impostazioni generali della postazione	157
8.2.1. Proprietà della postazione	157
8.2.2. Componenti di protezione	162
8.2.3. Hardware e software sulle postazioni SO Windows	164
8.3. Configurazione delle impostazioni della postazione	165
8.3.1. Permessi dell'utente della postazione	165
8.3.2. Calendario dei task della postazione	168
8.3.3. Componenti da installare del pacchetto antivirus	174
8.3.4. Parametri di connessione	175
8.3.5. Chiavi di licenza	176
8.4. Configurazione dei componenti antivirus	179
8.5. Scansione antivirus delle postazioni	183
8.5.1. Interruzione dei componenti in esecuzione per tipo	184
8.5.2. Avvio della scansione della postazione	185
8.5.3. Configurazione di Scanner	185
8.6. Visualizzazione delle statistiche della postazione	194
8.6.1. Statistiche	194
8.6.2. Grafici	204
8.6.3. Identificatori di protezione	206
8.6.4. Quarantena	206
8.6.5. Report di supporto tecnico	210
8.7. Invio dei file di installazione	212
8.8. Invio di messaggi alle postazioni	213
Capitolo 9. Gestione delle postazioni in ambienti virtuali	217
9.1. Connessione delle postazioni a Server di scansione	218
9.2. Integrazione con l'infrastruttura dei desktop virtuali	222
Capitolo 10: Configurazione del Server Dr.Web	227
10.1. Gestione delle licenze	227
10.1.1. Gestione licenze	227
10.1.2. Report sull'utilizzo delle licenze	237
10.2. Log	238
10.2.1. Log in tempo reale	238
10.2.2. Log di verifica	240
10.2.3. Log del Server Dr.Web	242



10.2.4. Log di aggiornamento del repository	245
10.2.5. Log dei messaggi	247
10.3. Configurazione del Server Dr.Web	248
10.3.1. Generali	249
10.3.2. Traffico	252
10.3.3. Rete	255
10.3.4. Statistiche	262
10.3.5. Sicurezza	267
10.3.6. Cache	269
10.3.7. Database	269
10.3.8. Moduli	272
10.3.9. Posizione	273
10.3.10. Licenze	274
10.3.11. Log	275
10.4. Accesso remoto al Server Dr.Web	276
10.5. Configurazione dell'agent SNMP Dr.Web	277
10.6. Configurazione del calendario di Server Dr.Web	278
10.7. Configurazione del web server	291
10.7.1. Generali	292
10.7.2. Avanzate	294
10.7.3. Trasporto	295
10.7.4. Sicurezza	295
10.7.5. Moduli	297
10.7.6. Gestori	298
10.8. Procedure personalizzate	300
10.9. Modelli di messaggio	305
10.10. Configurazione degli avvisi	306
10.10.1. Configurazione degli avvisi	306
10.10.2. Avvisi nella console web	313
10.10.3. Avvisi non inviati	315
10.11. Gestione del repository di Server Dr.Web	317
10.11.1. Stato del repository	321
10.11.2. Aggiornamenti differiti	322
10.11.3. Configurazione generale del repository	323
10.11.4. Configurazione dettagliata del repository	328
10.11.5. Contenuti del repository	334



10.11.6. Hash di minacce conosciuti	336
10.12. Controllo delle applicazioni	338
10.12.1. Modalità test	341
10.12.2. Applicazioni affidabili	342
10.12.3. Prontuario applicazioni	346
10.13. Funzioni aggiuntive	349
10.13.1. Gestione del database	349
10.13.2. Statistiche di Server Dr.Web	352
10.13.3. Copie di backup	353
10.13.4. Utility	355
10.13.5. Prodotti aziendali	356
10.14. Caratteristiche di una rete con diversi Server Dr.Web	358
10.14.1. Struttura di una rete con diversi Server Dr.Web	359
10.14.2. Configurazione delle relazioni tra i Server Dr.Web	361
10.14.3. Utilizzo di una rete antivirus con diversi Server Dr.Web	368
10.14.4. Cluster dei Server Dr.Web	369
Capitolo 11: Aggiornamento dei componenti di Dr.Web Enterprise Security Suite durante il funzionamento	375
11.1. Aggiornamento di Server Dr.Web e ripristino da copia di backup	375
11.2. Aggiornamento dei Server Dr.Web nel cluster	377
11.3. Aggiornamento del repository di Server Dr.Web manualmente	378
11.4. Aggiornamento del repository di Server Dr.Web secondo il calendario	379
11.5. Aggiornamento del repository di un Server Dr.Web non connesso a internet	380
11.5.1. Copiatura del repository di un altro Server Dr.Web	381
11.5.2. Loader di repository Dr.Web	381
11.6. Limitazione degli aggiornamenti delle postazioni	385
11.7. Aggiornamento di Agent Dr.Web in modalità mobile	388
Capitolo 12: Configurazione dei componenti aggiuntivi	390
12.1. Server proxy Dr.Web	390
12.1.1. Configurazione del Server proxy in remoto	394
12.2. NAP Validator	399
Indice analitico	403



Capitolo 1: Introduzione

1.1. Scopo del documento

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

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

1. Guida all'installazione

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

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

2. Manuale dell'amministratore

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

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

3. Allegati

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



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

Inoltre, sono forniti i seguenti manuali:

1. Guida rapida all'installazione della rete antivirus

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



2. Manuali per la gestione delle postazioni

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

3. Manuali dell'utente

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

4. Guida alle Web API

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

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

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



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

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

1.2. Segni convenzionali e abbreviazioni

Segni convenzionali

In questo manuale vengono utilizzati i seguenti simboli:

Simbolo	Commento
	Nota importante o istruzione.
	Avviso di possibili situazioni di errore, nonché di punti importanti cui prestare particolare attenzione.
<i>Rete antivirus</i>	Un nuovo termine o un termine accentato nelle descrizioni.
<indirizzo_IP>	Campi in cui nomi di funzione vanno sostituiti con valori effettivi.
Salva	Nomi dei pulsanti di schermo, delle finestre, delle voci di menu e di altri elementi dell'interfaccia del programma.
CTRL	Nomi dei tasti della tastiera.



Simbolo	Commento
C:\Windows\	Nomi di file e directory, frammenti di codice.
Allegato A	Riferimenti incrociati ai capitoli del documento o collegamenti ipertestuali a risorse esterne.

Abbreviazioni

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

- DB, DBMS — database, database management system,
- SAM Dr.Web — Sistema di aggiornamento mondiale di Dr.Web,
- LAN — rete locale,
- SO — sistema operativo,
- SW, software — programmi per computer,
- ACL — lista di controllo degli accessi (Access Control List),
- CDN — rete di distribuzione di contenuti (Content Delivery Network),
- DFS — file system distribuito (Distributed File System),
- DNS — sistema dei nomi a dominio (Domain Name System),
- FQDN — nome di dominio completo (Fully Qualified Domain Name),
- GUI — interfaccia utente grafica (Graphical User Interface), versione del programma con la GUI — una versione che utilizza gli strumenti della GUI,
- MIB — database delle informazioni di gestione (Management Information Base),
- MTU — dimensione massima di un pacchetto dati (Maximum Transmission Unit),
- NAP — Network Access Protection,
- TTL — tempo di vita pacchetto (Time To Live),
- UDS — socket di dominio UNIX (UNIX Domain Socket).

Capitolo 2: Dr.Web Enterprise Security Suite

2.1. Sul prodotto

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

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

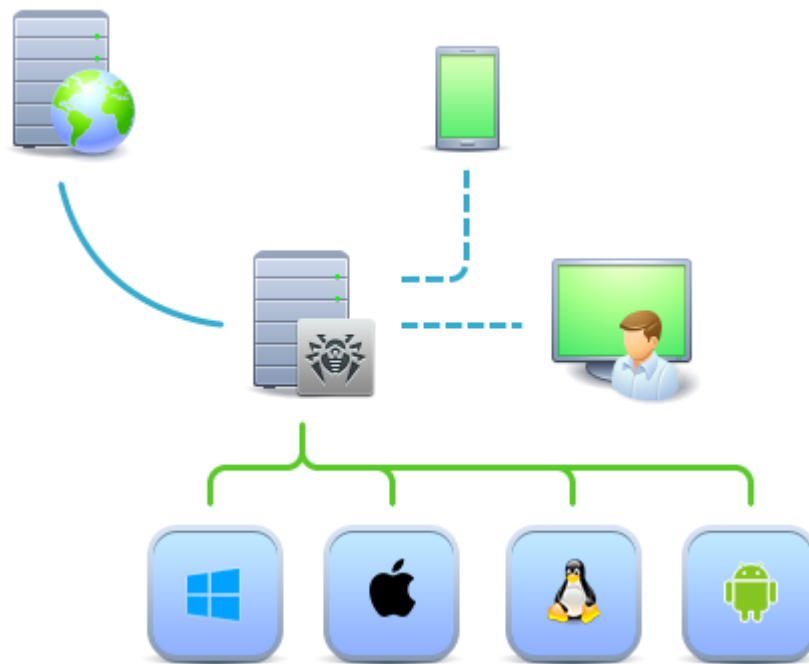


Immagine 1-1. Struttura logica della rete antivirus

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



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

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

Server di protezione centralizzata

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

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

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

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

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

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

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

Database unico

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

È possibile utilizzare i seguenti tipi di database:

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

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

- MySQL, Maria DB,
- Oracle,



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

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

Pannello di controllo di protezione centralizzata

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

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

- Windows Internet Explorer,
- Microsoft Edge,
- Mozilla Firefox,
- Google Chrome,
- Yandex.Browser.

Un elenco di possibili varianti di utilizzo è riportato in **Guida all'installazione**, p. [Requisiti di sistema](#).

Il Pannello di controllo fornisce le seguenti possibilità:

- Comodità di installazione di Antivirus sulle postazioni protette, in particolare, è possibile: installare in remoto su postazioni eseguendo una scansione della rete preliminare per cercare computer; creare pacchetti con identificatori univoci e con i parametri di connessione al Server di protezione centralizzata per semplificare il processo di installazione di Antivirus da parte dell'amministratore o per consentire agli utenti di installare Antivirus sulle postazioni in modo autonomo.
- Gestione semplificata delle postazioni della rete antivirus attraverso il metodo di gruppi (per informazioni dettagliate v. sezione [Capitolo 7: 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 dei pacchetti antivirus; assegnare i permessi per configurare e gestire i pacchetti antivirus dei computer protetti agli utenti di questi computer (per informazioni dettagliate v. sezione [Capitolo 8: Gestione delle postazioni](#)).



- Gestione centralizzata della scansione antivirus delle postazioni, in particolare è possibile: avviare la scansione antivirus in remoto sia secondo un calendario prestabilito che su una richiesta diretta dell'amministratore dal Pannello di controllo; configurare in modo centralizzato le impostazioni di scansione antivirus che vengono trasmesse alle postazioni per il successivo avvio di una scansione locale con queste impostazioni (per informazioni dettagliate v. sezione [Scansione antivirus delle postazioni](#)).
- Ottenimento di informazioni statistiche sullo stato delle postazioni protette, di statistiche di virus, di informazioni sullo stato del software antivirus installato, sullo stato dei componenti antivirus in esecuzione, nonché di un elenco degli hardware e dei software della postazione protetta (per informazioni dettagliate v. sezione [Visualizzazione delle statistiche della postazione](#)).
- Sistema flessibile di amministrazione del Server di protezione centralizzata e della rete antivirus grazie alla possibilità di delimitare i permessi di diversi amministratori, nonché la possibilità di connettere amministratori attraverso sistemi di autenticazione esterni, come Active Directory, LDAP, RADIUS, PAM (per informazioni dettagliate v. sezione [Capitolo 6: Amministratori della rete antivirus](#)).
- Gestione delle licenze di protezione antivirus delle postazioni con un sistema ramificato di assegnazione delle licenze a postazioni e gruppi di postazioni, nonché di trasferimento delle licenze tra diversi Server di protezione centralizzata in caso di una configurazione di rete antivirus con diversi server (per informazioni dettagliate v. sezione [Gestione licenze](#)).
- Ampio set di impostazioni per la configurazione del Server Dr.Web dei suoi singoli componenti, tra l'altro, è possibile: impostare un calendario per la manutenzione; connettere procedure personalizzate; configurare in modo flessibile l'aggiornamento da SAM di tutti i componenti della rete antivirus e la successiva distribuzione degli aggiornamenti alle postazioni; configurare i sistemi di avviso dell'amministratore sugli eventi della rete antivirus con vari metodi di consegna dei messaggi; configurare le relazioni tra i server per una configurazione di rete antivirus con diversi server (per informazioni dettagliate v. sezione [Capitolo 10: Configurazione del Server Dr.Web](#)).



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

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

Pannello di controllo mobile di protezione centralizzata

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



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

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



8. Ricerca di postazioni e gruppi nella rete antivirus per nome, indirizzo o ID.

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

Protezione delle postazioni della rete

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

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

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

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

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

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

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

Postazioni SO Windows

Scansione antivirus

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

Monitoraggio di file

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

Monitoraggio di email

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

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



Monitoraggio del traffico web

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

Office control

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

Firewall

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

Quarantena

Isolamento di oggetti dannosi e sospetti in una directory speciale.

Auto-protezione

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

Protezione preventiva

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

Controllo delle applicazioni

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

Postazioni con SO della famiglia UNIX

Scansione antivirus

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



Scansione antivirus, gestione della quarantena

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

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

Controllo del traffico web

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

Monitoraggio di file per i sistemi GNU/Linux

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

Monitoraggio di file per le directory Samba

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

Monitoraggio di file NSS

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

Controllo delle connessioni di rete

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



Monitoraggio di email

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

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

Postazioni macOS

Scansione antivirus

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

Monitoraggio di file

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

Monitoraggio del traffico web

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

Quarantena

Isolamento di oggetti dannosi e sospetti in una directory speciale.

Dispositivi mobili SO Android

Scansione antivirus

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

Monitoraggio di file

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

Filtro chiamate ed SMS

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



Antifurto

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

Limitazione dell'accesso a risorse Internet

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

Firewall

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

Aiuto nella risoluzione di problemi

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

Controllo dell'esecuzione di applicazioni

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

Assicurazione della comunicazione tra i componenti della rete antivirus

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

Server proxy Dr.Web

Il Server proxy può opzionalmente essere incluso nella struttura della rete antivirus. L'obiettivo principale del Server proxy è quello di provvedere alla comunicazione tra il Server Dr.Web e le postazioni protette nel caso non sia possibile organizzare l'accesso diretto.

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

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



Compressione del traffico

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

Cifratura del traffico

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

Funzioni aggiuntive

NAP Validator

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

Loader di repository

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

Server di scansione Dr.Web

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

2.2. Contenuto del pacchetto

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

1. In caso di SO della famiglia UNIX:

- `drweb-esuite-server-<versione_pacchetto>-<build>-<versione_SO>.tar.gz.run`
Pacchetto di Server Dr.Web.
- `drweb-reloader-<sistema_operativo>-<numero_di_bit>`
Versione console di Loader di repository Dr.Web.

2. In caso di SO Windows:

- `drweb-esuite-server-<versione_pacchetto>-<build>-<versione_SO>.exe`
Pacchetto di Server Dr.Web.



- `drweb-<versione_pacchetto>-<build>-esuite-agent-full-windows.exe`
Installer completo di Agent Dr.Web.
- `drweb-reploader-windows-<numero_di_bit>.exe`
Versione console di Loader di repository Dr.Web.
- `drweb-reploader-gui-windows-<numero_di_bit>.exe`
Versione grafica di Loader di repository Dr.Web.

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

- software di Server Dr.Web per il sistema operativo corrispondente;
- dati di sicurezza di Server Dr.Web;
- software di Pannello di controllo della sicurezza Dr.Web;
- software di Agent Dr.Web e pacchetto antivirus per postazioni con SO Windows;
- modulo di aggiornamento di Agent Dr.Web per Windows;
- Antispam Dr.Web per Windows;
- database dei virus, database dei filtri incorporati dei componenti antivirus e di Antispam Dr.Web per Windows;
- documentazione;
- notizie di Doctor Web.

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

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

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



Informazioni dettagliate sulla gestione del repository di Server Dr.Web sono riportate in



Manuale dell'amministratore, sezione [Gestione del repository di Server Dr.Web](#).



Capitolo 3: Concessione delle licenze

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

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



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

File della chiave di licenza

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



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

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

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

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

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



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

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



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

L'utilizzo dei file della chiave di licenza per una rete antivirus già dispiegata è descritto in p. [Gestione licenze](#).

3.1. Caratteristiche delle licenze

1. Server Dr.Web non viene concesso in licenza.



L'UUID di Server Dr.Web che nelle versioni precedenti di Dr.Web Enterprise Security Suite era memorizzato nella chiave di licenza di Server Dr.Web adesso è memorizzato nel file di configurazione di Server Dr.Web (a partire dalla versione 10).

- Quando viene installato un nuovo Server Dr.Web, viene generato un nuovo UUID.
- Quando il Server Dr.Web viene aggiornato dalle versioni precedenti, l'UUID viene preso automaticamente dal file di configurazione della versione precedente e viene scritto nel file di configurazione del Server Dr.Web che viene installato.

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

2. Le chiavi di licenza sono rilevanti soltanto per le postazioni protette. È possibile assegnare licenze sia a singole postazioni, che a gruppi di postazioni: in questo caso una chiave di licenza vale per tutte le postazioni che la ereditano da questo gruppo. Per assegnare un file della chiave contemporaneamente a tutte le postazioni della rete antivirus, cui non sono state assegnate le impostazioni individuali della chiave di licenza, assegnare la chiave di licenza al gruppo **Everyone**.
3. Il file della chiave di licenza può essere impostato durante l'installazione di Server Dr.Web (v. **Guida all'installazione**, p. [Installazione di Server Dr.Web](#)).

È possibile però installare un Server Dr.Web anche senza una chiave di licenza. La licenza può essere aggiunta in seguito sia localmente e sia può essere ricevuta attraverso la comunicazione tra i server.



4. Attraverso la comunicazione tra i server è possibile trasferire un numero opzionale di licenze dalle chiavi conservate su questo Server Dr.Web a un Server Dr.Web adiacente per un determinato periodo di tempo.
5. È possibile utilizzare alcune licenze diverse, per esempio licenze con diverse scadenze o con un diverso insieme di componenti antivirus per postazioni protette. Ogni chiave di licenza può essere assegnata contemporaneamente a più oggetti di licenza (gruppi e postazioni). Più chiavi di licenza possono essere assegnate contemporaneamente allo stesso oggetto di licenza.
6. Quando vengono assegnate più chiavi ad un oggetto, prestare attenzione alle seguenti caratteristiche:
 - a) Se diverse chiavi dello stesso oggetto hanno un diverso elenco dei componenti antivirus consentiti, l'elenco dei componenti consentiti per le postazioni viene determinato tramite l'intersezione degli insiemi di componenti nelle chiavi. Per esempio, se a un gruppo di postazioni sono state assegnate una chiave con il supporto di Antispam ed una senza il supporto di Antispam, l'installazione di Antispam sulle postazioni sarà vietata.
 - b) Le impostazioni di licenza per un oggetto vengono calcolate sulla base di tutte le chiavi assegnate a questo oggetto. Se le scadenze delle chiavi di licenza sono diverse, allora dopo che è scaduta una chiave con la validità minima è necessario sostituirla o eliminarla manualmente. Se la chiave scaduta impostava limitazioni all'installazione di componenti antivirus, è necessario modificare le impostazioni dell'oggetto di licenza 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 questo oggetto. È inoltre necessario tenere conto della possibilità di trasferimento delle licenze attraverso la comunicazione tra i server su un Server Dr.Web adiacente (v. p. 4). In questo caso dal numero totale di licenze vengono sottratte le licenze trasferite sul Server Dr.Web adiacente.



Le chiavi di licenza vengono gestite attraverso la [Gestione licenze](#).

Quando una chiave di licenza viene impostata nella Gestione licenze, tutte le informazioni su questa licenza vengono salvate nel database.

3.2. Distribuzione delle licenze attraverso le relazioni tra i server

In una rete antivirus con diversi Server Dr.Web è possibile trasferire un numero opzionale di licenze tra i Server Dr.Web per un determinato periodo di tempo.



Per la possibilità di trasferimento di licenze tra i Server Dr.Web configurare le relazioni tra i server come descritto in sezione [Configurazione delle relazioni tra i Server Dr.Web](#).

La distribuzione di licenze è possibile per le seguenti varianti di relazioni:

- Il Server Dr.Web principale rilascia licenze e il Server Dr.Web subordinato accetta licenze secondo le impostazioni di distribuzione licenze della relazione (non modificabili).



- Trasferimento di licenze tra Server Dr.Web paritari. In questo caso per il Server Dr.Web che rilascia licenze nelle impostazioni della relazione nella sezione **Licenze** deve essere spuntato il flag **Invia**, mentre per il Server Dr.Web che riceve licenze il flag **Ricevi**.

Per configurare il Server Dr.Web che rilascerà licenze

1. Aprire il Pannello di controllo del Server Dr.Web della rete antivirus che rilascerà licenze ai Server Dr.Web adiacenti.
2. Nel menu principale del Pannello di controllo selezionare la voce **Amministrazione**, nel [menu di gestione](#) selezionare la voce **Gestione licenze**.
3. Aggiungere una chiave di licenza come descritto in sezione [Gestione licenze](#), se la chiave non è stata ancora aggiunta in precedenza. Il numero di licenze nella chiave deve corrispondere al numero totale di postazioni connesse sia a questo Server Dr.Web che a tutti i Server Dr.Web che riceveranno licenze da questa chiave.

Nel caso generale può essere sufficiente una chiave di licenza da cui le licenze verranno distribuite tra tutti i Server Dr.Web.

4. Calcolare quante licenze da questa chiave possono essere trasferite ai Server Dr.Web adiacenti. Nel calcolo tenere presente che dai Server Dr.Web adiacenti anche può essere trasferita una parte delle licenze ad altri Server Dr.Web. In questo caso dalla chiave del Server Dr.Web principale deve essere trasferito il numero totale di licenze che si intende distribuire ulteriormente lungo la catena. Tenere presente inoltre che il Server Dr.Web principale non potrà utilizzare le licenze distribuite prima della fine del periodo di distribuzione di queste licenze e del loro ritorno.
5. Configurare la distribuzione di licenze su Server Dr.Web adiacenti dalla chiave di licenza come descritto in sezione [Gestione licenze](#).

Nell'impostazione **Data di scadenza della licenza** impostare la data finale per il trasferimento delle licenze. Il periodo di trasferimento può essere inferiore o uguale al periodo di validità della licenza stessa. Dopo il periodo indicato tutte le licenze verranno revocate dal Server Dr.Web adiacente e torneranno nella lista delle licenze disponibili della chiave di licenza originale. Se necessario, è possibile modificare questo periodo in qualsiasi momento come descritto in sezione [Gestione licenze](#).

6. Se necessario, modificare le impostazioni di distribuzione delle licenze. Per farlo, passare alla sezione **Configurazione del Server Dr.Web**.
7. Nella scheda **Licenze** configurare le seguenti impostazioni riguardanti il Server Dr.Web che rilascia licenze:
 - **Periodo di rinnovo automatico delle licenze rilasciate** — periodo di tempo per cui vengono rilasciate le licenze dalla chiave su questo Server Dr.Web. Dopo la fine di questo periodo viene eseguito il rinnovo automatico delle licenze rilasciate per lo stesso periodo. Il rinnovo automatico verrà eseguito fino a quando durerà il periodo di distribuzione delle licenze impostato in Gestione licenze al passaggio 5.
Questo meccanismo assicura il ritorno delle licenze sul Server Dr.Web principale nel caso in cui il Server Dr.Web subordinato verrà disconnesso e non potrà restituire le licenze rilasciate.



- **Periodo di sincronizzazione delle licenze** — periodicità di sincronizzazione delle informazioni sulle licenze rilasciate tra i Server Dr.Web. La sincronizzazione delle licenze consentirà di determinare che il numero di licenze rilasciate dal Server Dr.Web principale corrisponde al numero di licenze ricevute dal Server Dr.Web subordinato. Questo meccanismo consente di identificare errori e casi di falsificazione nel trasferimento delle licenze.
- **Periodo di creazione del report** — periodicità con cui sul Server Dr.Web verranno creati i report sulle chiavi di licenza da esso utilizzate. Se un report sull'utilizzo delle licenze viene creato da un Server Dr.Web subordinato, subito dopo la creazione questo report viene inviato sul Server Dr.Web principale. I report creati vengono inoltre inviati ad ogni connessione (incluso il riavvio) del Server Dr.Web, e inoltre, quando sul Server Dr.Web principale cambia il numero di licenze rilasciate. L'impostazione viene configurata sul Server Dr.Web principale, ma viene utilizzata anche dal Server Dr.Web subordinato nell'invio dei report.
- **Periodo di conteggio delle postazioni attive per il report sulle licenze** — periodo durante cui verrà conteggiato il numero di postazioni attive per la creazione del report sull'utilizzo delle licenze. Il valore 0 prescrive di prendere in considerazione nel report tutte le postazioni, indipendentemente dal loro stato di attività. L'impostazione viene configurata sul Server Dr.Web principale, ma viene utilizzata anche dal Server Dr.Web subordinato nell'invio dei report.

8. Salvare le modifiche apportate e riavviare il Server Dr.Web.

Per configurare il Server Dr.Web che riceverà licenze

1. Aprire il Pannello di controllo del Server Dr.Web della rete antivirus che riceverà licenze dal Server Dr.Web adiacente.
2. Se necessario, modificare le impostazioni di distribuzione delle licenze. Per farlo, passare alla sezione **Configurazione del Server Dr.Web**.
3. Nella scheda **Licenze** impostare **Intervallo per il rinnovo preliminare delle licenze ricevute** — intervallo di tempo prima della fine del periodo di rinnovo automatico delle licenze ricevute dal Server Dr.Web adiacente, a partire da cui questo Server Dr.Web richiede il rinnovo automatico preliminare di queste licenze.

L'uso di questa impostazione dipende dal tipo di connessione selezionato nell'impostazione **Parametri di connessione** durante la configurazione della relazione tra i Server Dr.Web (v. sezione [Configurazione delle relazioni tra i Server Dr.Web](#)):

- Per il tipo di connessione periodica: se il periodo di riconnessione definito nell'impostazione della relazione è superiore al **Periodo di rinnovo automatico delle licenze rilasciate** definito sul Server Dr.Web che ha rilasciato le licenze, il rinnovo automatico di queste licenze verrà inizializzato prima che finisca il **Periodo di rinnovo automatico delle licenze rilasciate**.
 - Per la connessione permanente: questa impostazione non viene utilizzata.
4. Salvare le modifiche apportate e riavviare il Server Dr.Web.



3.3. Aggiornamento automatico delle licenze


Una licenza per Dr.Web Enterprise Security Suite può essere aggiornata in maniera automatica.

L'aggiornamento automatico della licenza sottintende i seguenti aspetti:

- Quando scade una chiave di licenza, essa può essere sostituita automaticamente dal programma con una chiave di licenza precedentemente acquistata.
- L'aggiornamento automatico viene eseguito per una chiave di licenza specifica per cui è stato acquistato un rinnovo.
- La chiave di licenza che verrà utilizzata per l'aggiornamento automatico si trova sui server della società Doctor Web fino alla sua scadenza.

Procedura per l'aggiornamento automatico delle licenze

La procedura per l'aggiornamento automatico delle licenze viene avviata nei seguenti casi:

- Quando l'amministratore preme il pulsante  **Controlla disponibilità degli aggiornamenti e sostituisci chiavi di licenza** nella barra delle applicazioni nella [Gestione licenze](#) del Pannello di controllo.
- Quando viene eseguito il task **Aggiornamento del repository** dal [calendario di Server Dr.Web](#). In questo caso nelle impostazioni del task deve essere spuntato il flag **Aggiorna chiavi di licenza**.



L'aggiornamento automatico della chiave di licenza viene avviato solo nel caso in cui la licenza da aggiornare appartiene a questo Server Dr.Web: inizialmente è stata aggiunta manualmente od ottenuta attraverso l'aggiornamento automatico. Per licenze ottenute dai Server Dr.Web adiacenti attraverso le relazioni tra i server la procedura di aggiornamento automatico non viene avviata.

La procedura per l'aggiornamento automatico delle licenze contiene le seguenti fasi:

1. Verifica della disponibilità di una chiave di licenza sui server della società Doctor Web (SAM).
2. Caricamento della chiave di licenza da SAM sul Server Dr.Web con la successiva aggiunta della chiave al database e alla Gestione licenze.
3. Distribuzione della nuova chiave di licenza sugli oggetti della chiave precedente.

A seconda dei risultati dell'esecuzione di ciascuna fase, la procedura può essere completata in modo normale in qualsiasi di esse.

Sono possibili i seguenti risultati dell'esecuzione dell'aggiornamento automatico:

1. *La chiave di licenza per l'aggiornamento automatico è assente su SAM.*
Nessuna azione verrà eseguita.



2. *La chiave di licenza per l'aggiornamento automatico è disponibile su SAM. La lista dei componenti concessi in licenza della chiave corrente è diversa da quella della chiave nuova (nella chiave nuova non c'è qualche componente che c'è in quella corrente) e/o la chiave di licenza nuova ha un minor numero di licenze rispetto alla chiave di licenza corrente.*

La nuova licenza viene scaricata dai server dell'azienda Doctor Web, viene aggiunta alla Gestione licenze e al database di Server Dr.Web, ma non viene distribuita sugli oggetti di licenza. In tale situazione è necessario distribuire manualmente la chiave di licenza.

All'amministratore viene inviato un avviso **Chiave di licenza non può essere aggiornata automaticamente**. Il motivo specifico per cui la chiave non può essere distribuita automaticamente verrà riportato nell'avviso.

3. *La chiave di licenza per l'aggiornamento automatico è disponibile su SAM. Le liste dei componenti concessi in licenza della chiave corrente e di quella nuova corrispondono o nella chiave nuova ci sono più componenti concessi in licenza rispetto alla chiave corrente, compresi tutti i componenti della chiave corrente; il numero di licenze della chiave di licenza nuova è superiore o uguale a quello della chiave di licenza corrente.*

La nuova licenza viene scaricata dai server dell'azienda Doctor Web, viene aggiunta alla Gestione licenze e al database di Server Dr.Web e viene distribuita su tutti gli oggetti di licenza su cui era distribuita la licenza precedente, compresi i Server Dr.Web adiacenti.

La vecchia licenza verrà rimossa automaticamente quando non verrà utilizzata da nessun Server Dr.Web subordinato. Pertanto, se al momento dell'aggiornamento automatico un Server Dr.Web subordinato era disconnesso, la vecchia licenza verrà conservata fino a quando questo Server Dr.Web subordinato non si riconnetterà.

La vecchia licenza verrà conservata fino a quando non verrà rimossa manualmente nei seguenti casi:

- Se non è possibile distribuire la licenza ottenuta tramite l'aggiornamento automatico su un Server Dr.Web subordinato (il Server Dr.Web è stato disconnesso in modo permanente).
- Se su un Server Dr.Web subordinato viene utilizzata una versione di protocollo che non supporta le funzionalità di aggiornamento automatico. In questo caso le licenze verranno trasferite sul Server Dr.Web subordinato, ma non verranno distribuite.

All'amministratore viene inviato un avviso **Chiave di licenza è aggiornata automaticamente**. L'avviso di aggiornamento verrà inviato da ciascun Server Dr.Web su cui verrà distribuita la nuova licenza.



Tutti gli avvisi da inviare all'amministratore vengono configurati nella sezione **Amministrazione** → **Configurazione degli avvisi**.

Dopo l'invio di ciascun avviso viene eseguita la [procedura personalizzata Aggiornamento automatico della chiave di licenza](#).



Aggiornamento delle licenze manuale

Se si è acquistata una chiave di licenza per l'aggiornamento automatico della chiave corrente, non è richiesto aggiungere la nuova chiave manualmente nella Gestione licenze. A seconda della situazione (la variante 2 nella procedura sopra) può essere richiesta soltanto la distribuzione manuale sugli oggetti di licenza.

Tuttavia, se prima dell'esecuzione della [procedura per l'aggiornamento automatico delle licenze](#) si è aggiunta in autonomo attraverso la Gestione licenze una nuova chiave soggetta all'aggiornamento automatico secondo la variante 3 (v. la procedura sopra), allora durante l'esecuzione del task verrà effettuata soltanto la distribuzione della nuova chiave di licenza. In questo caso sono possibili le seguenti varianti:

- a) La nuova chiave di licenza è stata distribuita manualmente su tutti gli oggetti su cui era distribuita la chiave precedente (quella che viene aggiornata). In tale caso durante l'esecuzione del task di aggiornamento non verranno apportate alcune modifiche.
- b) La nuova chiave di licenza è stata distribuita manualmente su alcuni oggetti di quelli su cui era distribuita la chiave precedente (quella che viene aggiornata). In tale caso durante l'esecuzione del task di aggiornamento la nuova chiave verrà distribuita su tutti gli oggetti rimanenti della chiave precedente che non hanno ancora ricevuto l'aggiornamento.

Se la nuova chiave di licenza è stata distribuita manualmente su ulteriori oggetti che non c'erano nella lista della chiave precedente, dopo l'esecuzione del task la nuova chiave rimarrà distribuita anche su questi oggetti. In questo caso sono possibili le seguenti varianti:

- Il numero di licenze è sufficiente a tutti gli oggetti di licenza: a quelli che c'erano nella chiave precedente e a quelli assegnati manualmente alla nuova chiave. Tale situazione è possibile, in particolare, se la nuova chiave contiene un numero maggiore di licenze. In tale caso durante l'esecuzione del task di aggiornamento non verranno apportate alcune modifiche.
- Il numero di licenze non è sufficiente per la distribuzione a tutti gli oggetti di licenza posseduti dalla chiave precedente perché delle licenze sono state assegnate manualmente ad altri oggetti. Per gli oggetti che non hanno avuto licenze, l'aggiornamento non verrà eseguito, tuttavia, la chiave precedente verrà rimossa comunque, e gli oggetti rimarranno senza licenza. Quando compariranno licenze disponibili, tutti gli oggetti che non hanno avuto licenze otterranno una nuova chiave di licenza. In questo caso le azioni dipendono dal tipo di oggetto di licenza:
 - Se le licenze dalla nuova chiave non sono bastate alle postazioni di questo Server Dr.Web, la verifica delle licenze disponibili verrà eseguita ogni volta quando una postazione cercherà di connettersi al Server Dr.Web. Se al momento di una connessione verrà rilevata una licenza liberata, quest'ultima verrà concessa a tale postazione.
 - Se le licenze dalla nuova chiave non sono bastate per essere rilasciate ai Server Dr.Web adiacenti, la verifica delle licenze disponibili verrà eseguita automaticamente circa una volta al minuto. Quando compariranno licenze disponibili, esse verranno date ai Server Dr.Web adiacenti.



File della chiave di licenza

Notare le seguenti caratteristiche dei file della chiave di licenza quando viene eseguito l'aggiornamento automatico:

- Quando viene eseguito l'aggiornamento automatico, la nuova licenza viene scaricata dai server dell'azienda Doctor Web, le informazioni su di essa vengono salvate nel database di Server Dr.Web e visualizzate in Gestione licenze. In questo caso non viene creato alcun file della chiave di licenza.
- Per ottenere un file della chiave di licenza, utilizzare l'opzione **Amministrazione** → **Gestione licenze** → **Esporta chiave**. Un file della chiave di licenza può inoltre essere ottenuto con l'esecuzione della procedura personalizzata **Aggiornamento automatico della chiave di licenza**.
- Quando la licenza viene rimossa, le informazioni su di essa vengono rimosse da Gestione licenze e dal database di Server Dr.Web, però il file della chiave di licenza rimane nella directory di Server Dr.Web.



Capitolo 4: Introduzione all'uso

4.1. Creazione della rete antivirus

Brevi istruzioni per l'installazione di una rete antivirus:

1. Progettare uno schema della struttura della rete antivirus, includere in esso tutti i computer, macchine virtuali e dispositivi mobili protetti.

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



Il Server Dr.Web può essere installato su qualsiasi computer e non solo su quello che svolge le funzioni di server LAN. I requisiti principali per tale computer sono riportati in **Guida all'installazione**, p. [Requisiti di sistema.](#)

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

Per l'installazione di Server Dr.Web e Agent Dr.Web, è necessario un singolo accesso (fisico o tramite strumenti di gestione e avvio programmi remoto) alle relative postazioni. Tutte le operazioni successive vengono eseguite dalla postazione di lavoro dell'amministratore della rete antivirus (anche possibilmente dall'esterno della rete locale) e non richiedono l'accesso ai Server Dr.Web o alle postazioni.

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



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

La descrizione dettagliata della gestione dei gruppi di amministratori e dei permessi di accesso è riportata in [Capitolo 6: Amministratori della rete antivirus.](#)



- In base allo schema progettato determinare quali prodotti per quali sistemi operativi dovranno essere installati sui nodi della rete corrispondenti. Informazioni dettagliate sui prodotti disponibili sono riportate nella sezione [Contenuto del pacchetto](#).

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



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

- Installare il pacchetto principale di Server Dr.Web su uno o diversi computer selezionati. L'installazione viene descritta in **Guida all'installazione**, p. [Installazione di Server Dr.Web](#). Insieme al Server Dr.Web viene installato il Pannello di controllo della sicurezza Dr.Web. Di default, Server Dr.Web viene avviato automaticamente dopo l'installazione e dopo ogni riavvio del sistema operativo.
- Se necessario, installare e configurare il Server proxy. La descrizione è riportata in **Guida all'installazione**, p. [Installazione del Server proxy Dr.Web](#).
- Se la rete antivirus consiste di macchine virtuali, si consiglia di utilizzare il Server di scansione. Le procedure di installazione e configurazione sono descritte in **Guida all'installazione**, p. [Installazione di Server di scansione Dr.Web](#).
- Per configurare il Server Dr.Web e il software antivirus su postazioni, è necessario connettersi al Server Dr.Web attraverso il Pannello di controllo della sicurezza Dr.Web.



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

Il Pannello di controllo è disponibile sull'indirizzo:

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

o

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

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

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

- Nome utente — **admin**.
- La password:
 - in caso di SO Windows — la password che è stata impostata quando veniva installato il Server Dr.Web.



- in caso di SO della famiglia UNIX — la password che è stata creata automaticamente durante l'installazione di Server Dr.Web (v. inoltre **Guida all'installazione**, p. [Installazione di Server Dr.Web per SO della famiglia UNIX](#)).

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

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

7. Effettuare la configurazione iniziale del Server Dr.Web (una descrizione dettagliata delle impostazioni è riportata in [Capitolo 10: Configurazione di Server Dr.Web](#)):
 - a. Nella sezione [Gestione licenze](#) aggiungere uno o più chiavi di licenza e distribuirle ai gruppi corrispondenti, in particolare, al gruppo **Everyone**. Il passaggio è obbligatorio se durante l'installazione di Server Dr.Web la chiave di licenza non è stata impostata.
 - b. Nella sezione [Configurazione generale del repository](#) impostare quali componenti della rete antivirus verranno aggiornati da SAM Dr.Web. Se la rete antivirus includerà postazioni protette con SO Android, SO Linux, macOS, è necessario caricare i **Prodotti aziendali Dr.Web**.

Nella sezione [Stato del repository](#) aggiornare i prodotti nel repository di Server Dr.Web. L'aggiornamento può richiedere un lungo tempo. Attendere che il processo di aggiornamento sia completato prima di continuare l'ulteriore configurazione.



Se è installato il Server Dr.Web versione 13, di default gli aggiornamenti dei prodotti del repository **Database di Dr.Web per Android**, **Agent Dr.Web per UNIX** e **Server proxy Dr.Web** vengono scaricati da SAM solo quando questi prodotti vengono richiesti dalle postazioni. Per maggiori informazioni v. p. [Configurazione dettagliata del repository](#).

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

- c. Sulla pagina **Amministrazione** → **Server Dr.Web** sono riportate informazioni sulla versione di Server Dr.Web. Se è disponibile una nuova versione, aggiornare il Server Dr.Web, come descritto in p. [Aggiornamento di Server Dr.Web e ripristino da copia di backup](#).
- d. Se necessario, configurare [Configurazione delle connessioni di rete](#) per modificare le impostazioni di rete di default utilizzate per l'interazione di tutti i componenti della rete antivirus.
- e. Se necessario, configurare la lista degli amministratori del Server Dr.Web. Inoltre, è disponibile l'autenticazione esterna degli amministratori. Per maggiori informazioni v. [Capitolo 6: Amministratori della rete antivirus](#).
- f. Prima di iniziare ad utilizzare il software antivirus, è consigliabile modificare l'impostazione della directory per il backup dei dati critici del Server Dr.Web (v. p.



[Configurazione del calendario di Server Dr.Web](#)). È preferibile collocare questa directory su un altro disco locale per ridurre la probabilità di una perdita simultanea dei file del software Server Dr.Web e della copia di backup.

8. Configurare il software antivirus per postazioni (la configurazione dei gruppi e delle postazioni è descritta dettagliatamente in [Capitolo 7](#) e [Capitolo 8](#)):
 - a. Se necessario, creare gruppi di postazioni personalizzati.
 - b. Configurare il gruppo **Everyone** e i gruppi personalizzati creati. In particolare, configurare la sezione dei componenti da installare.
9. Installare il software Agent Dr.Web sulle postazioni.

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

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



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

10. Subito dopo l'installazione sui computer, gli Agent Dr.Web si connettono automaticamente al Server Dr.Web. Le postazioni antivirus vengono autenticate sul Server Dr.Web secondo i criteri scelti (v. p. [Criteri di approvazione delle postazioni](#)):



- a. In caso di installazione dai pacchetti di installazione e inoltre in caso di configurazione della conferma automatica sul Server Dr.Web, le postazioni vengono registrate automaticamente al momento della prima connessione al Server Dr.Web, e ulteriore conferma non è richiesta.
 - b. In caso di installazione dagli installer e di impostazione della conferma di accesso manuale, l'amministratore deve confermare manualmente le nuove postazioni in modo da registrarle sul Server Dr.Web. In questo caso, le nuove postazioni non vengono connesse automaticamente, ma vengono messe dal Server Dr.Web nel gruppo nuovi arrivi.
11. Dopo che la postazione si è connessa al Server Dr.Web e ha ottenuto le impostazioni, su di essa viene installato il relativo set di componenti del pacchetto antivirus, definito nelle impostazioni del gruppo primario della postazione.



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

12. È possibile configurare le postazioni e il software antivirus anche dopo l'installazione (la descrizione dettagliata è riportata in [Capitolo 8](#)).

4.2. Configurazione delle connessioni di rete

Informazioni generali

Al Server Dr.Web si connettono i seguenti client:

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

Una connessione viene sempre stabilita da parte del client.

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

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

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

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

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

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

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



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

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

Configurazione del firewall

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

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

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

4.2.1. Connessioni dirette

Configurazione del Server Dr.Web

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

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

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

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



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

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



Configurazione dell'Agent Dr.Web

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

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

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

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

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

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

4.2.2. Servizio di rilevamento di Server Dr.Web

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

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

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

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

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



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

Questo parametro viene configurato nelle impostazioni del Pannello di controllo:

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

4.2.3. Utilizzo del protocollo SRV

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

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

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



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

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

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

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

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



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

4.3. Connessione sicura

4.3.1. Cifratura e compressione del traffico dati

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



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

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

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

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

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

Criterio di coordinazione delle impostazioni

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

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

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

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

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



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

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

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

Connessione attraverso Server proxy Dr.Web

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

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

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

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

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

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



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

Segni convenzionali

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

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

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

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



Impostazioni di cifratura e di compressione sul Server Dr.Web

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

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



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

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


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



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

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



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

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



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

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

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

In caso di SO Linux:

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

In caso di SO FreeBSD:

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



Impostazioni di cifratura e di compressione sulle postazioni

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

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

Agent Dr.Web per Windows

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

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

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



Antivirus Dr.Web per Android

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

Antivirus Dr.Web per Linux

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

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

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

Antivirus Dr.Web per macOS

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

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

4.3.2. Strumenti per la connessione sicura

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

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

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

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

La chiave privata viene utilizzata nei seguenti casi:

a) Creazione delle chiavi pubbliche e dei certificati.

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



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

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

b) Autenticazione di Server Dr.Web.

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

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

c) Decifratura dei dati.

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

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

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

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

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

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

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

Il certificato viene utilizzato nei seguenti casi:

a) Autenticazione di Server Dr.Web.

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

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

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



b) *Cifratura dei dati.*

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

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

d) *Autenticazione di Server proxy.*

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

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

4. Chiave privata di web server.

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

5. Certificato di web server.

È disponibile per tutti i componenti della rete antivirus.

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

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

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

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

4.3.3. Connessione dei client al Server Dr.Web

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

Al Server Dr.Web possono connettersi i seguenti client:

- **Agent Dr.Web.**

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



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

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

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

• **Installer di Agent Dr.Web.**

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

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

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

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

• **Server Dr.Web adiacenti.**

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

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

• **Server proxy Dr.Web.**

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

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



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



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

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

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



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

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

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

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

Per maggiori informazioni v. **Guida all'installazione**, [Installazione di Server Dr.Web per SO Windows](#) e [Utilizzo del protocollo SRV](#).

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

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

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

Per maggiori informazioni v. [Configurazione di calendario del Server Dr.Web](#).

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

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



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

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

Per maggiori informazioni v. [Autenticazione degli amministratori](#).

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

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

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

Per maggiori informazioni v. **Guida all'installazione**, [Installazione di Agent Dr.Web con utilizzo del servizio Active Directory](#).

5. Ricerca delle postazioni del dominio Active Directory

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

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

Per maggiori informazioni v. [Scanner di rete](#).

6. Ricerca degli utenti del dominio Active Directory

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

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



Capitolo 5: Componenti della rete antivirus e la loro interfaccia

5.1. Server Dr.Web

Una rete antivirus costruita sulla base di Dr.Web Enterprise Security Suite 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 Dr.Web. In tale caso, il software server viene installato su più computer contemporaneamente.

Server Dr.Web è un servizio residente in memoria operativa. Il software Server Dr.Web è progettato per diversi sistemi operativi (per l'elenco completo dei sistemi operativi supportati v. **Guida all'installazione**, sezione [Requisiti di sistema](#)).

Funzioni principali

Il Server Dr.Web svolge le seguenti funzioni:

- avviare un'installazione dei pacchetti antivirus su un computer selezionato o in un gruppo di computer selezionato,
- 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 directory di installazione centralizzata e della directory di aggiornamento,
- 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

Server Dr.Web fornisce la raccolta e la registrazione delle informazioni sul funzionamento dei pacchetti antivirus, che vengono trasmesse su di esso dal software sui computer protetti (Agent Dr.Web, per maggiori informazioni v. sotto). Le informazioni vengono registrate in un log degli eventi generale realizzato sotto forma di database. In una rete di piccole dimensioni (non più di 400–600 computer) per la registrazione degli eventi nel log generale può essere utilizzato il database interno. Per le reti di grandi dimensioni si consiglia di utilizzare un database esterno.



Il database incorporato è progettato per la connessione al Server Dr.Web di circa 400–600 postazioni. Se lo permettono la configurazione dell'hardware del computer su cui è



installato il Server Dr.Web e il carico di altri compiti eseguiti su questo computer, è possibile connettere circa 1000–1500 postazioni.

Altrimenti, è necessario utilizzare un database esterno. A seconda della configurazione e del carico sul computer che svolge le funzioni di Server Dr.Web, il database esterno può essere collocato sullo stesso computer o su un computer dedicato.

Se è utilizzato un database esterno e al Server Dr.Web sono connesse più di 10000 postazioni, sono consigliabili i seguenti requisiti minimi:

- processore con velocità 3GHz,
- da 6 core del processore,
- 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 antivirus della postazione, nonché la versione del software,
- ora e data di aggiornamento dei database dei virus, nonché le sue versioni,
- versione del SO installato sui computer protetti, tipo di processore, posizione delle directory di sistema del SO ecc.,
- configurazione e modalità di funzionamento dei pacchetti antivirus,
- eventi di virus: nome del virus informatico rilevato, data di rilevamento, azioni eseguite, il risultato della cura ecc.

Il Server Dr.Web avvisa l'amministratore della rete antivirus sul verificarsi di eventi relativi al funzionamento della rete antivirus tramite la posta elettronica o gli strumenti broadcast standard dei sistemi operativi Windows. La configurazione degli eventi che provocano l'invio degli avvisi e di altri parametri di avviso è descritta in p. [Configurazione degli avvisi](#).

Web server

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

- autenticazione e autorizzazione di amministratori nel Pannello di controllo;
- automatizzazione del funzionamento delle pagine del Pannello di controllo;
- supporto di pagine dinamicamente generate del Pannello di controllo;
- supporto di connessioni sicure HTTPS con i client.



5.1.1. Gestione di Server Dr.Web sotto SO Windows

Interfaccia e gestione del Server Dr.Web

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

Gli elementi che consentono di effettuare la configurazione e la gestione di base del Server Dr.Web vengono collocati nel menu principale di SO Windows **Programmi** nella directory **Dr.Web Server** nel processo di installazione di Server Dr.Web:

- La directory **Gestione del server** contiene i seguenti comandi:
 - **Log dettagliato** — per impostare il livello di dettaglio **Tutto** per il log di funzionamento del Server Dr.Web.
 - **Avvia** — per avviare il servizio Server Dr.Web.
 - **Arresta** — per arrestare il servizio Server Dr.Web.
 - **Ricarica il repository da disco** — per rileggere da disco il repository del Server Dr.Web.
 - **Ricarica modelli** — per rileggere i modelli di avviso dell'amministratore.
 - **Riavvia** — per riavviare il servizio Server Dr.Web.
 - **Verifica database** — per avviare una verifica del database incorporato.
 - **Log standard** — per impostare il livello di dettaglio **Informazioni** per il log di funzionamento del Server Dr.Web.



Dopo l'esecuzione dei comandi **Log dettagliato** e **Log standard** è necessario riavviare il Server Dr.Web per applicare le modifiche. Per tale scopo eseguire il comando **Riavvia**.



Le impostazioni avanzate di registrazione del log sono disponibili nella sezione [Log](#) del Pannello di controllo.

I relativi comandi sono descritti in maggior dettaglio in documento **Allegati**, [G3. Server Dr.Web](#).

- La voce **Interfaccia web** — per aprire il Pannello di controllo e per connettersi al Server Dr.Web installato su questo computer (sull'indirizzo <http://localhost:9080>).
- La voce **Documentazione** — per aprire la documentazione dell'amministratore in formato HTML.

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

La directory di installazione di default (può essere modificata durante l'installazione): c :
\\Program Files\\DrWeb Server

- **bin** — file eseguibili di Server Dr.Web.



- `ds-modules` — moduli di script decompressi.
- `etc` — file di configurazione principali dei componenti della rete antivirus.
- `fonts` — tipi di carattere per documenti PDF.
- `var` — la directory contiene le sottodirectory:
 - `backup` — backup dei database e di altri dati critici.
 - `extensions` — script di procedure personalizzate, ideati per automatizzare l'esecuzione di determinati task.
 - `file-cache` — cache dei file.
 - `installers-cache` — cache per memorizzare i pacchetti di installazione Agent Dr.Web individuali e di gruppo alla creazione di postazioni nel Pannello di controllo. Viene creata alla creazione dei pacchetti di installazione.
 - `plugins` — oggetti temporanei dei plugin.
 - `objects` — cache degli oggetti del Pannello di controllo.
 - `reports` — directory temporanea per la generazione e la memorizzazione dei report. Viene creata, se necessario.
 - `repository` — directory del repository in cui vengono messi gli aggiornamenti attuali dei database dei virus, dei file dei pacchetti antivirus e dei componenti della rete antivirus. La directory include le sottodirectory per i singoli componenti software funzionali e all'interno di esse si trovano le sottodirectory per i singoli sistemi operativi. La directory deve essere scrivibile per l'account utente sotto cui viene avviato il Server Dr.Web (di regola, è l'utente **LocalSystem**).
 - `sessions` — sessioni del Pannello di controllo.
 - `tmp` — file temporanei.
 - `twin-cache` — database dei virus decompressi per la retrocompatibilità con le versioni precedenti di Agent Dr.Web. Può inoltre contenere altri file decompressi dal repository, per esempio, un installer di Agent Dr.Web.
 - `upload` — directory per il caricamento di file temporanei che vengono impostati tramite il Pannello di controllo. Viene creata al caricamento di file di grandi dimensioni.
- `vfs` — moduli di script e language pack compressi.
- `webmin` — elementi del Pannello di controllo.
- `websockets` — script per l'uso di web socket.

La directory di backup (può essere modificata durante la rimozione): `<disco_di_installazione>` :
`\Drweb Backup`.



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



File di configurazione principali

File	Descrizione	Directory predefinita
agent.key (il nome può essere diverso)	chiave di licenza di Agent Dr.Web	etc
certificate.pem	certificato per SSL	
database.conf	modello di impostazione del database con i parametri di default	
download.conf	impostazioni di rete per la generazione dei pacchetti di installazione di Agent Dr.Web	
drwcsd.conf (il nome può essere diverso)	file di configurazione del Server Dr.Web.	
drwcsd.conf.distr	modello di file di configurazione di Server Dr.Web con i parametri di default	
drwcsd.pri	chiave di cifratura privata	
enterprise.key (il nome può essere diverso)	chiave di licenza di Server Dr.Web. Viene salvata solo se era presente dopo l'aggiornamento dalle versioni precedenti. Se viene installato un nuovo Server Dr.Web 13.0, è assente	
frontdoor.conf	file di configurazione per l'utility di diagnostica remota del Server Dr.Web	
http-alerter-certs.pem	certificati per la convalida dell'host apple-notify.drweb.com nel caso di invio delle notifiche push	
private-key.pem	chiave privata RSA	
yalocator.apikey	Chiave API per l'estensione Yandex Locator	
webmin.conf	file di configurazione del Pannello di controllo	
auth-ads.conf	file di configurazione per l'autenticazione esterna degli amministratori attraverso Active Directory	
auth-ldap.conf	file di configurazione per l'autenticazione esterna degli amministratori attraverso LDAP	
auth-ldap-rfc4515.conf	file di configurazione dell'autenticazione esterna degli amministratori attraverso LDAP in base a uno schema semplificato	



File	Descrizione	Directory predefinita
auth-radius.conf	file di configurazione per l'autenticazione esterna degli amministratori attraverso RADIUS	
database.sqlite	database incorporato	var
*.pub	chiave di cifratura pubblica	sezione Amministrazione → Chiavi di crittografia nel Pannello di controllo

Avvio e arresto di Server Dr.Web

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

Inoltre, Server Dr.Web può essere avviato, riavviato o arrestato 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** di 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 sottodirectory `bin` della directory di installazione di Server Dr.Web (v. inoltre documento **Allegati**, [G3. Server Dr.Web](#)):
 - `drwcsd start` — avvio del Server Dr.Web.
 - `drwcsd restart` — riavvio completo del servizio Server Dr.Web.
 - `drwcsd stop` — arresto normale del Server Dr.Web.



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



5.1.2. Gestione di Server Dr.Web sotto SO della famiglia UNIX

Interfaccia e gestione del Server Dr.Web

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

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

`/opt/drwcs/` in caso di SO Linux e `/usr/local/drwcs` in caso di SO FreeBSD:

- `bin` — file eseguibili di Server Dr.Web.
- `doc` — file dei contratti di licenza.
- `ds-modules` — moduli di script decompressi.
- `fonts` — tipi di carattere per documenti PDF.
- `lib` — set di librerie per il funzionamento di Server Dr.Web.
- `vfs` — moduli di script e language pack compressi.
- `webmin` — elementi del Pannello di controllo.
- `websockets` — script per l'uso di web socket.

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

- `backup` — backup dei database e di altri dati critici.
- `coredump` — dump di arresto anomalo di Server Dr.Web. Viene creato alla comparsa dei dump.
- `etc` — file di configurazione principali dei componenti della rete antivirus.
- `extensions` — script di procedure personalizzate, ideati per automatizzare l'esecuzione di determinati task.
- `installers-cache` — cache per memorizzare i pacchetti di installazione Agent Dr.Web individuali e di gruppo alla creazione di postazioni nel Pannello di controllo. Viene creata alla creazione dei pacchetti di installazione.
- `file-cache` — cache dei file.
- `log` — file di log di Server Dr.Web.
- `plugins` — oggetti temporanei dei plugin.
- `objects` — cache degli oggetti del Pannello di controllo.
- `reports` — directory temporanea per la generazione e la memorizzazione dei report. Viene creata, se necessario.
- `repository` — directory di aggiornamento in cui vengono messi gli aggiornamenti attuali dei database dei virus, dei file dei pacchetti antivirus e dei componenti della rete antivirus. La directory include le sottodirectory per i singoli componenti software funzionali e all'interno di esse si trovano le sottodirectory per i singoli sistemi operativi. La



directory deve essere scrivibile per l'account utente sotto cui viene avviato il Server Dr.Web (di regola, è l'utente **drwcs**).

- `run` — ID del processo Server Dr.Web.
- `sessions` — sessioni del Pannello di controllo.
- `tmp` — file temporanei.
- `twin-cache` — database dei virus decompressi per la retrocompatibilità con le versioni precedenti di Agent Dr.Web. Può inoltre contenere altri file decompressi dal repository, per esempio, un installer di Agent Dr.Web.
- `upload` — directory per il caricamento di file temporanei che vengono impostati tramite il Pannello di controllo. Viene creata al caricamento di file di grandi dimensioni.

`/etc/opt/drweb.com/` in caso di SO Linux e `/usr/local/etc/drweb.com` in caso di SO FreeBSD:

- `software/drweb-esuite.remove` — script per la rimozione del Server Dr.Web.
- sono possibili file e directory aggiuntivi.

`/usr/local/etc/rc.d/` in caso di SO FreeBSD:

- `drwcsd` — script per l'avvio e l'arresto del Server Dr.Web.

`/var/tmp/drwcs` — backup dopo la rimozione del Server Dr.Web.

File di configurazione principali

File	Descrizione	Directory predefinita
<code>agent.key</code> (il nome può essere diverso)	chiave di licenza di Agent Dr.Web	<ul style="list-style-type: none">• in caso di SO Linux: <code>/var/opt/drwcs/etc</code>• in caso di 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>database.conf</code>	modello di impostazione del database con i parametri di default	
<code>download.conf</code>	impostazioni di rete per la generazione dei pacchetti di installazione di Agent Dr.Web	
<code>drwcsd.conf</code> (il nome può essere diverso)	file di configurazione del Server Dr.Web.	
<code>drwcsd.conf.distr</code>	modello di file di configurazione di Server Dr.Web con i parametri di default	
<code>drwcsd.pri</code>	chiave di cifratura privata	



File	Descrizione	Directory predefinita
<code>enterprise.key</code> (il nome può essere diverso)	chiave di licenza di Server Dr.Web. Viene salvata solo se era presente dopo l'aggiornamento dalle versioni precedenti. Se viene installato un nuovo Server Dr.Web 13.0, è assente	
<code>frontdoor.conf</code>	file di configurazione per l'utility di diagnostica remota del Server Dr.Web	
<code>http-alerter-certs.pem</code>	certificati per la convalida dell'host <code>apple-notify.drweb.com</code> nel caso di invio delle notifiche push	
<code>private-key.pem</code>	chiave privata RSA	
<code>yalocator.apikey</code>	Chiave API per l'estensione Yandex Locator	
<code>webmin.conf</code>	file di configurazione del Pannello di controllo	
<code>auth-ldap.conf</code>	file di configurazione per l'autenticazione esterna degli amministratori attraverso LDAP	
<code>auth-ldap-rfc4515.conf</code>	file di configurazione dell'autenticazione esterna degli amministratori attraverso LDAP in base a uno schema semplificato	
<code>auth-pam.conf</code>	file di configurazione per l'autenticazione esterna degli amministratori attraverso PAM	
<code>auth-radius.conf</code>	file di configurazione per l'autenticazione esterna degli amministratori attraverso RADIUS	
<code>database.sqlite</code>	database incorporato	<ul style="list-style-type: none">• in caso di SO Linux: <code>/var/opt/drwcs</code>• in caso di SO FreeBSD: <code>/var/drwcs</code>
<code>*.pub</code>	chiave di cifratura pubblica	sezione Amministrazione → Chiavi di crittografia nel Pannello di controllo


Avvio e arresto di Server Dr.Web

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

Inoltre, Server Dr.Web può essere avviato, riavviato o arrestato 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 .
- Tramite il relativo comando console (v, inoltre documento **Allegati**, [G3. Server Dr.Web](#)):
 - Avvio:
 - in caso di SO FreeBSD:

```
# /usr/local/etc/rc.d/drwcsd start
```
 - in caso di SO Linux:

```
# /etc/init.d/drwcsd start
```
 - Riavvio:
 - in caso di SO FreeBSD:

```
# /usr/local/etc/rc.d/drwcsd restart
```
 - in caso di SO Linux:

```
# /etc/init.d/drwcsd restart
```
 - Arresto:
 - in caso di SO FreeBSD:

```
# /usr/local/etc/rc.d/drwcsd stop
```
 - In caso di SO Linux:

```
# /etc/init.d/drwcsd stop
```



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

5.2. Protezione delle postazioni



Le impostazioni dei componenti antivirus, configurabili attraverso il Pannello di controllo, sono descritte dettagliatamente nel **Manuale dell'amministratore** per la gestione delle postazioni per il sistema operativo corrispondente.

Un computer protetto tramite un pacchetto antivirus installato, in conformità con le sue funzioni nella rete antivirus, viene denominato *postazione* della rete antivirus. Va ricordato che a seconda delle sue funzioni svolte nella rete locale tale computer può essere sia una postazione o un dispositivo mobile che un server della rete locale.

Le postazioni vengono protette tramite i pacchetti antivirus Dr.Web progettati per i sistemi operativi corrispondenti.

I pacchetti antivirus vengono installati sulle postazioni protette e si connettono a un Server Dr.Web. Ciascuna postazione fa parte di uno o più gruppi registrati su questo Server Dr.Web (per maggiori informazioni v. p. [Gruppi di sistema e custom](#)). La trasmissione di informazioni tra la postazione e il Server Dr.Web viene effettuata attraverso il protocollo utilizzato nella rete locale (TCP/IP versione 4 o 6).



Installazione

Un pacchetto antivirus può essere installato su una postazione in uno dei seguenti modi:

1. Localmente. L'installazione locale viene eseguita direttamente sul computer o sul dispositivo mobile dell'utente. Può essere eseguita sia dall'amministratore che dall'utente.
2. In remoto. L'installazione remota viene eseguita nel Pannello di controllo attraverso la rete locale. Viene eseguita dall'amministratore della rete antivirus. L'intervento dell'utente in tale caso non è richiesto.



Le procedure di installazione dei pacchetti antivirus su postazioni vengono descritte nel dettaglio nella **Guida all'installazione**.

Gestione

Se la postazione è connessa con il Server Dr.Web, all'amministratore sono disponibili le seguenti funzioni realizzate dal pacchetto antivirus sulla postazione:

- Configurazione centralizzata di Antivirus sulle postazioni tramite il Pannello di controllo.
L'amministratore può vietare all'utente o lasciargli la possibilità di modificare in autonomo le impostazioni di Antivirus sulla postazione.
- Configurazione del calendario di scansioni antivirus e di altri task eseguibili sulla postazione.
- Ottenimento delle statistiche di scansione e di altre informazioni sul funzionamento dei componenti antivirus e sullo stato della postazione.
- Avvio e arresto di una scansione antivirus ecc.

Aggiornamento

Server Dr.Web scarica gli aggiornamenti e li distribuisce sulle postazioni connesse. In questo modo l'ottimale strategia per la protezione dalle minacce viene stabilita, mantenuta e regolata automaticamente a prescindere dal livello di qualifica degli utenti delle postazioni.

Nel caso di una disconnessione provvisoria di una postazione dalla rete antivirus, Antivirus sulla postazione utilizza la copia locale delle configurazioni, la protezione antivirus sulla postazione rimane operativa (durante un periodo che non supera il periodo di validità della licenza di utente), ma il software non viene aggiornato. Se per la postazione è consentito il funzionamento in *Modalità mobile*, quando la postazione si disconnette dal Server Dr.Web, per la postazione sarà disponibile l'aggiornamento dei database dei virus direttamente dai server SAM.

Il principio di funzionamento delle postazioni in modalità mobile è descritto in p.

[Aggiornamento di Agent Dr.Web in modalità mobile.](#)



5.3. 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: **Servizio** → **Opzioni Internet** → **Sicurezza** → **Siti attendibili**.

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

Connessione al Server Dr.Web

Su qualunque computer con accesso di rete al Server Dr.Web, il Pannello di controllo è disponibile sull'indirizzo:

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

o

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

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

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

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



Una password dimenticata può essere ripristinata, v. [Ripristino della password amministratore](#).

In caso di caricamento via HTTPS (connessione sicura SSL), il browser chiede la conferma del certificato utilizzato dal Server Dr.Web. La richiesta della conferma può essere accompagnata dalle supposizioni su quello che il certificato sia inaffidabile 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 versioni successive, in caso di caricamento via HTTPS, viene restituito un errore, e il Pannello di controllo non viene caricato. In questo caso sulla pagina di errore è necessario selezionare la voce **Aggiungi sito alla lista esclusioni** (sotto il messaggio di errore). Dopo questa operazione 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 [5-1](#)) è suddivisa in *intestazione del menu principale* e in *area operativa*.

Menu principale

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

- sezione [Amministrazione](#),
- sezione [Rete antivirus](#),
- [Barra di ricerca](#),
- l'account amministratore sotto cui è stato effettuato l'accesso al Pannello di controllo. Inoltre, può essere disponibile il [menu delle relazioni tra i server](#),
- sezione [Eventi](#),
- sezione [Impostazioni](#),
- sezione [Guida](#),
- pulsante **Esci** per terminare la sessione corrente di utilizzo del Pannello di controllo.

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 del pannello centrale.

La lingua dell'interfaccia viene impostata separatamente per ciascun account amministratore (v. p. [Creazione ed eliminazione degli account amministratori e dei gruppi](#)).

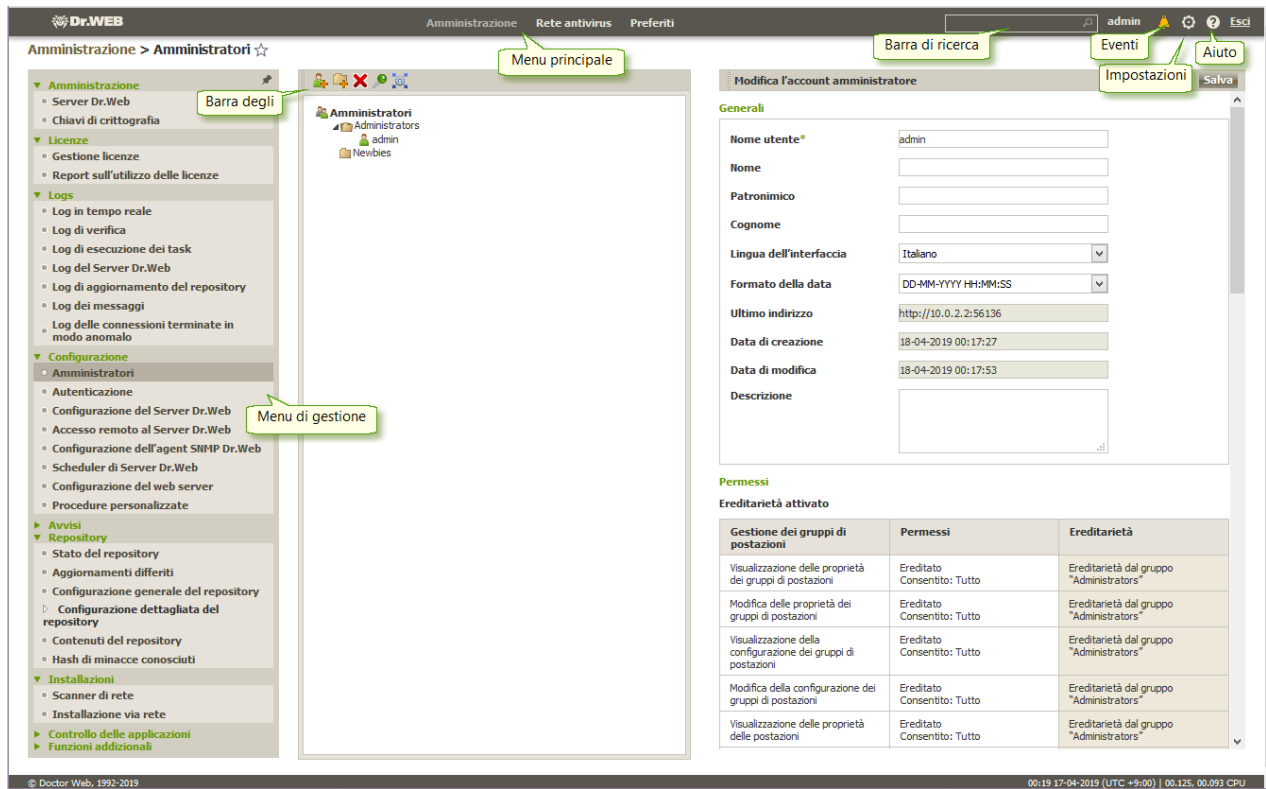


Immagine 5-1. Finestra del Pannello di controllo della sicurezza Dr.Web. Fare clic sugli elementi nella casella verde per andare alla sezione corrispondente

Menu di gestione

Per visualizzare e modificare le informazioni, utilizzare il menu di gestione locato nella parte sinistra della finestra.

Il menu di gestione può essere minimizzato. In questo caso verranno visualizzati soltanto i nomi delle sezioni del menu. Al passaggio del mouse sopra una sezione vengono visualizzate le voci del menu disponibili in questa sezione.

Per gestire la visualizzazione del menu di gestione, si utilizzano le icone locate nell'angolo superiore destro:

🔓 **Sblocca menu** — per levare il blocco e visualizzare il menu in forma minimizzata.

🔒 **Blocca menu** — per bloccare la posizione espansa del menu.

Menu delle relazioni tra i server





Le informazioni relative all'organizzazione di una rete antivirus con diversi server e alla configurazione delle relazioni tra i server vengono riportate nella sezione [Caratteristiche di una rete con diversi Server Dr.Web](#).



Se ci sono le relazioni di tipo "tra i server" con altri Server Dr.Web, le seguenti funzioni vengono aggiunte per il nome utente amministratore al menu principale:

- Accanto al nome amministratore viene visualizzato il nome del Server Dr.Web corrente.
- Quando si fa clic sul nome amministratore, si apre una lista a discesa dei Server Dr.Web collegati. Se il nome non è impostato per una relazione, viene visualizzato il suo identificatore.

Quando si fa clic su una relazione, sono possibili due varianti delle azioni:

- Si apre il Pannello di controllo del Server Dr.Web collegato, se durante la configurazione della relazione è stato indicato l'indirizzo IP del Pannello di controllo. L'azione è analoga a quella del pulsante  →  nella barra degli strumenti per la gestione delle relazioni.
- Se l'indirizzo del Pannello di controllo del Server Dr.Web adiacente non è impostato per questa relazione, si apre la sezione di configurazione delle relazioni in modo che sia possibile impostare l'indirizzo IP.

5.3.1. Amministrazione



Selezionare la voce **Amministrazione** nel menu principale del Pannello di controllo.

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. Amministrazione

- **Server Dr.Web** — apre un pannello attraverso cui è possibile visualizzare informazioni principali sul Server Dr.Web, nonché riavviarlo tramite il pulsante  o arrestarlo tramite il pulsante , situati nella parte superiore destra del pannello. Inoltre, se ci sono aggiornamenti di Server Dr.Web scaricati, da questa sezione è disponibile la sezione [Aggiornamenti di Server Dr.Web](#) con una lista delle versioni di Server Dr.Web per l'aggiornamento e il backup. Per ripristinare l'integrità del Server Dr.Web e tornare allo stato della revisione corrente, premere il pulsante **Ripristina Server**.
- **Chiavi di crittografia** — consente di esportare (salvare localmente) le chiavi di crittografia pubblica e privata e inoltre il certificato di Server Dr.Web.

2. Licenze

- [Gestione licenze](#) — consente di gestire i file della chiave di licenza.
- [Report sull'utilizzo delle licenze](#) — contiene informazioni sull'uso delle licenze, tra l'altro anche sui Server Dr.Web adiacenti.



3. Log

- [Log in tempo reale](#) — consente di visualizzare una lista di eventi e modifiche relativi al funzionamento di Server Dr.Web che vengono restituiti in tempo reale (immediatamente al momento del verificarsi di un evento).
- [Log di verifica](#) — consente di visualizzare la lista degli eventi e delle modifiche apportate tramite i sottosistemi di gestione di Dr.Web Enterprise Security Suite.
- **Log di esecuzione dei task** — contiene l'elenco dei task impostati sul Server Dr.Web con una nota sull'esecuzione e commenti.
- [Log del Server Dr.Web](#) — contiene l'elenco dei log degli eventi relativi al funzionamento del Server Dr.Web.
- [Log di aggiornamento del repository](#) — contiene un elenco di aggiornamenti da SAM che include informazioni dettagliate sulle revisioni aggiornate dei prodotti.
- [Log dei messaggi](#) — contiene tutti i messaggi di testo che sono stati inviati dall'amministratore sulle postazioni della rete antivirus.
- **Log delle connessioni terminate in modo anomalo** — contiene tutti i casi di interruzioni anomale delle connessioni del Server Dr.Web con i client: postazioni, installer di Agent Dr.Web, Server Dr.Web adiacenti, Server proxy.

4. Configurazione

- [Amministratori](#) — apre il pannello di gestione degli account amministratori della 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 Dr.Web.
- [Accesso remoto al Server Dr.Web](#) — contiene le impostazioni per la connessione dell'utility di diagnostica remota del Server Dr.Web.
- [Configurazione dell'agent SNMP Dr.Web](#) — apre il pannello di configurazione dei parametri di connessione all'agent SNMP Dr.Web.
- [Scheduler di Server Dr.Web](#) — apre il pannello di configurazione del calendario dei task del Server Dr.Web.
- [Configurazione del web server](#) — apre il pannello delle impostazioni principali del Web server.
- [Procedure personalizzate](#) — apre il pannello delle impostazioni delle procedure personalizzate.


5. Avvisi

- [Avvisi della web console](#) — permette di visualizzare e gestire gli avvisi dell'amministratore ricevuti tramite il metodo **Web console**.



- [Avvisi non inviati](#) — permette di rintracciare e gestire gli avvisi dell'amministratore che non è stato possibile inviare secondo le impostazioni della sezione **Configurazione degli avvisi**.
- [Configurazione degli avvisi](#) — permette di configurare gli avvisi dell'amministratore sugli eventi della rete antivirus.
- [Modelli di messaggio](#) — lista dei modelli di messaggio di testo che vengono inviati dall'amministratore sulle postazioni della rete antivirus.

6. Repository

- [Stato del repository](#) — permette di controllare lo stato del repository: data di ultimo aggiornamento dei componenti del repository e il loro stato. E inoltre, permette di aggiornare il repository da SAM.
- [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 delle impostazioni di connessione a SAM e di 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 file del repository.
- **Hash di minacce conosciuti** — consente di eseguire la ricerca nei bollettini con gli hash di minacce conosciuti. Per cercare per campo della tabella degli hash, premere il pulsante .

La sezione è disponibile solo se è stato concesso in licenza l'uso dei bollettini degli hash di minacce conosciuti. La presenza di una licenza è riportata nelle informazioni sulla chiave di licenza che possono essere visualizzate nella sezione [Gestione licenze](#), parametro **Liste consentite dei bollettini di hash** (è sufficiente una licenza in almeno una delle chiavi di licenza utilizzate dal Server Dr.Web).

7. Installazioni

- [Scanner di rete](#) — permette di impostare una lista delle reti e scansionare le reti, cercando il software antivirus installato, determinando lo stato di protezione dei computer, nonché di installare il software antivirus.
- **Installazione via rete** — permette di semplificare l'installazione del software Agent Dr.Web su postazioni specifiche (v. **Guida all'installazione**, p. [Installazione di Agent Dr.Web con utilizzo del Pannello di controllo della sicurezza Dr.Web](#)).



8. Controllo delle applicazioni

- [Applicazioni affidabili](#) — liste delle applicazioni il cui avvio è sempre consentito sulle postazioni con il componente installato Controllo delle applicazioni (le liste consentite vengono selezionate nelle impostazioni del [profilo](#) assegnato alla postazione).
- [Prontuario applicazioni](#) — lista di tutte le applicazioni installate sulle postazioni.

9. Funzioni aggiuntive

- [Gestione del database](#) — consente di fare la manutenzione diretta del database con cui interagisce Server Dr.Web.
- [Statistiche del Server Dr.Web](#) — contiene le statistiche di funzionamento di questo Server Dr.Web.
- **Console SQL** — fornisce la possibilità di eseguire query SQL al database utilizzato dal Server Dr.Web.
- **Console Lua** — fornisce la possibilità di eseguire script Lua, sia quelli digitati direttamente nella console che quelli caricati da file.



L'amministratore con l'accesso alla console Lua ottiene l'accesso a tutto il file system all'interno della directory di Server Dr.Web e ad alcuni comandi di sistema sul computer con il Server Dr.Web installato.

Per vietare l'accesso alla console Lua, disattivare il permesso **Funzioni aggiuntive** per il relativo amministratore (v. p. [Amministratori e gruppi di amministratori](#)).

- [Copie di backup](#) — consente di visualizzare e salvare i contenuti delle copie di backup dei dati critici del Server Dr.Web.
- [Utility](#) — apre una sezione per il caricamento delle utility aggiuntive per l'utilizzo di Dr.Web Enterprise Security Suite.

5.3.2. Rete antivirus

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

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](#)
- [Identificatori di protezione](#)



- [Componenti di protezione](#)
- [Quarantena](#)
- [Hardware e software](#)
- **Dispositivi rilevati**
- **Sessioni degli utenti**
- **Postazioni non attive**
- [Proprietà](#)
- [Regole di appartenenza al gruppo](#) (in caso di selezione di un gruppo definito dall'utente)
- [Server proxy Dr.Web](#) (quando vengono selezionati i Server proxy o il loro gruppo)

2. [Statistiche](#)

3. Configurazione

- [Server proxy Dr.Web](#) (se viene selezionato un Server proxy o il gruppo **Proxies** con i relativi sottogruppi)
- [Permessi](#)
- [Scheduler](#)
- [Componenti da installare](#)
- [Parametri di connessione](#)
- [Limitazioni degli aggiornamenti](#)
- **Agent Dr.Web per UNIX** — consente di configurare la periodicità di invio delle statistiche di minacce rilevate per le postazioni sotto SO della famiglia UNIX.
- 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 antivirus, configurabili attraverso il Pannello di controllo, sono descritte dettagliatamente nel **Manuale dell'amministratore** per la gestione delle postazioni per il sistema operativo corrispondente.

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 MAIUSCOLO.

L'aspetto dell'icona di un elemento della lista dipende dal tipo o dallo stato di questo elemento (vedi [tabella 5-1](#)).

Tabella 5-1. Icone degli elementi della lista gerarchica

Icona	Descrizione
Gruppi. Icone principali	
	Gruppi visualizzati sempre nella lista gerarchica.
	<p>I gruppi non verranno visualizzati nella lista gerarchica se:</p> <ul style="list-style-type: none"> • ai gruppi è stata applicata l'azione  Imposta la visibilità del gruppo →  Nascondi se vuoto e al momento i gruppi non contengono postazioni, • ai gruppi è stata applicata l'azione  Imposta la visibilità del gruppo →  Nascondi e al momento nella sezione  Impostazioni della vista albero è deselezionato il flag Mostra gruppi nascosti.
	<p>L'icona di regole di appartenenza viene visualizzata accanto all'icona principale dei gruppi personalizzati per cui sono state stabilite le regole di collocamento automatico delle postazioni nel gruppo.</p> <p>Per visualizzare l'icona, selezionare nella barra degli strumenti  Impostazioni della vista albero → Mostra icona delle regole di appartenenza.</p>
Postazioni. Icone principali	
	Postazione disponibile con il software antivirus installato.
	<p>Questa è una postazione disponibile con il software antivirus installato. La gravità dello stato della postazione è Media. Per determinare le azioni dell'amministratore richieste, precisare la situazione su questa postazione nella sezione Stato.</p> <p>Per visualizzare l'icona, selezionare nella barra degli strumenti  Impostazioni della vista albero → Mostra gravità dello stato delle postazioni.</p>
	<p>Questa è una postazione disponibile con il software antivirus installato. La gravità dello stato della postazione è Massima o Alta. Per determinare le azioni dell'amministratore richieste, precisare la situazione su questa postazione nella sezione Stato.</p>



Icona	Descrizione
	Per visualizzare l'icona, selezionare nella barra degli strumenti  Impostazioni della vista albero → Mostra gravità dello stato delle postazioni.
	Postazione non disponibile.
	Software antivirus su postazione è disinstallato.
	Stato della postazione in caso di installazione remota di Agent Dr.Web via rete. La postazione si trova in tale stato dal momento di un'installazione riuscita di Agent Dr.Web su questa postazione fino al momento della prima connessione della postazione al Server Dr.Web.
Server proxy. Icone principali	
	Server proxy non connesso al Server Dr.Web.
	Il Server proxy è connesso al Server Dr.Web, ma non utilizza le impostazioni configurate per esso.
	Il Server proxy è connesso al Server Dr.Web e utilizza le impostazioni configurate per esso.
Server di scansione. Icone principali	
	Server di scansione disponibile.
	Server di scansione disponibile. La gravità dello stato è Media . Per determinare le azioni dell'amministratore richieste, precisare la situazione su questo Server di scansione nella sezione Stato . Per visualizzare l'icona, selezionare nella barra degli strumenti  Impostazioni della vista albero → Mostra gravità dello stato delle postazioni.
	Server di scansione disponibile. La gravità dello stato è Massima o Alta . Per determinare le azioni dell'amministratore richieste, precisare la situazione su questo Server di scansione nella sezione Stato . Per visualizzare l'icona, selezionare nella barra degli strumenti  Impostazioni della vista albero → Mostra gravità dello stato delle postazioni.
	Server di scansione non disponibile.
Icone aggiuntive per gruppi, postazioni, Server proxy e Server di scansione	
	L'icona delle impostazioni individuali viene visualizzata sulle icone principali delle postazioni, dei gruppi, dei Server proxy e Server di scansione per cui sono state definite le impostazioni individuali. Per visualizzare l'icona, selezionare nella barra degli strumenti  Impostazioni della vista albero → Mostra icona delle impostazioni individuali. Per esempio, se le impostazioni individuali sono definite per una postazione con il software antivirus installato attualmente sulla rete, la sua icona avrà il seguente aspetto:  .



Icona	Descrizione
Criteri	
	Criterio o versione di un criterio con le impostazioni dei componenti antivirus delle postazioni. Per visualizzare l'icona, selezionare nella barra degli strumenti Impostazioni della vista albero → Mostra icona del criterio .
Profili	
	Profilo in cui sono memorizzate impostazioni del componente Controllo applicazioni, modalità attiva.
	Profilo in cui sono memorizzate impostazioni del componente Controllo applicazioni, modalità di test.
	Profilo disattivato in cui sono memorizzate impostazioni del componente Controllo applicazioni.
	Profilo per la conservazione delle impostazioni del componente Controllo applicazioni per cui è impostato un gruppo di applicazioni affidabili che non è presente nel repository del Server Dr.Web.

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 i parametri generali della lista gerarchica. Selezionare la voce corrispondente dalla lista a cascata:

✖ **Rimuovi gli oggetti selezionati** — per rimuovere oggetti della lista gerarchica. Per fare ciò, selezionare uno o più oggetti dalla lista e fare clic su **Rimuovi gli oggetti selezionati**.


✖ **Rimuovi le regole di appartenenza** — per rimuovere le regole di sistemazione automatica di postazioni in gruppi.


1 **Imposta questo gruppo come primario** — per impostare come primario un gruppo selezionato nella lista gerarchica per tutte le postazioni che ne fanno parte.


1 **Assegna gruppo primario alle postazioni** — per assegnare il gruppo primario alle postazioni selezionate nella lista gerarchica. In questo caso se nella lista gerarchica è selezionato un gruppo, a tutte le postazioni che ne fanno parte verrà assegnato il gruppo primario selezionato.


🌿 **Unisci postazioni** — per unire postazioni sotto un singolo account nella lista gerarchica. Può essere utilizzata quando una stessa postazione è stata registrata sotto diversi account.





 **Rimuovi impostazioni individuali** — per rimuovere le impostazioni individuali dell'oggetto selezionato nella lista. In tale caso l'oggetto eredita le impostazioni dal gruppo primario. Se nella lista gerarchica è selezionato un gruppo, le impostazioni verranno rimosse anche a tutte le postazioni che ne fanno parte.


 [Invia messaggio su postazioni](#) — per inviare agli utenti un messaggio di contenuto arbitrario.


 **Riavvia la postazione** — per lanciare in remoto il processo di riavvio di una postazione. Per scoprire se è richiesto il riavvio di una postazione, per esempio, in connessione con l'aggiornamento/la modifica di componenti antivirus, andare alla sezione [Stato](#) per questa postazione.


 **Disinstalla Agent Dr.Web** — per rimuovere l'Agent Dr.Web e il software antivirus dalla postazione o dal gruppo di postazioni selezionato.

 **Installa Agent Dr.Web** — per aprire [Scanner di rete](#) per installare l'Agent Dr.Web sulle postazioni selezionate. Questa voce è attiva solo se vengono selezionate postazioni nuove confermate o postazioni con Agent Dr.Web disinstallato.


 [Recupera le postazioni rimosse](#) — per recuperare le postazioni precedentemente rimosse. Questa voce è attiva solo se postazioni vengono selezionate dal sottogruppo **Deleted** nel gruppo **Status**.


 [Invia i file di installazione](#) — per inviare i file di installazione per le postazioni selezionate nella lista sugli indirizzi email definiti nelle impostazioni di questa sezione.

 [Annulla l'assegnazione del profilo agli oggetti](#) — per rimuovere il profilo dalla lista dei profili assegnati agli oggetti selezionati. La voce è attiva quando si selezionano oggetti cui è assegnato il profilo (sono visualizzati nell'albero come oggetti nidificati di questo profilo).

 [Crea il report per il supporto tecnico](#) — per raccogliere un report di supporto tecnico contenente informazioni di sistema per una postazione o un gruppo di postazioni.


+ Aggiungi oggetto della rete — per creare un nuovo elemento della rete antivirus. Per fare ciò, selezionare la voce corrispondente dalla lista a cascata:


 **Crea postazione** — per creare una nuova postazione (v. **Guida all'installazione**, p. [Installazione di Agent Dr.Web attraverso il pacchetto di installazione individuale](#)).

 **Crea gruppo** — per creare un nuovo gruppo di postazioni.


 **Crea relazione** — per creare una relazione con un Server Dr.Web adiacente.

 **Crea criterio** — per creare un nuovo criterio che definisce le impostazioni di postazioni.


 **Crea Server proxy** — per creare un nuovo account per la connessione di un Server proxy (v. **Guida all'installazione**, p. [Creazione dell'account del Server proxy Dr.Web](#)).


 **Crea profilo** — per creare un nuovo profilo in cui vengono memorizzate le impostazioni di componenti antivirus delle postazioni.


 **Dati e configurazione:**

 **Registra le informazioni in file CSV** — per registrare dati generali sulle postazioni selezionate della rete antivirus in un file in formato CSV.




 **Registra le informazioni in file HTML** — per registrare dati generali sulle postazioni selezionate della rete antivirus in un file in formato HTML.


 **Registra le informazioni in file XML** — per registrare dati generali sulle postazioni selezionate della rete antivirus in un file in formato XML.


 **Registra le informazioni in file PDF** — per registrare dati generali sulle postazioni selezionate della rete antivirus in un file in formato PDF.





Quando vengono selezionate le opzioni sopraelencate dalla sezione **Dati e configurazione**, verranno esportate solo le informazioni sulle postazioni selezionate e sulle postazioni che fanno parte dei gruppi selezionati.


 **Esporta la configurazione** — per salvare in file la configurazione di un oggetto selezionato della rete antivirus. Per questa opzione verrà offerto di selezionare le sezioni di configurazione da salvare.


 **Importa la configurazione** — per caricare da file la configurazione di un oggetto selezionato della rete antivirus. Per questa opzione verrà offerto di selezionare un file da cui verrà caricata la configurazione e inoltre le sezioni di configurazione da caricare.


 **Esporta le statistiche** — per salvare in file le statistiche di funzionamento dei componenti antivirus per gli oggetti selezionati della rete antivirus. Per questa opzione verrà offerto di selezionare le sezioni delle statistiche da salvare e il formato di esportazione.


 **Propaga la configurazione** — per propagare la configurazione di un oggetto selezionato verso altri oggetti della rete antivirus. Per questa opzione verrà offerto di selezionare oggetti su cui verrà propagata la configurazione e inoltre le sezioni di configurazione da propagare.

 **Assegna criterio** — per assegnare il criterio selezionato a un gruppo o singole postazioni. Per questa opzione verrà richiesto di selezionare gli oggetti a cui può essere assegnato il criterio selezionato.


 **Assegna il profilo** — per assegnare un profilo con impostazioni, selezionato nell'albero della rete antivirus, agli oggetti: postazioni, utenti e gruppi. Per questa opzione, verrà offerto di selezionare gli oggetti a cui verrà assegnato il profilo.

 **Imposta la visibilità del gruppo.** Consente di modificare i parametri di visualizzazione dei gruppi. Per questo scopo, selezionare un gruppo dalla lista gerarchica e indicare nella lista a cascata una delle seguenti varianti (l'icona del gruppo cambierà, vedi [tabella 5-1](#)):


 **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 fare ciò, selezionare dalla lista a cascata una delle seguenti varianti:




 **Ripristina i componenti falliti** — per ripristinare forzatamente lo stato dei componenti che non funzionano correttamente. Viene ripristinata la revisione del prodotto che è attualmente installata sulla postazione.

 **Interrompi i componenti in esecuzione** — per interrompere il funzionamento di tutti i componenti antivirus in esecuzione sulla postazione. È possibile arrestare e avviare i componenti antivirus separatamente nella sezione [Componenti di protezione](#).


 **Scansiona** — consente di eseguire la scansione di una postazione in una delle modalità selezionate dalla lista a cascata:


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


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


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


 **Scansione personalizzata.** In questa modalità è possibile selezionare qualsiasi cartella e file per la successiva scansione tramite Dr.Web Agent Scanner.

 **Postazioni non confermate** — consente di gestire la lista dei nuovi arrivi — postazioni di cui la registrazione non è confermata (per maggiori informazioni v. sezione [Criteri di approvazione delle postazioni](#)). Questa voce è attiva solo se le postazioni vengono selezionate dal sottogruppo **Newbies** del gruppo **Status**. Quando la registrazione sul Server Dr.Web verrà confermata, le postazioni verranno cancellate automaticamente dal sottogruppo predefinito **Newbies**. Per gestire la registrazione delle postazioni, selezionare dalla lista a cascata una delle seguenti varianti:


 **Consenti l'accesso delle postazioni selezionate e assegna gruppo primario** — per confermare l'accesso della postazione al Server Dr.Web e assegnarle un gruppo primario dalla lista proposta.


 **Annulla l'azione impostata per l'esecuzione al momento della connessione** — per annullare l'azione sulla postazione non confermata, che è stata precedentemente impostata per l'esecuzione al momento della connessione della postazione al Server Dr.Web.

 **Nega l'accesso delle postazioni selezionate** — per negare l'accesso della postazione al Server Dr.Web.

 **Parametri di blocco.** Consente di modificare i parametri di accesso delle postazioni al Server Dr.Web. Dalla lista a cascata selezionare il parametro:






 **Periodo di blocco** — per impostare un intervallo di date durante cui la postazione non potrà accedere al Server Dr.Web.

 **Impostazioni della vista albero** — per modificare l'aspetto dell'albero della rete antivirus. Per attivare il parametro, impostare i flag corrispondenti nel menu a discesa:

- per i gruppi:
 - **Appartenenza a tutti i gruppi** — per duplicare la visualizzazione della postazione nella lista se fa parte di più gruppi allo stesso tempo (solo per i gruppi con l'icona di cartella bianca — vedi [tabella 5-1](#)). Se il flag è selezionato, la postazione è visualizzata in tutti i gruppi di cui fa parte. Se il flag è deselezionato, la postazione è visualizzata una volta nella lista.
 - **Mostra gruppi nascosti** — per 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.
 - **Mostra solo i gruppi con postazioni attivate** — per visualizzare solo i gruppi con postazioni che si sono connesse al Server Dr.Web almeno una volta.
- per i client del Server Dr.Web (postazioni, Server proxy e Server Dr.Web adiacenti):
 - **Mostra identificatori dei client** — per visualizzare gli identificatori univoci dei client del Server Dr.Web.
 - **Mostra nomi dei client** — per visualizzare i nomi dei client del Server Dr.Web, se disponibili.



Non è possibile disattivare contemporaneamente la visualizzazione degli identificatori e dei nomi dei client. Uno dei parametri **Mostra identificatori dei client** e **Mostra nomi dei client** sarà sempre selezionato.

- **Mostra indirizzi dei client** — per visualizzare gli indirizzi IP dei client del Server Dr.Web.
- **Mostra server delle postazioni** — per visualizzare i nomi o gli indirizzi IP dei Server Dr.Web a cui sono connesse le postazioni. Riguarda le postazioni incluse in un cluster dei Server Dr.Web.
- **Mostra icona del criterio** — per visualizzare l'icona del criterio accanto all'icona della postazione a cui è assegnato il criterio.
- **Mostra gravità dello stato delle postazioni** — per visualizzare la gravità dello status per le postazioni attive. Verrà aggiunta una gradazione di colore per le postazioni a seconda del loro status (vedi [tabella 5-1](#)). Se l'opzione è disattivata, per una postazione con gli status cui corrispondono le icone  e  verrà visualizzata un'icona comune .
- **Mostra postazioni bloccate** — per visualizzare le postazioni il cui accesso al Server Dr.Web è bloccato.



- per tutti gli elementi:
 - **Mostra icona delle impostazioni individuali** — per visualizzare un indicatore che denota la presenza di impostazioni individuali sulle icone dei gruppi e dei client del Server Dr.Web: postazioni, Server proxy e Server Dr.Web adiacenti.
 - **Mostra descrizioni** — per visualizzare le descrizioni dei gruppi e dei client del Server Dr.Web: postazioni, Server proxy e Server Dr.Web adiacenti (le descrizioni vengono impostate nelle proprietà di un elemento).
 - **Mostra numero di client** — per visualizzare il numero di client del Server Dr.Web: postazioni, Server proxy e Server Dr.Web adiacenti per tutti i gruppi della rete antivirus in cui questi client sono inclusi.
 - **Mostra icona delle regole di appartenenza** — per visualizzare un indicatore sulle icone delle postazioni che sono state aggiunte a un gruppo in modo automatico secondo le regole di appartenenza, nonché sulle icone dei gruppi a cui le postazioni sono state aggiunte in modo automatico.

🔍 Impostazioni di filtraggio — consente di filtrare gli elementi visualizzati dell'albero della rete antivirus tramite la ricerca in base a parametri impostati. Per impostare i criteri di ricerca, spuntare i flag di fronte ai criteri richiesti dalla lista a cascata. Nel campo **Ricerca** inserire la stringa di ricerca. Premere **Applica** per iniziare la ricerca in base ai parametri impostati.

I criteri di ricerca sono analoghi ai criteri descritti in sezione [Barra di ricerca](#), ad eccezione del criterio aggiuntivo **Configurazione**. Il criterio viene utilizzato per la ricerca in base a valori specifici dei parametri dei componenti antivirus installati sulle postazioni. Se viene selezionato questo criterio, si aprirà la barra di ricerca con le seguenti impostazioni:

- **Componente** — dalla lista a cascata selezionare il nome di un componente antivirus, nelle cui impostazioni verrà effettuata la ricerca. Per semplificare la selezione di un componente dalla lista, è possibile utilizzare la ricerca: iniziare a digitare il nome nel campo componente, il sistema proporrà automaticamente le varianti contenenti i caratteri immessi.
- **Parametro** — dalla lista a cascata selezionare il nome del parametro, in base ai valori del quale è disponibile la ricerca. Non è disponibile una ricerca per parametro con una complessa struttura di valori ammissibili.
- **Valore** — impostare il valore del parametro selezionato sopra. A seconda dei valori ammissibili di un parametro specifico, viene fornita o una lista a cascata con i valori ammissibili o un campo di input in cui l'utente può inserire un valore dalla tastiera.

Per resettare i parametri di ricerca impostati, premere il pulsante **Di default**.



↕ Impostazioni di ordinamento dei client — per modificare il parametro di ordinamento e l'ordinamento dei client del Server Dr.Web: postazioni, Server proxy e Server Dr.Web adiacenti nell'albero della rete antivirus.





- Per selezionare il parametro in base a cui verranno ordinate le postazioni, impostare uno dei seguenti flag (è possibile selezionare solo un parametro):
 - **Identificatore** — per ordinare per identificatore del client univoco.
 - **Nome** — per ordinare per nome del client.



- **Indirizzo** — per ordinare per indirizzo di rete del client. I client che non hanno un indirizzo di rete verranno visualizzati in ordine casuale senza essere ordinati.
- **Data di creazione** — per ordinare per data di creazione dell'account di client sul Server Dr.Web.
- **Data dell'ultima connessione** — per ordinare per data dell'ultima connessione al Server Dr.Web.
- Per selezionare la direzione di ordinamento, impostare uno dei seguenti flag:
 - **Ordina crescente.**
 - **Ordina decrescente.**



Le sezioni  **Impostazioni della vista albero** e  **Impostazioni di ordinamento dei client** sono interdipendenti:

- Se viene selezionato un parametro di ordinamento nella sezione  **Impostazioni di ordinamento dei client**, la visualizzazione di questo parametro viene attivata automaticamente nella sezione  **Impostazioni della vista albero**, se era disattivata.
- Se nella sezione  **Impostazioni della vista albero** viene disattivata la visualizzazione del parametro di ordinamento selezionato nella sezione  **Impostazioni di ordinamento dei client**, l'ordinamento per questo parametro cambia automaticamente nell'ordinamento per nome del client. Se in questo caso la visualizzazione dei nomi dei client è disattivata, l'ordinamento cambia in quello per identificatore del client (non possono essere disattivati contemporaneamente il nome e l'identificatore).

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.
2. Nella parte destra della finestra del Pannello di controllo si apre una barra con le proprietà del gruppo o della postazione selezionata. Queste impostazioni sono descritte in modo dettagliato in p. [Modifica dei gruppi](#) e [Proprietà della postazione](#).




Alla selezione nella lista gerarchica della voce **Rete antivirus** nella barra delle proprietà verranno visualizzate informazioni di riepilogo sui gruppi e sulle postazioni della rete antivirus, nonché sul numero di licenze disponibili.

5.3.3. Preferiti



Il Pannello di controllo per un'amministrazione comoda consente di salvare segnalibri a pagine dell'interfaccia nella lista dei preferiti. Per esempio per un passaggio veloce alle pagine del Pannello di controllo il più spesso visitate.





Gestione della lista dei preferiti

1. Nel menu principale del Pannello di controllo selezionare la voce **Preferiti**.
2. Si aprirà la lista delle pagine del Pannello di controllo aggiunte ai segnalibri.
3. Premere **Modifica**.
4. Utilizzando la lista dei preferiti, è possibile:
 - Aprire una pagina inclusa nella lista dei preferiti. Per farlo, premere il segnalibro corrispondente a questa pagina nella lista dei preferiti.
 - Modificare l'ordinamento dei segnalibri. Per farlo, premere l'icona  a sinistra del segnalibro e spostare il segnalibro in alto o in basso.
 - Rimuovere tutti i segnalibri dalla lista preferiti. Per farlo, selezionare il segnalibro che si vuole rimuovere o tutti i segnalibri. Premere **Rimuovi**, quindi **Salva**.

Aggiunzione di un segnalibro ai preferiti

1. Passare alla pagina del Pannello di controllo che si vuole aggiungere ai preferiti.
2. Accanto al nome della pagina sopra il menu di gestione premere l'icona .
3. Si aprirà la finestra **Aggiunzione del segnalibro**. Nel campo **Nome** il nome della pagina viene aggiunto automaticamente nel formato *<Voce del menu principale> > <Voce del menu di gestione>*. Se necessario, si può modificare il nome del segnalibro.
4. Sono disponibili le seguenti azioni:
 - Per salvare la pagina nella lista dei preferiti, premere **Aggiungi**. L'icona accanto al nome della pagina cambierà a .
 - Per chiudere la finestra senza modificare la lista dei preferiti, premere **Annulla**.

Modifica e cancellazione del segnalibro dai preferiti

1. Passare alla pagina del Pannello di controllo che si vuole modificare o cancellare dai preferiti.
2. Accanto al nome della pagina sopra il menu di gestione premere l'icona .
3. Si aprirà la finestra **Modifica del segnalibro**. Sono disponibili le seguenti azioni:
 - Per modificare il segnalibro, modificare il suo nome nel campo **Nome**. Premere **Aggiorna** per accettare le modifiche.
 - Per cancellare la pagina dalla lista dei preferiti, premere **Rimuovi**. L'icona accanto al nome della pagina cambierà a .



5.3.4. Barra di ricerca

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



Per una ricerca avanzata in base a parametri, utilizzare l'elemento [Impostazioni di filtraggio](#) nella barra degli strumenti della voce **Rete antivirus**.

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 della postazione** — per cercare postazioni per identificatore univoco.
 - **ID del gruppo** — per cercare gruppi per identificatore univoco.
 - **Nome utente** — per cercare postazioni per nome utente sulla postazione.
 - **Indirizzo IP** — per cercare postazioni per indirizzo IP.
 - **Indirizzo MAC** — per cercare postazioni per indirizzo MAC.
 - **Hardware** — per cercare postazioni per nome dell'hardware installato sulla postazione o del suo produttore.
 - **Programma** — per cercare postazioni per nome del software installato sulla postazione.
 - **Descrizione** — per cercare postazioni e gruppi per descrizione.




Per iniziare una ricerca delle postazioni per parametro, premere il pulsante **Ricerca**.
2. Inserire la stringa in base alla quale verrà effettuata la ricerca. Può essere impostata:
 - una stringa specifica per la completa corrispondenza con il parametro di ricerca,
 - una maschera della stringa di ricerca: è consentito il carattere *.
3. Premere il tasto INVIO per iniziare la ricerca. Si aprirà l'albero della rete antivirus.
4. Nell'albero della rete antivirus saranno visualizzati tutti gli elementi trovati secondo i parametri di ricerca, in particolare:
 - 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 oggetto trovato**.

5.3.5. Eventi

Per avvisare l'amministratore di eventi che richiedono attenzione, si usa la sezione visualizzata nel menu principale tramite l'icona  **Eventi**.



L'icona può essere nei seguenti stati:

-  — non ci sono avvisi di eventi della rete.
-  — ci sono nuovi avvisi di eventi secondari.
-  — ci sono nuovi avvisi di eventi importanti che richiedono l'intervento dell'amministratore.

Per la lista degli eventi sono possibili le seguenti azioni:



1. Con un clic sull'icona si apre una lista a discesa degli eventi della rete antivirus. L'icona cambia automaticamente in .
2. Quando si fa clic sulla riga dell'avviso di un evento, si passa alla sezione del Pannello di controllo responsabile delle funzionalità corrispondenti.
3. La costola di ogni avviso nella lista degli avvisi è contrassegnata da un colore che corrisponde all'importanza dell'evento (nello stesso modo dell'icona). Quando si passa alla sezione responsabile delle funzionalità dell'avviso, l'avviso viene considerato come letto e la costola cambia colore al grigio.

Tabella 5-2. Lista dei possibili avvisi di eventi della rete antivirus

Evento	Importanza	Sezione del Pannello di controllo	Descrizione
Avvisi di nuovi arrivi	secondario	Rete antivirus Si apre il gruppo Newbies nell'albero della rete antivirus	Al Server Dr.Web si sono connesse nuove postazioni e sono in attesa della conferma di accesso da parte dell'amministratore. È possibile nel caso in cui nella configurazione del Server Dr.Web è impostato il valore Conferma l'accesso manualmente per l'impostazione Modalità di registrazione dei nuovi arrivi .
Notizie non lette	secondario	 Supporto → Notizie	Sono disponibili notizie della società Doctor Web non lette.
Nuovi avvisi	secondario	Amministrazione → Avvisi della web console	Sono disponibili nuovi avvisi dell'amministratore ricevuti tramite Web console .
Avvisi critici	importante		
Sono disponibili aggiornamenti del Server	importante	Amministrazione → Server Dr.Web	L'aggiornamento del Server Dr.Web è stato caricato nel repository ed è disponibile per l'installazione.
La configurazione del Server è stata modificata. È necessario riavviare il Server.	importante	Amministrazione → Configurazione del Server Dr.Web	Le impostazioni del file di configurazione del Server Dr.Web sono state modificate dopo l'avvio del Server Dr.Web. È necessario riavviare il Server Dr.Web per accettare le nuove impostazioni.



Evento	Importanza	Sezione del Pannello di controllo	Descrizione
La configurazione del web server è stata modificata. È necessario riavviare il Server.	importante	Amministrazione → Configurazione del web server	Le impostazioni del file di configurazione del web server sono state modificate dopo l'avvio del Server Dr.Web. È necessario riavviare il Server Dr.Web per accettare le nuove impostazioni.

5.3.6. Impostazioni

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



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 della rete antivirus corrente (v. anche p. [Amministratori e gruppi di amministratori](#)).

Generali




I valori dei campi contrassegnati con il carattere * sono da impostare.

Se necessario, modificare i seguenti parametri:

- **Nome utente*** dell'amministratore — login per l'accesso al Pannello di controllo.
- Nome e cognome dell'amministratore.
- **Indirizzo email** associato all'account.
- **Lingua dell'interfaccia** utilizzata da questo amministratore.



I testi dell'interfaccia per la lingua selezionata verranno aggiornati automaticamente dopo il salvataggio delle impostazioni dell'amministratore. In particolare, verranno automaticamente impostati i flag nelle sezioni **Amministrazione** → **Configurazione generale del repository** → **Server Dr.Web** → **Lingue del Pannello di controllo della sicurezza Dr.Web** e **Amministrazione** → **Configurazione generale del repository** → **Server Dr.Web** → **Documentazione**.

- **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
- **Fuso orario** — la data e l'ora degli eventi nell'interfaccia verranno visualizzati in base al fuso orario selezionato.
- **Descrizione** dell'account.
- Per cambiare la password, premere il pulsante  **Cambia password** nella barra degli strumenti.

I seguenti parametri sono di sola lettura:

- **Identificatore** dell'account amministratore.
- **Tipo di autenticazione** per questo account (v. [Autenticazione degli amministratori](#)):
 - **Interna** — sulla base delle credenziali memorizzate nel database di Server Dr.Web.
 - **Esterna** — tramite sistemi esterni.
- Date di creazione account e di ultima modifica parametri.
- **Ultimo indirizzo** — visualizza l'indirizzo di rete dell'ultima connessione sotto questo account.


Permessi

I permessi amministratore e la modifica degli stessi sono descritti nella sezione [Modifica degli account amministratori e dei gruppi](#).

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 simili alle impostazioni locate nella barra degli strumenti della voce  **Impostazioni della vista albero** nella sezione del menu principale **Rete antivirus**:




- per i gruppi:



- **Appartenenza a tutti i gruppi** — per duplicare la visualizzazione della postazione nella lista se fa parte di più gruppi allo stesso tempo (solo per i gruppi con l'icona di cartella bianca — vedi [tabella 5-1](#)). Se il flag è selezionato, la postazione è visualizzata in tutti i gruppi di cui fa parte. Se il flag è deselezionato, la postazione è visualizzata una volta nella lista.
- **Mostra gruppi nascosti** — per 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.
- **Mostra solo i gruppi con postazioni attivate** — per visualizzare solo i gruppi con postazioni che si sono connesse al Server Dr.Web almeno una volta.
- per i client del Server Dr.Web (postazioni, Server proxy Dr.Web e Server Dr.Web adiacenti):
 - **Mostra identificatori dei client** — per visualizzare gli identificatori univoci dei client del Server Dr.Web.
 - **Mostra nomi dei client** — per visualizzare i nomi dei client del Server Dr.Web.




Non è possibile disattivare contemporaneamente la visualizzazione degli identificatori e dei nomi dei client. Uno dei parametri **Mostra identificatori dei client** e **Mostra nomi dei client** sarà sempre selezionato.

- **Mostra indirizzi dei client** — per visualizzare gli indirizzi IP dei client del Server Dr.Web.
- **Mostra server delle postazioni** — per visualizzare i nomi o gli indirizzi IP dei Server Dr.Web a cui sono connesse le postazioni. Riguarda le postazioni incluse in un cluster dei Server Dr.Web.
- **Mostra gravità dello stato delle postazioni** — per visualizzare la gravità dello status per le postazioni attive. Verrà aggiunta una gradazione di colore per le postazioni a seconda del loro status (vedi [tabella 5-1](#)). Se l'opzione è disattivata, per una postazione con gli status cui corrispondono le icone  e  verrà visualizzata un'icona comune .
- **Mostra icona del criterio** — per visualizzare l'icona del criterio accanto all'icona della postazione a cui è assegnato il criterio.
- **Mostra postazioni bloccate** — per visualizzare le postazioni il cui accesso al Server Dr.Web è bloccato.
- per tutti gli elementi:
 - **Mostra icona delle impostazioni individuali** — per visualizzare un indicatore che denota la presenza di impostazioni individuali sulle icone dei gruppi e dei client del Server Dr.Web: postazioni, Server proxy Dr.Web e Server Dr.Web adiacenti.
 - **Mostra descrizioni** — per visualizzare le descrizioni dei gruppi e dei client del Server Dr.Web: postazioni, Server proxy Dr.Web e Server Dr.Web adiacenti (le descrizioni vengono impostate nelle proprietà dell'elemento).
 - **Mostra numero di client** — per visualizzare il numero di client del Server Dr.Web: postazioni, Server proxy Dr.Web e Server Dr.Web adiacenti per tutti i gruppi della rete antivirus in cui questi client sono inclusi.



- **Mostra icona delle regole di appartenenza** — per visualizzare un indicatore sulle icone delle postazioni che sono state aggiunte a un gruppo in modo automatico secondo le regole di appartenenza, nonché sulle icone dei gruppi a cui le postazioni sono state aggiunte in modo automatico.

Impostazioni di ordinamento dei client

Le impostazioni di questa sottosezione consentono di modificare il parametro in base a cui viene effettuato l'ordinamento e l'ordine dell'ordinamento dei client del Server Dr.Web: postazioni, Server proxy Dr.Web e Server Dr.Web adiacenti nell'albero della rete antivirus, e sono analoghe alle impostazioni situate nella barra degli strumenti della voce  **Impostazioni di ordinamento dei client** nella sezione del menu principale **Rete antivirus**:

- Per selezionare il parametro in base a cui verranno ordinate le postazioni, impostare uno dei seguenti flag (è possibile selezionare solo un parametro):
 - **Identificatore** — per ordinare per identificatore del client univoco.
 - **Nome** — per ordinare per nome del client.
 - **Indirizzo** — per ordinare per indirizzo di rete del client. I client che non hanno un indirizzo di rete verranno visualizzati in ordine casuale senza essere ordinati.
 - **Data di creazione** — per ordinare per data di creazione dell'account di client sul Server Dr.Web.
 - **Data dell'ultima connessione** — per ordinare per data dell'ultima connessione al Server Dr.Web.
- Per selezionare la direzione di ordinamento, impostare uno dei seguenti flag:
 - **Ordina crescente.**
 - **Ordina decrescente.**

Intervallo di tempo

In questa sottosezione viene configurato l'intervallo di tempo entro cui vengono visualizzati i 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 che era selezionato 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

Dalla lista a cascata **Periodo di inattività ammissibile** selezionare un periodo di tempo dopo cui una 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** è possibile selezionare il tipo di carattere da utilizzare nell'esportazione dei report in formato PDF.
- Nel campo **Dimensione carattere dei report** è possibile 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 una visualizzazione delle statistiche divisa in pagine.
- Nel campo **Numero di caratteri dopo il troncamento di righe lunghe** viene impostato il numero massimo di caratteri visibili dopo il troncamento di righe lunghe nelle tabelle dei log e degli avvisi.
- Spuntare il flag **Mostra grafici** per visualizzare dati grafici sulle pagine dei report statistici. Se il flag è tolto, la visualizzazione dei dati grafici è disattivata.

Abbonamento

In questa sottosezione si configura l'abbonamento alle notizie dell'azienda Doctor Web. Spuntare i flag per ricevere le notizie delle seguenti categorie:


- **Sugli aggiornamenti** — notizie sugli aggiornamenti dei prodotti Dr.Web.
- **Sulle promozioni** — notizie sulle promozioni dell'azienda Doctor Web.
- **Sui virus** — panoramiche mensili sull'attività di virus e notizie sulle minacce e sugli attacchi più importanti.
- **Sui prodotti Dr.Web** — notizie sui prodotti Dr.Web.







- **Su Dr.Web AV-Desk** — notizie sul servizio web Dr.Web AV-Desk.
- **Notizie aziendali** — notizie sugli eventi dell'azienda Doctor Web.

Spuntare il flag **Abbonamento automatico a nuove sezioni** per attivare l'aggiunzione automatica di nuove sezioni sulla pagina **Notizie** nel Pannello di controllo.


5.3.7. Aiuto

Per ottenere aiuto nel corso dell'utilizzo di Dr.Web Enterprise Security Suite, nel menu principale premere il pulsante  **Aiuto**. Si aprirà un menu contestuale contenente le seguenti voci:

-  **Documentazione** — per aprire la sezione della documentazione amministratore che corrisponde alla sezione del Pannello di controllo in cui ci si trova al momento. Se per la sezione corrente del Pannello di controllo non esiste la sezione corrispondente nella documentazione, la voce  **Documentazione** non verrà visualizzata nel menu contestuale dell'icona .
-  **Supporto** — per aprire la sezione **Supporto** del Pannello di controllo (vedi sotto).

Supporto

La sezione **Supporto** contiene i seguenti elementi:

1. Link delle risorse ausiliarie.
 - **Forum** — per passare al forum dell'azienda Doctor Web.
 - **Notizie** — per passare alla pagina delle notizie dell'azienda Doctor Web.
 - **Contatta il servizio di supporto tecnico** — per passare alla pagina del supporto tecnico Doctor Web.
 - **Spedisci un file sospetto** — per aprire il modulo di invio di un virus al laboratorio Doctor Web.
 - **Wikipedia Doctor Web** — per passare alla pagina della knowledge base dedicata ai prodotti dell'azienda Doctor Web.
 - **Segnala un falso positivo di Office control** — per aprire un modulo attraverso cui è possibile inviare un messaggio di un falso positivo o di un mancato riconoscimento di link malevoli da parte del componente Office control.
2. Sezione **Documentazione**. Ciascun documento è disponibile in formato HTML, nonché PDF — a condizione che per la lingua selezionata dell'interfaccia del Pannello di controllo sia spuntato il flag corrispondente, nonché sia data l'istruzione di aggiornare la documentazione in formato PDF nella sezione **Configurazione generale del repository** → **Server Dr.Web** → [Documentazione](#). Per aprire un documento in formato HTML, cliccare sul nome del manuale richiesto. Lo stesso documento può essere aperto in formato PDF tramite il pulsante  nella colonna **Scarica**. Per comodità, la documentazione è suddivisa in diverse sottosezioni:



- **Installazione e utilizzo di Dr.Web Enterprise Security Suite (documentazione dell'amministratore)**

I manuali in questa sottosezione forniscono una visione particolareggiata di come funziona il servizio Dr.Web Enterprise Security Suite. Dai materiali raggruppati qui è possibile scoprire l'ordine di dispiegamento e configurazione della protezione antivirus completa e le caratteristiche dell'interazione dei suoi componenti con programmi di terzi, nonché conoscere le ultime modifiche alla versione installata di Dr.Web Enterprise Security Suite.

- **Gestione delle postazioni protette da Dr.Web Enterprise Security Suite (documentazione dell'amministratore)**

Questi manuali contengono informazioni sulla configurazione e la gestione centralizzata di diversi prodotti dell'azienda Doctor Web, quando sono inclusi nella rete antivirus Dr.Web Enterprise Security Suite.

- **Documentazione dell'utente**

Questi materiali forniscono informazioni dettagliate sull'installazione e la configurazione di diversi prodotti dell'azienda Doctor Web, nonché le raccomandazioni per l'uso e la risoluzione dei problemi tipici riscontrati dagli utenti.



Al download della documentazione attraverso il Pannello di controllo mobile Dr.Web su un dispositivo con il sistema operativo Android il documento viene salvato automaticamente nella cartella Download.

Se Server Dr.Web funziona attraverso il protocollo HTTPS con un certificato autofirmato, prima di scaricare la documentazione su un dispositivo con il sistema operativo Android, assicurarsi che questo certificato di Server Dr.Web sia installato sul dispositivo.

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

5.4.1. Scanner di rete

Funzioni di Scanner di rete

- Scansione della rete per rilevare postazioni.
- Determina la presenza di 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](#).

Principio di funzionamento di Scanner di rete

Scanner di rete supporta le seguenti modalità di ricerca:



1. Ricerca in Active Directory.
2. Ricerca attraverso NetBIOS.
3. Ricerca attraverso ICMP.
4. Ricerca attraverso TCP.
5. Modalità aggiuntiva: rilevamento della presenza di Agent Dr.Web.

Principio di azioni, se tutte le modalità sono attivate:

1. Le prime tre modalità vengono avviate in parallelo. Le postazioni già interrogate non vengono interrogate per la seconda volta.
2. Dopo la fine della ricerca attraverso ICMP si attiva la ricerca attraverso TCP per gli indirizzi che non hanno risposto. Se la ricerca attraverso ICMP è disattivata, si attiva subito la ricerca attraverso TCP in parallelo con le prime due modalità.



La ricerca attraverso ICMP si basa sull'invio delle richieste ping, che possono essere bloccate a causa di criteri di rete (in particolare dalle impostazioni di un firewall).

Per esempio:

Se in SO Windows (Vista e versioni successive) nelle impostazioni di rete è stata impostata **Rete pubblica**, il sistema operativo bloccherà tutte le richieste ping.

3. Per le postazioni rilevate a seguito della ricerca tramite le prime quattro modalità viene avviata un'interrogazione per rilevare gli Agent Dr.Web.



Scanner di rete può rilevare su una postazione solo la presenza di Agent Dr.Web 4.44 e versioni successive, ma non può interagire con Agent Dr.Web delle versioni precedenti.

Agent Dr.Web installato su una postazione protetta processa le relative richieste di Scanner di rete che arrivano su una determinata porta. Di default, viene utilizzata la porta `udp/2193`. Pertanto, anche in Scanner di rete di default viene offerto di interrogare questa porta. Scanner di rete conclude che Agent Dr.Web è disponibile o non disponibile su una postazione basandosi sulla possibilità di scambiarsi informazioni (richiesta-risposta) sulla porta sopraccitata.



Se su una postazione la ricezione di pacchetti su `udp/2193` è proibita (per esempio, tramite firewall), Agent Dr.Web non può essere rilevato, e pertanto, Scanner di rete ritiene che Agent Dr.Web non sia installato sulla postazione.



Avvio dello Scanner di rete

Per eseguire una scansione della rete

1. Aprire la finestra di Scanner di rete. Per farlo, selezionare la voce **Amministrazione** nel menu principale del Pannello di controllo, nella finestra che si è aperta selezionare la voce del menu di gestione **Scanner di rete**. Si aprirà la finestra di Scanner di rete.
2. Spuntare il flag **Attiva la ricerca attraverso ICMP** per cercare postazioni attraverso il protocollo ICMP nei limiti degli indirizzi IP impostati.
3. Spuntare il flag **Attiva la ricerca attraverso TCP** per cercare postazioni attraverso il protocollo TCP nei limiti degli indirizzi IP impostati.

Configurare le impostazioni per questa modalità:

- **Scansione rapida.** In modalità di scansione della rete rapida vengono interrogate soltanto le porte principali sulle postazioni: 445, 139, 22, 80.
- **Scansione avanzata.** In modalità di scansione della rete avanzata viene verificata una pluralità di porte più comunemente utilizzate. Le porte vengono scansionate in un ordine rigorosamente specificato: 445, 139, 135, 1025, 1027, 3389, 22, 80, 443, 25, 21, 7, 19, 53, 110, 115, 123, 220, 464, 465, 515, 873, 990, 993, 995, 1194, 1433, 1434, 2049, 3306, 3690, 4899, 5222, 5269, 5432, 6000, 6001, 6002, 6003, 6004, 6005, 6006, 6007, 6446, 9101, 9102, 9103, 10050, 10051, 8080, 8081, 98, 2193, 8090, 8091, 24554, 60177, 60179.

- **Indirizzi IPv4** — lista degli indirizzi IPv4:

- singoli indirizzi: 10.4.0.10
- un intervallo con trattino: 172.16.0.1-172.16.0.123
- un intervallo con prefisso di rete: 192.168.0.0/24

Se vengono indicati diversi indirizzi, utilizzare ";" o "," come separatore.

- **Indirizzi IPv6** — lista degli indirizzi IPv6:

- singoli indirizzi: fe80::9109:1808:8e44:735b%3
- un intervallo con trattino: [FC00::0001]-[FC00::ffff]
- un intervallo con prefisso di rete: [::ffff:10.0.0.1]/7

Se vengono indicati diversi indirizzi, utilizzare ";" o "," come separatore.

4. Spuntare il flag **Attiva la ricerca attraverso NetBIOS** per cercare postazioni attraverso il protocollo NetBIOS.

Configurare le impostazioni per questa modalità:

- **Domini** — lista dei domini in cui verranno cercate le postazioni. Utilizzare una virgola come separatore per diversi domini.
- Spuntare il flag **Scansione avanzata** per eseguire una scansione avanzata con l'utilizzo delle informazioni dai browser di rete.

5. Spuntare il flag **Attiva la ricerca in Active Directory** per cercare le postazioni nel dominio Active Directory.



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

Le ricerche di postazioni nel dominio Active Directory viene eseguita solo tramite il protocollo sicuro `ldaps`.

Configurare le impostazioni per questa modalità:

- **Controller di Active Directory** — controller di Active Directory, ad esempio, `dc.example.com`.
- **Nome utente** — nome utente dell'utente di Active Directory.
- **Password** — password dell'utente di Active Directory.




Per Server Dr.Web SO Windows le impostazioni di ricerca in Active Directory sono opzionali. Come dati di registrazione di default vengono utilizzati i dati dell'account utente sotto cui il processo Server Dr.Web è stato avviato (di regola è LocalSystem).

Per Server Dr.Web SO della famiglia UNIX le impostazioni devono essere obbligatoriamente configurate.





- Dalla lista a cascata **Protezione della connessione** selezionare il tipo di scambio di dati crittografati:
 - **STARTTLS** — il passaggio alla connessione protetta viene effettuato attraverso il comando `STARTTLS`. Di default per la connessione è previsto l'utilizzo della porta 25.
 - **SSL/TLS** — aprì una connessione protetta crittografata separata. Di default per la connessione è previsto l'utilizzo della porta 465.
 - **No** — non usare la crittografia. Lo scambio di dati avverrà su una connessione non protetta.
- 6. Nella sezione **Parametri generali** configurare le impostazioni utilizzate da tutte le modalità di ricerca:
 - **Time-out (s)** — tempo massimo in secondi di attesa della risposta da una postazione.
 - **Numero di richieste a una postazione** — numero massimo di richieste a una postazione in attesa della risposta.
 - **Numero di richieste simultanee** — numero massimo di postazioni su cui le richieste vengono inviate allo stesso tempo.
 - Spuntare il flag **Mostra nomi delle postazioni** affinché vengano visualizzati sia l'indirizzo IP che il nome a dominio delle postazioni trovate. Se una postazione non è registrata sul server DNS, viene visualizzato solo il suo indirizzo IP.
 - Spuntare il flag **Determina la presenza di Agent** affinché venga determinata la presenza di Agent Dr.Web installato sulla postazione. Se l'opzione è disattivata, per tutte le postazioni trovate verrà visualizzato uno stato che lo stato del software antivirus sulla postazione è sconosciuto.




Se l'opzione **Determina la presenza di Agent** è disattivata, per tutte le postazioni trovate verrà visualizzato lo stato , cioè lo stato del software antivirus sulla postazione è sconosciuto.

- **Porta** — numero di porta del protocollo UDP su cui Scanner di rete deve connettersi ad Agent Dr.Web durante la ricerca. L'intervallo dei valori è 1-65535. Di default viene utilizzata la porta 2193.
7. Fare clic sul pulsante **Scansiona**. A questo punto inizia la scansione della rete.
 8. Durante la scansione della rete nella finestra viene caricata una lista dei computer con l'indicazione della presenza di Agent Dr.Web.

Espandere gli elementi della directory corrispondenti ai gruppi di lavoro (domini). Tutti gli elementi della directory, corrispondenti ai gruppi di lavoro e a singole postazioni, sono contrassegnati da varie icone, il cui significato è riportato di seguito:

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

È inoltre possibile espandere gli elementi della directory corrispondenti alle postazioni con le icone  per visualizzare la lista dei componenti installati.

5.5. Schema interazione dei componenti della rete antivirus

In [immagine 5-2](#) è rappresentato lo schema generale di un frammento di rete antivirus.

Questo schema visualizza una rete antivirus che include solo un Server Dr.Web. In grandi aziende è preferibile installare una rete antivirus con diversi Server Dr.Web per la distribuzione del carico tra di essi.

In questo esempio la rete antivirus è 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 che essi abbiano l'accesso a Internet.

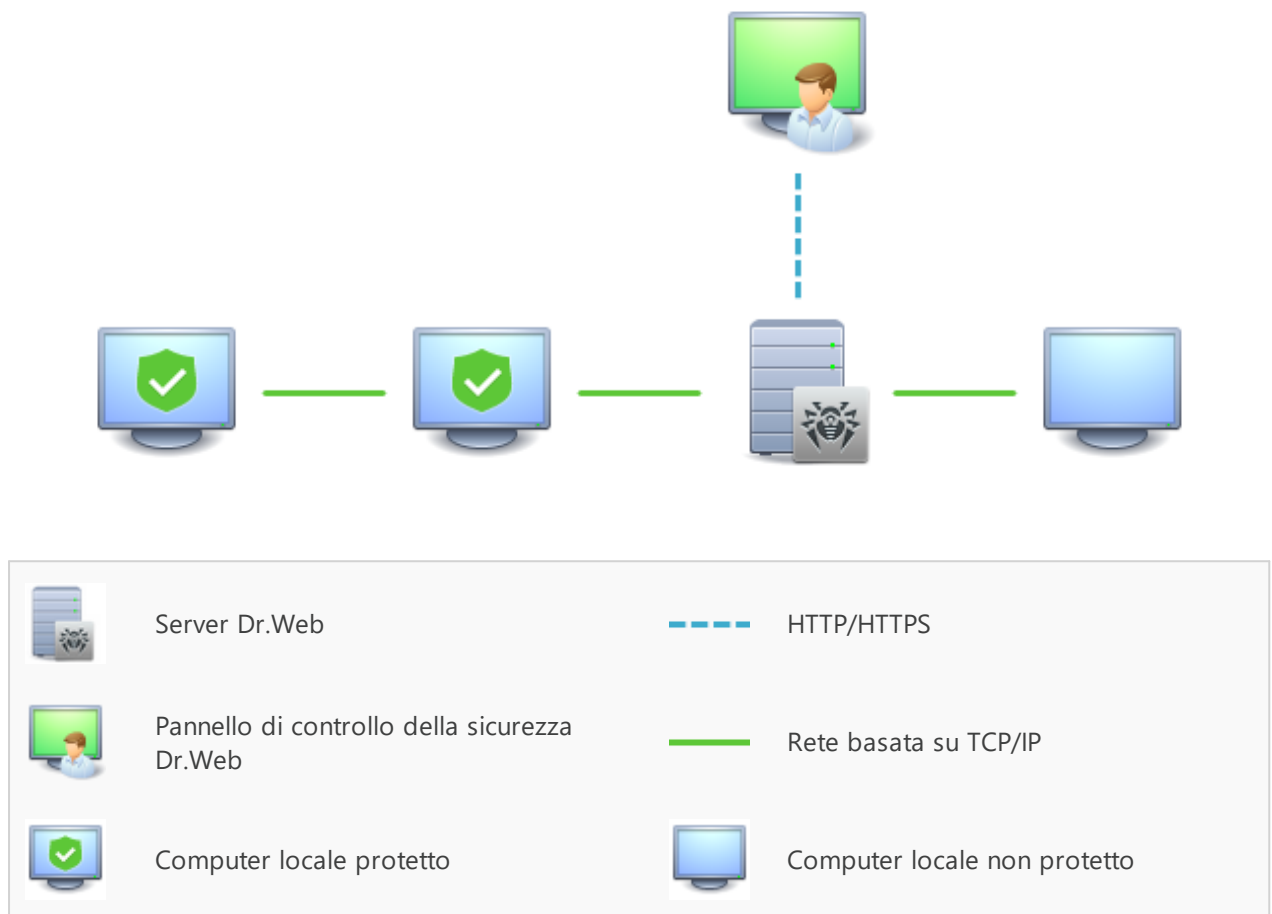


Immagine 5-2. Struttura della rete antivirus

Ad avvio del 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 Dr.Web.
3. Viene caricata la directory di aggiornamento, viene inizializzato il sistema di informazione di segnalazione (sistema di avviso).
4. Viene controllata l'integrità del database del Server Dr.Web.
5. Vengono eseguiti i task dello Scheduler del Server Dr.Web.
6. Attesa delle informazioni dagli Agent Dr.Web e dei comandi dai Pannelli di controllo.

L'intero flusso di comandi, dati e informazioni statistiche passa necessariamente attraverso Server Dr.Web. Anche il Pannello di controllo si scambia informazioni solamente con il Server Dr.Web; le modifiche alla configurazione di una postazione e la trasmissione di comandi ad Agent Dr.Web vengono effettuati dal Server Dr.Web sulla base dei comandi del Pannello di controllo.

Così, il frammento della rete antivirus ha una struttura logica illustrata in [immagine 5-3](#).

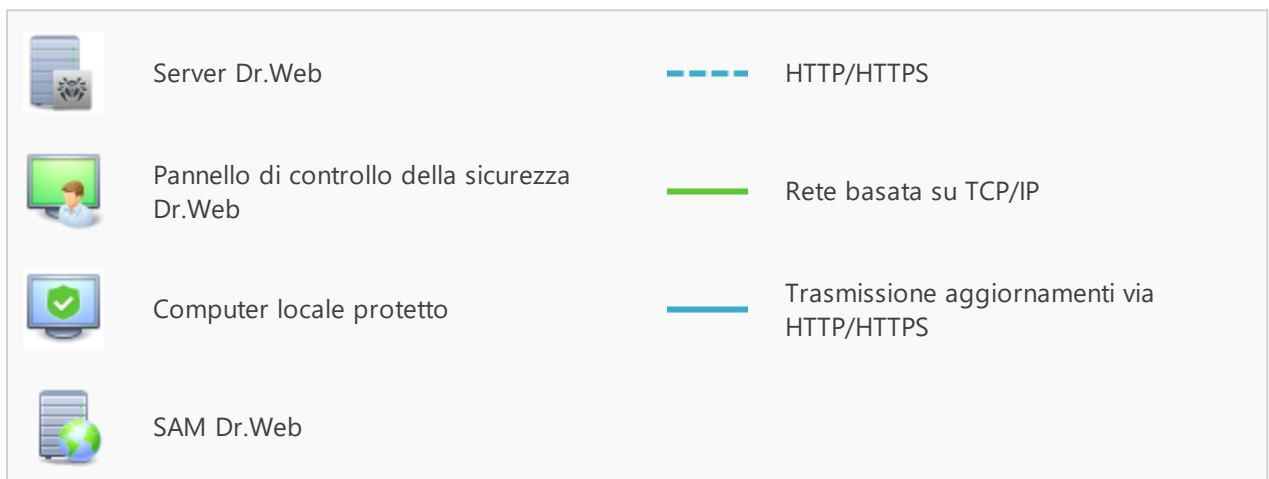
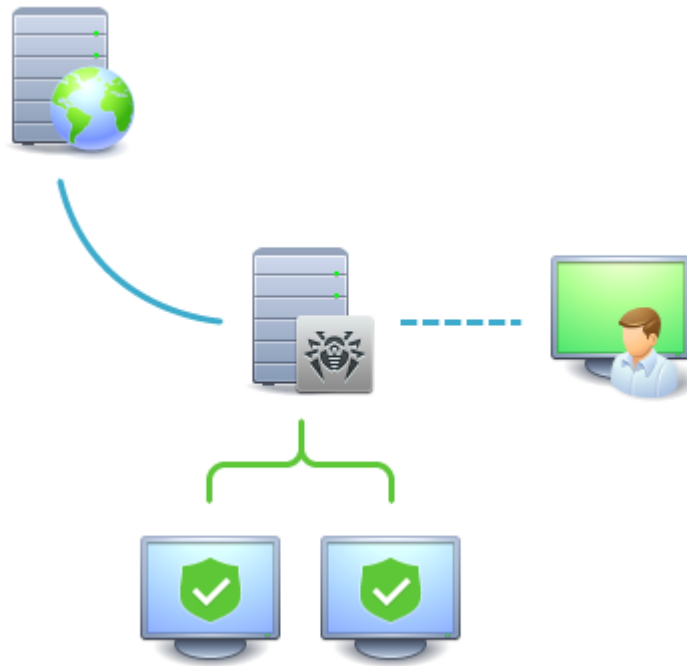


Immagine 5-3. Struttura logica della rete antivirus

Tra il Server Dr.Web e le postazioni (linea sottile continua in [immagine 5-3](#)) vengono trasmesse:

- le richieste dell'Agent Dr.Web per l'ottenimento del calendario centralizzato e il calendario centralizzato di questa postazione,
- le impostazioni dell'Agent Dr.Web e del pacchetto antivirus,
- le richieste per i task successivi da eseguire (scansione, aggiornamento dei database dei virus ecc.),
- i file dei pacchetti antivirus — quando l'Agent ha ricevuto il relativo task di installazione,
- gli aggiornamenti del software e dei database dei virus — per l'esecuzione di un task di aggiornamento,
- i messaggi dell'Agent Dr.Web sulla configurazione della postazione,



- le statistiche di funzionamento dell'Agent Dr.Web e dei pacchetti antivirus da includere nel log centralizzato,
- gli avvisi sugli eventi di virus e su altri eventi da registrare.

A seconda delle impostazioni e del numero di postazioni, il volume di traffico tra le postazioni e il Server Dr.Web può essere abbastanza grande. Pertanto, la rete antivirus Dr.Web Enterprise Security Suite prevede la possibilità di compressione di traffico. Per la descrizione dell'utilizzo di questa modalità opzionale v. p. [Cifratura e compressione del traffico dati](#).

Il traffico tra il Server Dr.Web e la postazione può essere cifrato. Questo consente di evitare la divulgazione delle informazioni trasmesse via il canale descritto, nonché la sostituzione furtiva del software che viene caricato sulle postazioni. Di default, questa possibilità è attivata. Per la descrizione dell'utilizzo di questa modalità v. p. [Cifratura e compressione del traffico dati](#).

Dal web server di aggiornamento al Server Dr.Web (linea spessa continua in [immagine 5-3](#)) attraverso il protocollo HTTP vengono trasmessi i file necessari per la replica delle directory centralizzate di installazione e di aggiornamento, nonché informazioni di servizio sull'avanzamento di tale processo. L'integrità delle informazioni trasmesse (dei file del software Dr.Web Enterprise Security Suite e dei pacchetti antivirus) viene assicurata dall'utilizzo del metodo checksum: un file danneggiato o sostituito furtivamente durante la trasmissione non verrà accettato dal Server Dr.Web.

Tra il Server Dr.Web e il Pannello di controllo (linea tratteggiata in [immagine 5-3](#)) vengono trasmesse le informazioni sulla configurazione del Server Dr.Web (comprese le informazioni sulla topologia di rete) e le impostazioni delle postazioni. Queste informazioni vengono visualizzate nel Pannello di controllo, e se qualche impostazione viene modificata dall'utente (amministratore della rete antivirus), le informazioni sulle modifiche apportate vengono trasmesse sul Server Dr.Web.

La connessione del Pannello di controllo al Server Dr.Web selezionato viene stabilita solo dopo che l'amministratore di rete antivirus si è autenticato inserendo il nome utente e la password su tale Server Dr.Web.



Capitolo 6: 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 solo nella rete locale e richiedono i privilegi di amministratore in questa rete, e il debug di Server Dr.Web richiede l'accesso completo alla relativa directory di installazione.

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

6.1. Autenticazione degli amministratori

L'autenticazione di un amministratore per la connessione al Server Dr.Web è possibile nei seguenti modi:

- Con la conservazione dei dati sugli amministratori nel database del Server Dr.Web.
- Utilizzando le impostazioni LDAP/AD che consentono la connessione ai server LDAP ed Active Directory.
- Utilizzando il protocollo RADIUS.
- Utilizzando PAM (solo nei sistemi operativi della famiglia UNIX).

Quando il Server Dr.Web viene aggiornato da una versione precedente, possono inoltre essere disponibili i seguenti tipi di autenticazione (se erano attivati nella versione precedente):



Dopo la disattivazione di questi tipi di autenticazione, le relative sezioni saranno escluse dalle impostazioni del Pannello di controllo.

Quando il Server Dr.Web viene installato per la prima volta, queste sezioni non sono disponibili.



- Tramite Active Directory (nelle versioni del Server Dr.Web per SO Windows).
- Utilizzando il protocollo LDAP.

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

1. Per primo viene sempre eseguito il tentativo di autenticazione amministratore dal database del Server Dr.Web.
2. L'ordine di utilizzo dei metodi di autenticazione attraverso i sistemi esterni dipende dall'ordine in cui essi sono elencati nelle impostazioni definite nel Pannello di controllo.
3. Di default, i metodi di autenticazione attraverso i sistemi esterni sono disattivati.

Per modificare l'ordine di utilizzo dei modi di autenticazione

1. Selezionare la voce **Amministrazione** nel 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 l'ordine di sequenza, trascinare 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 Dr.Web.



Il nome utente amministratore deve essere univoco.

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

Ogni volta che si salvano modifiche della sezione **Autenticazione**, viene automaticamente salvato un backup della versione precedente del file di configurazione con i parametri di autenticazione degli amministratori. Vengono conservati gli ultimi 10 backup.

I backup si trovano nella stessa directory del file di configurazione e vengono denominati nel seguente formato:

`<nome_di_file>_<ora_di_creazione>`

dove `<nome_di_file>` dipende dal sistema di autenticazione: `auth-ads.conf`, `auth-ldap.conf`, `auth-radius.conf`, `auth-pam.conf`.

È possibile utilizzare i backup creati, in particolare, per ripristinare il file di configurazione se l'interfaccia del Pannello di controllo non è disponibile.

6.1.1. Autenticazione degli amministratori dal database del Server Dr.Web

Il metodo di autenticazione con la conservazione dei dati sugli amministratori nel database del Server Dr.Web viene utilizzato di default.



Per aprire la sezione di gestione degli account 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 Dr.Web.

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

6.1.2. Autenticazione con utilizzo di LDAP/AD

Per attivare l'autenticazione tramite LDAP/AD

1. Selezionare la voce **Amministrazione** nel 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/AD**.
4. Spuntare il flag **Utilizza l'autenticazione LDAP/AD**.
5. Premere il pulsante **Salva**.
6. Per rendere effettive le modifiche apportate, riavviare il Server Dr.Web.

La configurazione dell'autenticazione tramite il protocollo LDAP è possibile su qualsiasi server LDAP. Inoltre, con utilizzo dello stesso meccanismo, il Server Dr.Web sotto SO della famiglia UNIX può essere configurato per l'autenticazione in Active Directory sul controller di dominio.

Per comodità dell'utente è possibile cambiare nella sezione tra le impostazioni di autenticazione LDAP/AD semplificate o avanzate.



Le impostazioni di autenticazione LDAP/AD vengono salvate nel file di configurazione `auth-ldap-rfc4515.conf`.

Sono inoltre disponibili i file di configurazione con le impostazioni standard: `auth-ldap-rfc4515-check-group.conf`, `auth-ldap-rfc4515-check-group-novar.conf`, `auth-ldap-rfc4515-simple-login.conf`.

I principali attributi xml di autenticazione sono descritti nel documento **Allegati, B3**, [Autenticazione in caso di utilizzo di LDAP/AD](#).

6.1.3. Autenticazione con utilizzo di RADIUS

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

Prima di iniziare a configurare l'autenticazione tramite RADIUS, assicurarsi che il Dizionario `dictionary.drweb`, situato nella `directory etc` di Server Dr.Web, sia copiato nella



directory /usr/share/freeradius. Il dizionario conserva il set di attributi RADIUS dell'azienda Doctor Web (VSA — Vendor-Specific Attributes).

Tramite la riga di comando assegnare i permessi di accesso al file `dictionary.drweb` nella directory /usr/share/freeradius. Un esempio del comando si presenta nel seguente modo:

```
chmod 644 /usr/share/freeradius/dictionary.drweb
```

Alla fine del file /etc/raddb/dictionary aggiungere la seguente riga:

```
$INCLUDE/usr/share/freeradius/dictionary.drweb
```

All'inizio del file /etc/raddb aggiungere le seguenti righe:

```
<Nome_utente> Cleartext-Password := "<password>"  
DrWeb-ES-Adm-Flag = 1
```

Dopo aver completato questi passaggi, attivare l'autenticazione con utilizzo di RADIUS attraverso il Pannello di controllo.

Per attivare l'autenticazione tramite RADIUS

1. Selezionare la voce **Amministrazione** nel 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 il pulsante **Salva**.
6. Per rendere effettive le modifiche apportate, riavviare il Server Dr.Web.

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 (segreto).
- **Timeout** — tempo di attesa in secondi della risposta del server RADIUS.
- **Numero di tentativi** — numero di tentativi di connessione al server RADIUS.



Inoltre, per configurare i parametri aggiuntivi RADIUS, può essere utilizzato il file di configurazione `auth-radius.conf` situato nella directory `etc` di Server.

Oltre ai parametri configurati tramite il Pannello di controllo, nel file di configurazione può essere impostato il valore dell'identificatore NAS. Secondo la specifica RFC 2865, questo identificatore può essere utilizzato invece dell'indirizzo IP/del nome DNS come 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"/>
```

6.1.4. Autenticazione con utilizzo di PAM

Per attivare l'autenticazione tramite PAM

1. Selezionare la voce **Amministrazione** nel 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 il pulsante **Salva**.
6. Per rendere effettive le modifiche apportate, riavviare il Server Dr.Web.

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

Per configurare i parametri dell'autenticazione PAM, è possibile utilizzare i seguenti metodi:

- Configurare il metodo di autenticazione attraverso il Pannello di controllo: nella sezione **Amministrazione** → **Autenticazione** → **Autenticazione PAM**.
- File di configurazione `auth-pam.xml` situato nella directory `etc` del Server Dr.Web.
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 di Pannello di controllo	Elementi del file auth-pam.xml			Descrizione
	Tag	Attributo	Valori ammissibili	
Flag Utilizza autenticazione PAM	<code><enabled></code>	<code>value</code>	yes no	Il flag che determina se verrà utilizzato il metodo di autenticazione PAM.
Utilizzare <i>il drag and drop</i>	<code><order></code>	<code>value</code>	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	<code><service></code>	<code>name</code>	-	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 <code><service></code> non c'è nel file di configurazione), di default, viene utilizzato il nome <code>drwcs</code> .
Flag Il flag di controllo è obbligatorio	<code><admin-flag></code>	<code>mandatory</code>	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> .
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 è <code>DrWeb_Esuite_Admin</code> .

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.



6.1.5. Autenticazione con utilizzo di Active Directory



Prima di attivare l'autenticazione con utilizzo di Active Directory, assicurarsi che l'account per il quale si vuole attivare l'autenticazione non sia incluso nel gruppo **Utenti protetti**. In quanto Server Dr.Web è un servizio, un tentativo di autenticare un account che è incluso nel gruppo **Utenti protetti** avrà esito negativo. Informazioni dettagliate sul gruppo di sicurezza Utenti protetti sono ritrovabili sul [sito ufficiale di Microsoft](#).

Per attivare l'autenticazione tramite Active Directory

1. Selezionare la voce **Amministrazione** nel 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 il pulsante **Salva**.
6. Per rendere effettive le modifiche apportate, riavviare il Server Dr.Web.

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.



In caso di creazione automatica di un amministratore con l'autenticazione tramite Active Directory attivata, l'account amministratore viene automaticamente assegnato nel gruppo Newbies e richiede la riassegnazione manuale nel gruppo richiesto.

È possibile trasferire automaticamente l'account amministratore dal gruppo Newbies a quello stabilito a seconda dell'appartenenza ai gruppi di Active Directory tramite una procedura personalizzata, v. documento **Allegati**, [M1. Amministratori](#).

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-<versione_pacchetto>-<build>-esuite-modify-ad-schema-<versione_SO>.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 Dr.Web, non è necessario modificarlo nuovamente con utilizzo dell'utility dalla 13 versione del Server Dr.Web.

- 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** e l'attributo aggiuntivo **DrWebAdmin**.



Se l'applicazione dello schema modificato non è stata ancora completata, la classe **DrWebEnterpriseUser** può essere non trovata. In questo caso attendere per qualche tempo e ripetere il tentativo secondo il punto **c**).

- d) Con i permessi di amministratore avviare il file `drweb-<versione_pacchetto>-<build>-esuite-aduac-<versione_SO>.msi` (fa parte del pacchetto Dr.Web Enterprise Security Suite 13.0) e attendere il completamento dell'installazione.
2. L'interfaccia grafica per la modifica degli 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 del principio di funzionamento e dell'analisi degli attributi di autenticazione sono riportati nel documento **Allegati**, [B1. Autenticazione in caso di utilizzo di Active Directory](#).

Per l'ulteriore utilizzo dell'account Active Directory è necessario eseguire il login al Pannello di controllo di Server Dr.Web con le credenziali dell'utente Active Directory a cui precedentemente è stato impostato l'attributo corrispondente **Dr.Web Authentication**. Dopo questo, l'account utente comparirà nella directory **Newbies** nella sezione **Amministrazione** → **Amministratori**.

6.1.6. Autenticazione con utilizzo di LDAP



Questa sezione può essere configurata attraverso il Pannello di controllo solo quando il Server Dr.Web viene aggiornato da una versione precedente. Dopo la disattivazione di questo tipo di autenticazione, la relativa sezione sarà esclusa dalle impostazioni del Pannello di controllo.



Quando il Server Dr.Web viene installato per la prima volta, questa sezione non è disponibile.

Per attivare l'autenticazione tramite LDAP

1. Selezionare la voce **Amministrazione** nel 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 il pulsante **Salva**.
6. Per rendere effettive le modifiche apportate, riavviare il Server Dr.Web.

La configurazione dell'autenticazione tramite il protocollo LDAP è possibile su qualsiasi server LDAP. Inoltre, con utilizzo dello stesso meccanismo, il Server Dr.Web sotto SO della famiglia UNIX può essere configurato per l'autenticazione in Active Directory sul controller di dominio.



Le impostazioni di autenticazione LDAP vengono salvate nel file di configurazione `auth-ldap.conf`.

I principali attributi xml di autenticazione sono descritti nel documento **Allegati, B2. [Autenticazione in caso di utilizzo di LDAP](#)**.

A differenza di Active Directory, è possibile configurare il meccanismo per qualsiasi schema LDAP. Di default, viene eseguito il tentativo di utilizzare gli attributi di Dr.Web Enterprise Security Suite come sono definiti per Active Directory.

Il processo di autenticazione tramite LDAP è il 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.

6.2. Amministratori e gruppi di amministratori






Per aprire la sezione di gestione degli account 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 Dr.Web.



La sezione **Amministratori** è disponibile per tutti gli amministratori del Pannello di controllo. Tuttavia, l'intero albero gerarchico degli amministratori è disponibile soltanto per gli 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 l'albero gerarchico rispecchia soltanto il loro gruppo e i sottogruppi con gli account che ne fanno parte.

Nella barra degli strumenti della sezione **Amministratori** sono disponibili le seguenti opzioni:

-  [Crea account](#)
-  [Crea gruppo](#)
-  [Rimuovi gli oggetti selezionati](#)
-  [Cambia password](#)
-  [Propaga i permessi dell'amministratore](#)

6.2.1. 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 Dr.Web, 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 durante l'installazione del Server Dr.Web (v. di seguito).
- **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 Dr.Web, un account amministratore viene creato in modo automatico:

Parametro	Valore
Nome utente	admin
Password	Viene impostata all'installazione del Server Dr.Web (passaggio 9 nella procedura di installazione).
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. Un amministratore dal gruppo **Administrators** vede tutti gli amministratori a prescindere dai loro gruppi.



6.2.2. Permessi degli amministratori

Tutte le azioni degli amministratori nel Pannello di controllo vengono limitate da un set di permessi che può essere definito sia per un singolo account che per un gruppo di amministratori.

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

- **Assegnazione dei permessi**

I permessi vengono assegnati durante la creazione di un amministratore o di un gruppo di amministratori. Un account o un 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, amministratori o gruppi di amministratori ereditano permessi dal gruppo padre, ma l'ereditarietà può essere disattivata.

- Se l'ereditarietà è disattivata, un amministratore utilizza un set indipendente di permessi individuali, che viene impostato direttamente per il suo account. I permessi del gruppo padre non si applicano.
- Se un amministratore o un gruppo eredita permessi, i permessi non vengono sostituiti con quelli del gruppo padre, ma piuttosto il permesso assegnato 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 risultante di un oggetto a seconda dei permessi assegnati e dei permessi del gruppo padre è riportata in p. [Unione dei permessi](#).

- **Modifica dei permessi**

Quando vengono creati amministratori e gruppi di amministratori, non vi è la possibilità di modificarne i permessi. È possibile soltanto modificare i permessi degli oggetti già creati nella sezione delle impostazioni dell'account o del gruppo. Modificando le proprie impostazioni, si possono soltanto abbassare i permessi. Non è possibile modificare i permessi dell'amministratore predefinito **admin** e dei gruppi predefiniti **Administrators** e **Newbies**.

La procedura di modifica dei permessi è riportata in p. [Modifica dei permessi](#).

Modifica dei permessi

Per modificare i permessi di un amministratore o un 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. Dalla lista degli amministratori, selezionare l'account che si vuole modificare. Si apre la sezione di modifica delle proprietà.
3. Nella sottosezione **Permessi** è possibile modificare la lista delle azioni consentite per l'amministratore o il gruppo amministrativo selezionato.
4. Per gestire l'ereditarietà dei permessi dell'oggetto selezionato dal gruppo padre, utilizzare il pulsante di opzione:

 **Ereditarietà attivata**

 **Ereditarietà disattivata**

5. Le impostazioni principali vengono definite nella tabella dei permessi:
 - a) La prima colonna riporta i nomi dei permessi. L'intestazione della colonna dipende dalla specifica sezione che unisce i permessi per tipo.

 I permessi degli amministratori e le sezioni del Pannello di controllo di cui sono responsabili gli specifici permessi sono brevemente descritti nel documento **Allegati, B4. Sezioni subordinate dei permessi.**

- b) La colonna **Permessi** riporta le relative impostazioni per i permessi dalla prima colonna.


Oggetti di gestione	Lista delle impostazioni nella colonna Permessi	Principio di impostazione del permesso
Il permesso viene impostato per tutti gli oggetti		
Il permesso non implica la divisione in gruppi per oggetto di gestione.	Può essere riportato uno dei seguenti tipi di permessi: <ul style="list-style-type: none"> • Individuale — per questo oggetto sono configurate le impostazioni individuali. • Ereditato — le impostazioni sono ereditate dal gruppo padre. 	Selezionare / deselezionare il flag Concedi nella riga del permesso corrispondente.
Un permesso viene impostato per una lista di oggetti (postazioni, amministratori o gruppi)		
<ul style="list-style-type: none"> • <i>Concesso tutto</i> — il permesso è concesso per tutti gli oggetti di gestione. • <i>Vietato tutto</i> — il permesso non è concesso per tutti gli oggetti di gestione. • <i>Concesso per alcuni oggetti.</i> Deve essere impostata una lista di oggetti per cui questo permesso è concesso. Per tutti gli altri oggetti il permesso è considerato vietato. 	In caso dell'unione delle impostazioni vengono riportati allo stesso tempo i seguenti tipi di permessi: <ul style="list-style-type: none"> • Individuale — le impostazioni individuali configurate per questo oggetto. • Risultante — il risultato della fusione del permesso individuale dell'oggetto e 	Premere la lista degli oggetti (anche in caso in cui è impostata la variante Tutto). Si apre una finestra con l'albero della rete antivirus, l'albero dei gruppi di amministratori o l'albero delle tariffe a seconda del permesso che viene modificato. Selezionare gli oggetti richiesti nell'albero. Per selezionare più oggetti, utilizzare i tasti CTRL o MAIUSCOLO. Se necessario, spuntare il flag Per tutti i permessi della sezione per applicare queste



Oggetti di gestione	Lista delle impostazioni nella colonna Permessi	Principio di impostazione del permesso
<ul style="list-style-type: none">• <i>Vietato per alcuni oggetti.</i> Deve essere impostata una lista di oggetti per cui questo permesso non è concesso. Per tutti gli altri oggetti il permesso è considerato concesso.	<p>del permesso del gruppo padre.</p> <p>In caso dell'ereditarietà delle impostazioni viene riportato soltanto il tipo di permesso Ereditato.</p>	<p>impostazioni per tutti i permessi riportati nella stessa sezione del permesso che viene modificato.</p> <p>Premere il pulsante:</p> <ul style="list-style-type: none">• Concedi per consentire il permesso nei confronti degli oggetti selezionati.• Vieta per vietare il permesso nei confronti degli oggetti selezionati.



Per uno e lo stesso permesso che viene impostato nei confronti di una lista di oggetti non è possibile impostare allo stesso tempo le liste di oggetti vietati e consenti. Questi concetti si escludono a vicenda.

- c) Nella colonna **Ereditarietà** è riflesso lo stato di questo permesso relativamente al gruppo padre:
- **Ereditarietà dal gruppo** — è attivata l'ereditarietà dal gruppo padre indicato, i permessi individuali non sono impostati.
 - **Impostazioni individuali** — è disattivata l'ereditarietà dal gruppo padre, sono impostati i permessi individuali.
 - **Unione con il gruppo** — è attivata l'ereditarietà dal gruppo padre indicato, sono impostati i permessi individuali. Il permesso risultante dell'oggetto è stato calcolato tramite l'unione dei permessi del gruppo padre e dei permessi individuali (vedi p. [Unione dei permessi](#)).
In questo caso è possibile rimuovere i permessi individuali dell'oggetto. Per farlo, premere il pulsante  nella colonna **Ereditarietà**. Dopo la rimozione dei permessi individuali verrà impostata l'opzione **Ereditarietà dal gruppo**.

Unione dei permessi

Il calcolo del permesso risultante di un oggetto (un amministratore o un gruppo di amministratori), se l'ereditarietà è abilitata, dipende dai permessi dei gruppi padre e dai permessi assegnati all'oggetto stesso. La tabella sotto descrive il principio di ottenimento del permesso risultante di un oggetto:

Permesso del gruppo padre	Permesso del discendente sotto considerazione	Permesso risultante
Concesso tutto	Concesso per alcuni oggetti	Concesso per gli oggetti del discendente



Permesso del gruppo padre	Permesso del discendente sotto considerazione	Permesso risultante
Concesso per alcuni oggetti	Concesso per alcuni oggetti	Le liste di oggetti consentiti si uniscono
Concesso per alcuni oggetti	Concesso tutto	Concesso tutto
I permessi del padre e del discendente sono quelli di divieto, e uno di essi vieta tutto		Vietato tutto
Vietato per alcuni oggetti	Vietato per alcuni oggetti	Le liste di oggetti vietati si uniscono
Vietato tutto	Concesso tutto	Concesso tutto
Vietato per alcuni oggetti	Concesso tutto	Vietato per gli oggetti del padre
Vietato per alcuni oggetti	Concesso per alcuni oggetti	Dagli oggetti vietati vengono sottratti gli oggetti consentiti. Se dopo questo la lista di oggetti vietati non è vuota, il risultato è che sono vietati gli oggetti rimanenti. Altrimenti, il risultato è che sono consentiti tutti gli oggetti del discendente
Concesso per alcuni oggetti	Vietato tutto	Vietato tutto
Concesso tutto	Vietato per alcuni oggetti	Vietato per gli oggetti del discendente
Concesso per alcuni oggetti	Vietato per alcuni oggetti	Dagli oggetti consentiti vengono sottratti gli oggetti vietati. Se dopo questo la lista di oggetti consentiti è vuota, il risultato è che è vietato tutto. Altrimenti, il risultato è che sono consentiti gli oggetti rimanenti.

6.3. Gestione degli account amministratori e dei gruppi di amministratori

6.3.1. Creazione ed eliminazione degli account amministratori e dei gruppi



Il nome utente amministratore deve essere univoco.

Non è possibile connettere un amministratore tramite i sistemi di autenticazione esterni se sul Server Dr.Web 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** nel menu principale del Pannello di controllo, nella finestra che si è aperta selezionare la voce del menu di gestione **Amministratori**.
2. Nella barra degli strumenti premere 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 che verrà utilizzato per l'accesso al Pannello di controllo. Sono permesse le minuscole (a-z), le maiuscole (A-Z), le cifre (0-9), i caratteri "_" e ".".
 - Nei campi **Password** e **Confermare la password** impostare la password di accesso al Server Dr.Web e quindi al Pannello di controllo.



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



I campi per l'impostazione della password sono attivi soltanto per gli amministratori con l'autenticazione interna.

Non hanno importanza i valori di questi campi, impostati nel Pannello di controllo per gli amministratori con l'autenticazione esterna.

- Nei campi **Cognome**, **Nome** e **Patronimico** è possibile indicare i dati personali dell'amministratore.
- Indicare un **Indirizzo email**. Altrimenti, non sarà possibile resettare la password, se necessario.
- Dalla lista a cascata **Lingua dell'interfaccia** selezionare la lingua dell'interfaccia del Pannello di controllo, che verrà utilizzata dall'amministratore che viene creato (di default è impostata la lingua del browser o l'inglese).



Se si seleziona una lingua in cui i testi dell'interfaccia al momento non vengono aggiornati, verrà suggerito di attivare l'aggiornamento per questa lingua. Per fare ciò, andare attraverso il link alla sezione **Amministrazione** → **Configurazione generale del repository** → **Server Dr.Web** → **Lingue del Pannello di controllo della sicurezza Dr.Web**, impostare il flag per la lingua desiderata e premere **Salva**. Al prossimo aggiornamento del repository i testi dell'interfaccia per la lingua selezionata verranno aggiornati. È inoltre possibile avviare manualmente l'aggiornamento nella sezione **Stato del repository**.



- Dalla lista a cascata **Formato della data** selezionare il formato che verrà utilizzato da questo amministratore quando modifica le 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** è possibile impostare una descrizione dell'account.



I valori dei campi contrassegnati con il carattere * sono da impostare.

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.




In modo che l'amministratore aggiunto abbia informazioni operative sugli eventi nella rete antivirus, si consiglia subito dopo la creazione dell'account di configurare gli avvisi seguendo le istruzioni della sezione [Configurazione degli avvisi](#). Per fornire la possibilità di creazione dei report statistici secondo il calendario, è necessario attivare l'avviso **Report statistico**.

Aggiunzione di gruppi di amministratori



Per poter creare gruppi di amministratori, è necessario avere il permesso di **Creazione degli amministratori, dei gruppi di amministratori**.

Per aggiungere un nuovo account gruppo di amministratori

1. Selezionare la voce **Amministrazione** nel menu principale del Pannello di controllo, nella finestra che si è aperta selezionare la voce del menu di gestione **Amministratori**.
2. Nella barra degli strumenti premere l'icona  **Crea 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** è possibile 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, è necessario 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 gruppo

1. Selezionare la voce **Amministrazione** nel 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 **✗ Rimuovi gli oggetti selezionati**.
Se l'amministratore da rimuovere è l'autore di [task dal calendario di Server Dr.Web](#), prima di rimuovere il suo account, riassegnare i task a un altro amministratore nella parte destra della finestra. Quindi premere il pulsante **Rimuovi**.
4. Confermare la rimozione.

6.3.2. Ripristino della password amministratore

La password dell'account amministratore dimenticata può essere ripristinata nei seguenti modi:

1. Resettare la password all'accesso al Pannello di controllo della sicurezza Dr.Web.
2. Impostare una nuova password nella riga di comando all'avvio del Server Dr.Web.

Per resettare la password all'accesso al Pannello di controllo della sicurezza Dr.Web

1. Aprire la pagina di autenticazione (http://<Indirizzo_Server_Dr.Web>:9080 o https://<Indirizzo_Server_Dr.Web>:9081), dove come <Indirizzo_Server_Dr.Web> indicare l'indirizzo IP o il nome DNS del computer su cui è installato il Server Dr.Web.
2. Premere **Resetta password**.



3. Nella finestra che si è aperta compilare i campi **Nome utente** e **Indirizzo email** inserendo i dati dell'account amministratore di cui si vuole ripristinare la password.



L'indirizzo email che viene inserito deve coincidere con l'indirizzo specificato nelle [impostazioni dell'account](#) amministratore.

4. Premere **Invia link**. All'indirizzo email indicato verrà inviata un'email con un link per il reset della password.



L'email verrà inviata previa configurazione del server SMTP (vedi sezione [E-mail](#)).

5. Andare al link indicato e impostare una nuova password sulla pagina che si è aperta. Se l'email non è stata ricevuta, riprovare.

Per modificare la password all'avvio del Server Dr.Web tramite la riga di comando:

Avviare il Server Dr.Web dalla riga di comando indicando il parametro necessario per il cambio della password, il nome utente amministratore e la nuova password:

```
drwcsd modexecdb set-admin-password <nome_utente> <nuova_password>
```

6.3.3. Modifica degli account amministratori e dei gruppi




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

Per poter modificare il proprio account, è necessario avere il permesso di **Modifica delle proprie impostazioni**.

I valori dei campi contrassegnati con il carattere * sono da impostare.

Per modificare l'account amministratore

1. Dalla lista degli amministratori, selezionare l'account che si vuole modificare. Si apre la sezione di modifica delle proprietà.
2. Nella sottosezione **Generali** è possibile 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 della creazione account e dell'ultima modifica 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** è possibile modificare la lista delle azioni consentite per l'amministratore selezionato.

La procedura di modifica dei permessi è riportata nella sottosezione [Modifica dei permessi](#).

5. Per rendere effettive le modifiche apportate, premere il pulsante **Salva**.

Per modificare il gruppo di amministratori

1. Dalla lista degli amministratori, selezionare il gruppo che si vuole modificare. Si apre la sezione di modifica delle proprietà.

2. Nella sottosezione **Generali** è possibile modificare i parametri che sono stati impostati durante la [creazione](#).

3. Nella sottosezione **Gruppi** è possibile cambiare il gruppo padre. Nella lista sono riportati i gruppi disponibili che possono essere assegnati come gruppo padre. Di fronte al gruppo padre corrente è spuntato un flag. 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** è possibile modificare la lista delle azioni consentite per il gruppo di amministratori selezionato.

La procedura di modifica dei permessi è riportata nella sottosezione [Modifica dei permessi](#).


5. Per rendere effettive le modifiche apportate, premere il pulsante **Salva**.



È possibile assegnare il gruppo padre agli amministratori e ai gruppi di amministratori in uno dei seguenti modi:

- Si possono modificare le impostazioni dell'amministratore o del gruppo secondo il modo descritto [sopra](#).
- Trascinare un amministratore o un gruppo di amministratori nella lista gerarchica sopra il gruppo il quale si desidera assegnare come gruppo padre.

Per propagare i permessi di un amministratore o gruppo su un altro amministratore o gruppo

1. Nella lista degli amministratori selezionare un oggetto di cui i permessi si vogliono propagare. Questo può essere sia un amministratore che un gruppo di amministratori.
2. Nella barra degli strumenti premere il pulsante  **Propaga i permessi dell'amministratore**.
3. Nella finestra che si è aperta selezionare oggetti a cui si vogliono assegnare i permessi. Notare le seguenti caratteristiche:
 - È possibile selezionare uno o più oggetti a cui assegnare permessi. Questi possono essere sia amministratori che gruppi di amministratori.
 - Per gli oggetti selezionati i permessi vengono salvati come individuali. L'ereditarietà dal gruppo padre viene interrotta.
 - Non è ammessa l'assegnazione di permessi agli oggetti creati di default (i gruppi **Administrators**, **Newbies**, l'amministratore **admin**).
 - È possibile propagare permessi solo sugli oggetti consentiti nei permessi **Modifica degli account amministratori** e **Modifica delle proprietà e della configurazione dei gruppi di amministratori**.
 - Se la propagazione comporterà l'assegnazione di permessi che eccedono i propri permessi dell'amministratore che esegue l'operazione, viene restituito un errore di permessi insufficienti per l'esecuzione dell'operazione.
4. Premere il pulsante **Propaga**.



Capitolo 7: Gestione integrata delle postazioni

Per la gestione integrata delle postazioni e delle loro impostazioni vengono offerti i seguenti strumenti:

- **Gruppi.**

Una postazione può rientrare in un numero illimitato di gruppi. Obbligatoriamente nei gruppi predefiniti in base al suo stato e opzionalmente nei gruppi personalizzati. Tuttavia, solo uno dei gruppi è primario.

- **Criteri.**

A una postazione può essere assegnato solo un criterio o non assegnato nessun criterio.

- **Profili.**

I profili sono usati per configurare le impostazioni del componente [Controllo delle applicazioni](#). I profili possono essere assegnati sia a postazioni e gruppi di postazioni che a singoli utenti.

Per controllare l'avvio delle applicazioni sulle postazioni, è necessario che almeno un profilo attivo sia assegnato alla postazione o a un utente della postazione.

Tipi di impostazioni delle postazioni

- **Impostazioni ereditate.**


Quando viene creata una postazione, essa sempre eredita le impostazioni dal criterio o dal gruppo primario. Per maggiori informazioni consultare la sezione [Ereditarietà della configurazione della postazione](#).

- **Impostazioni individuali.**

Nel corso del funzionamento della postazione l'ereditarietà può essere interrotta e possono essere definite le impostazioni individuali.

Per definire le impostazioni individuali per una postazione, modificare la sezione delle impostazioni corrispondente.

Se le impostazioni individuali sono definite per una postazione, le impostazioni del criterio o gruppo primario assegnato e qualsiasi modifica delle stesse non influenzerà le impostazioni della postazione.

È possibile ripristinare l'ereditarietà dal criterio o gruppo primario. Per farlo, premere il pulsante  **Rimuovi impostazioni individuali** nella barra degli strumenti del Pannello di controllo nella sezione delle impostazioni corrispondenti o nella sezione delle proprietà della postazione.



In ciascuna sezione delle impostazioni degli elementi di configurazione di una postazione viene indicato se le impostazioni di questa sezione sono definite individualmente o sono ereditate dall'oggetto corrispondente.



Una parte delle sezioni delle impostazioni può essere definita individualmente, e una parte può essere ereditata da un criterio o dal gruppo primario, se nessun criterio è impostato.

È possibile impostare diverse configurazioni per diversi [gruppi](#) e diverse [postazioni](#), modificando le impostazioni corrispondenti.

7.1. Ereditarietà della configurazione della postazione

Quando viene creata una postazione o un gruppo, essi sempre ereditano impostazioni:

- Un nuovo gruppo eredita impostazioni dal suo gruppo padre in cui è direttamente incluso. Se non c'è un gruppo padre (il gruppo che viene creato è un gruppo radice nell'albero gerarchico), il gruppo eredita impostazioni dal gruppo **Everyone**.
- Una nuova postazione eredita impostazioni da un criterio che è stato assegnato durante la creazione della postazione. Se nessun criterio è stato assegnato, la postazione eredita impostazioni da uno dei gruppi di cui fa parte. Tale gruppo si chiama *primario*.

Nel corso del successivo funzionamento l'ereditarietà può essere interrotta e possono essere definite le impostazioni individuali della postazione.

Per il componente Controllo delle applicazioni il principio di ereditarietà delle impostazioni differisce da quello standard. Per maggiori informazioni vedi [Ereditarietà delle impostazioni per il componente Controllo delle applicazioni](#).

Priorità di applicazione delle impostazioni per le postazioni:

1. Se una postazione ha impostazioni individuali, vengono utilizzate le impostazioni individuali. In questo caso, alla postazione può essere assegnato un criterio. Se vengono configurate impostazioni individuali di una determinata sezione, l'ereditarietà delle impostazioni di questa sezione viene interrotta.
2. Se non ci sono impostazioni individuali, vengono utilizzate le impostazioni di un criterio assegnato.
3. Se non ci sono impostazioni individuali e non c'è alcun criterio assegnato, la postazione utilizza le impostazioni del suo gruppo primario.

Sono definite impostazioni individuali	Assegnato criterio	Impostazioni utilizzate
+	+	Impostazioni individuali
+	-	Impostazioni individuali
-	+	Impostazioni del criterio
-	-	Impostazioni del gruppo primario



Può non esserci nessun criterio assegnato a una postazione, ma una postazione ha sempre un gruppo primario.

Ereditarietà delle impostazioni delle postazioni da criteri

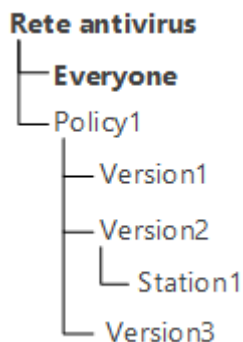
Se a una postazione è assegnato un criterio, viene impostata l'ereditarietà delle impostazioni della postazione dalle impostazioni del criterio.

Se vengono modificate le impostazioni di un criterio, le postazioni a cui è assegnato questo criterio ereditano le modifiche, ad eccezione dei casi in cui alle postazioni sono state assegnate impostazioni individuali. Quando viene creata una postazione, è possibile indicare quale dei criteri verrà assegnato alla postazione. Il criterio può essere sostituito in qualsiasi momento durante l'utilizzo. Se nessun criterio verrà assegnato, la postazione erediterà le impostazioni dal gruppo primario.

I criteri non hanno la struttura di ereditarietà gerarchica. Quando viene creato un criterio, le sue impostazioni vengono copiate come impostazioni individuali da un oggetto impostato (di default questo è il criterio **Default policy**). Solo una delle versioni del criterio è corrente e le sue impostazioni sono le impostazioni del criterio stesso. Solo la versione corrente può essere assegnata alle postazioni.

Per esempio:

La struttura della lista gerarchica è il seguente albero:



Alla postazione `Station1` è assegnato il criterio `Policy1`. La versione del criterio `Version2` è quella corrente per il criterio `Policy1`. Le impostazioni della versione `Version2` coincidono con le impostazioni del criterio `Policy1`, le quali sono impostazioni individuali.

Ereditarietà delle impostazioni delle postazioni da gruppi

Se a una postazione non è assegnato alcun criterio, viene impostata l'ereditarietà delle impostazioni della postazione dalle impostazioni del suo gruppo primario.



Se vengono modificate le impostazioni del gruppo primario, le postazioni incluse nel gruppo ereditano le modifiche, ad eccezione dei casi in cui alle postazioni sono state assegnate impostazioni individuali. Quando viene creata una postazione, è possibile indicare quale dei gruppi verrà considerato primario. Di default, il gruppo primario è **Everyone**. Il gruppo primario può essere sostituito in qualsiasi momento nel processo di utilizzo.



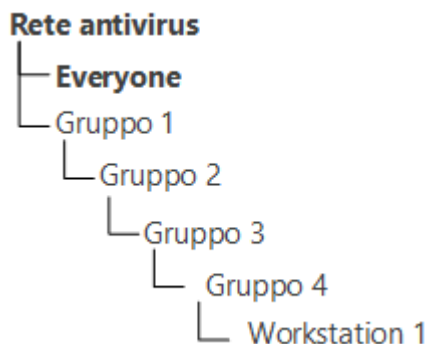
Se il gruppo primario non è **Everyone** e se il gruppo primario indicato, che è un gruppo radice nell'albero gerarchico della rete antivirus, non ha impostazioni individuali, la nuova postazione eredita le impostazioni del gruppo **Everyone**.

È possibile creare gruppi nidificati.

Se ci sono gruppi nidificati, se per la postazione non sono state definite impostazioni individuali, essa eredita elementi di 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 rilevate impostazioni individuali, la postazione eredita gli elementi di configurazione del gruppo **Everyone**.


Per esempio:

La struttura della lista gerarchica è il seguente albero:



Il Gruppo Gruppo4 è primario per la postazione Workstation1. Quando la postazione Workstation1 eredita impostazioni, la ricerca delle impostazioni viene eseguita nel seguente ordine: Workstation1 → Gruppo4 → Gruppo3 → Gruppo2 → Gruppo1 → Everyone.



Di default, la struttura della 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 della 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**.



Ereditarietà delle impostazioni per il componente Controllo delle applicazioni

Le impostazioni dei profili Controllo applicazioni possono essere assegnate non solo a postazioni e gruppi di postazioni, ma anche a singoli utenti e gruppi di utenti.

Priorità di impiego delle impostazioni:

1. Se ci sono impostazioni utente, hanno la massima priorità.
2. In assenza di impostazioni utente, viene data priorità alle impostazioni del gruppo di utenti.
3. Se non sono specificate le impostazioni per utenti e gruppi di utenti, l'ereditarietà viene effettuata in base alla [priorità di applicazione delle impostazioni per le postazioni](#).

7.2. Gruppi

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

Il raggruppamento di postazioni può servire ai seguenti scopi:

- Applicare operazioni di gruppo a tutte le postazioni che fanno parte di tale gruppo.
Sia per un gruppo singolo che per più gruppi selezionati è possibile avviare, visualizzare e terminare i task di scansione delle postazioni che fanno parte di tale gruppo. È inoltre possibile visualizzare le statistiche (tra l'altro, infezioni, virus, avvio/arresto, errori di scansione e di installazione ecc.) e le statistiche riassuntive 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. [Capitolo 7: Gestione integrata delle postazioni](#)).
- Sistemare (strutturare) la lista delle postazioni.

Si possono creare anche gruppi nidificati.

7.2.1. 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 Dr.Web è stato installato e fino a quando le postazioni non si connetteranno ad esso, solo 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 include tutte le postazioni conosciute dal Server Dr.Web. Il gruppo **Everyone** contiene le impostazioni predefinite di tutte le postazioni e i gruppi.

Active Directory

Il gruppo contiene utenti e gruppi di utenti registrati nel dominio Active Directory. Questo gruppo compare nell'albero della rete antivirus dopo l'esecuzione del task **Sincronizzazione con Active Directory** dal [calendario](#) del Server Dr.Web.

Configured

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

Neighbors

Il gruppo **Neighbors** contiene tutti i Server Dr.Web collegati con questo Server Dr.Web e si utilizza per gestire le relazioni tra i Server Dr.Web in una rete antivirus con diversi server (v. [Caratteristiche di una rete con diversi Server Dr.Web](#)).

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

Il gruppo **Neighbors** contiene gruppi nidificati che rispecchiano lo stato dei Server Dr.Web adiacenti connessi a questo Server Dr.Web:

- Il gruppo **All neighbors** contiene tutti i Server Dr.Web adiacenti connessi a questo Server Dr.Web.
- Il gruppo **Children** contiene i Server Dr.Web subordinati.
- Il gruppo **Offline** contiene tutti i Server Dr.Web non attivi al momento.
- Il gruppo **Online** contiene tutti i Server Dr.Web attivi al momento.
- Il gruppo **Parents** contiene i Server Dr.Web principali.
- Il gruppo **Peers** contiene i Server Dr.Web paritari.



Operating system

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 di gruppi che corrispondono ad una versione concreta del sistema operativo mobile Android.
- I sottogruppi della famiglia **macOS**. Questa famiglia include un set di gruppi che corrispondono a una versione concreta del sistema operativo macOS.
- I sottogruppi della famiglia **UNIX**. Questa famiglia include una serie di gruppi che corrispondono ai sistemi operativi della famiglia UNIX, per esempio, Linux, FreeBSD ecc.
- I sottogruppi della famiglia **Windows**. Questa famiglia include una serie di gruppi che corrispondono a una specifica versione del sistema operativo Windows.
- Categoria **Unknown OS**. Qui sono visualizzate le postazioni che funzionano con un sistema operativo sconosciuto al Server Dr.Web.

Policies

Il gruppo che contiene criteri studiati per configurare impostazioni delle postazioni.



Il gruppo **Policies** verrà visualizzato nell'albero della rete antivirus solo se l'uso di criteri è consentito nella configurazione di Server Dr.Web.

Profiles

Il gruppo che contiene profili con le impostazioni del componente Controllo delle applicazioni per le postazioni SO Windows. V. [Profili](#).

Proxies

Il gruppo che contiene i Server proxy Dr.Web per la connessione degli Agent Dr.Web e dei Server Dr.Web adiacenti.

Status

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

- Il gruppo **Deinstalled**. Non appena il software Agent Dr.Web viene rimosso da una postazione, la postazione viene trasferita automaticamente nel gruppo **Deinstalled**.



- Il gruppo **Deleted** contiene le postazioni che l'amministratore ha precedentemente rimosso dal Server Dr.Web. È possibile recuperare queste postazioni (v. [Rimozione e recupero della postazione](#)).
- Il gruppo **New** contiene le nuove postazioni che sono state create dall'amministratore attraverso il Pannello di controllo, ma l'Agent Dr.Web su di esse non è stato ancora installato.
- Il gruppo **Newbies** contiene tutte le postazioni di cui la registrazione sul Server Dr.Web al momento non è stata ancora confermata. Dopo la conferma della registrazione sul Server Dr.Web, le postazioni verranno automaticamente escluse da questo gruppo (per dettagli v. [Criteri di approvazione delle postazioni](#)).
- Il gruppo **Offline** contiene tutte le postazioni non attive al momento.
- Il gruppo **Online** contiene tutte le postazioni attive al momento (che rispondono alle richieste del Server Dr.Web).
- 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 sono al momento connesse al Server Dr.Web. Questi sottogruppi sono completamente virtuali e non possono contenere impostazioni, inoltre, non possono essere gruppi primari.

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

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

Per comodità, la tabella [7-1](#) 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 la possibilità di inclusione automatica delle postazioni nel gruppo (supporto dell'appartenenza automatica), nonché di modifica automatica della lista elementi del gruppo nel processo di funzionamento del Server Dr.Web.



- **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 7-1. Gruppi e parametri supportati

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



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

7.2.2. Gestione dei gruppi

7.2.2.1. Creazione ed eliminazione di gruppi

Per creare un nuovo gruppo



1. Selezionare la voce **Rete antivirus** nel menu principale del Pannello di controllo.
2. Selezionare la voce **+ Aggiungi oggetto della rete** nella barra degli strumenti, quindi dal sottomenu selezionare la voce **+ Crea gruppo**.
Si apre la finestra di creazione del gruppo.
3. Il campo di input **Identificatore** viene compilato in modo automatico. Se necessario, è possibile modificarlo durante la creazione. L'identificatore non deve includere spazi. In seguito l'identificatore del gruppo non può essere modificato.



4. Inserire nel campo **Nome** il nome del gruppo.
5. 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 impostazioni individuali. 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**.
6. Inserire un commento nel campo **Descrizione**.
7. Premere il pulsante **Salva**.

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

Per rimuovere 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.

7.2.2.2. Modifica dei gruppi

Per modificare le impostazioni del gruppo

1. Selezionare la voce **Rete antivirus** nel 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) Fare clic sul nome di un gruppo nella lista gerarchica della rete antivirus. Nella parte destra della finestra del Pannello di controllo si apre automaticamente 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.

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



Generali

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

- **Identificatore** — l'identificatore del gruppo univoco. Non è modificabile.
- **Nome** — il nome del gruppo. Se necessario, è possibile modificare il nome di un gruppo personalizzato. Per i gruppi predefiniti il campo **Nome** non è modificabile.
- **Gruppo padre** — il gruppo padre in cui rientra questo gruppo e da cui eredita la sua configurazione, se non sono configurate le impostazioni individuali. Se nessun gruppo padre è assegnato, il gruppo eredita le impostazioni dal gruppo **Everyone**.
- **Descrizione** — un campo opzionale per la descrizione del gruppo.

Informazioni sulle postazioni

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

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

Ente

Se alla creazione di un gruppo esso è stato definito come gruppo che rappresenta un ente o un'azienda, per la modifica sarà disponibile la sezione **Ente**. In questa sezione è possibile modificare le informazioni dell'ente che questo gruppo rappresenta. L'insieme di informazioni può essere diverso a seconda del paese in cui si trova l'ente.



Un gruppo può essere designato come gruppo che rappresenta un ente solo durante la creazione. Neanche è possibile annullare questa caratteristica dopo la creazione del gruppo.


Configurazione



Per ulteriori informazioni sull'ereditarietà delle impostazioni dai gruppi primari da parte delle postazioni, v. la sezione [Capitolo 7: Gestione integrata delle postazioni](#).



Nella sezione **Configurazione** è possibile modificare la configurazione di gruppi, la quale 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.	Chiavi di licenza
	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 questa 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
	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

Per i gruppi in cui sono definite impostazioni individuali nella sezione **Configurazione** viene indicato il numero di gruppi nidificati con l'ereditarietà interrotta e con le proprie impostazioni individuali, se presenti. Quando si fa clic su questa opzione, si apre una finestra con una lista dei gruppi per cui sono indicati i loro nomi e identificatori.

7.2.3. Inserimento delle postazioni in 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 di una postazione.
2. Si apre la barra delle proprietà della postazione. Inoltre, si può aprire la sezione delle proprietà della postazione selezionando nel [menu di gestione](#) la voce **Proprietà**. Nella finestra che si è aperta passare alla sottosezione **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 più 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, premendo i tasti della tastiera CTRL o MAIUSCOLO.
2. Nella barra degli strumenti premere **★ Generali** → **1. Assegna gruppo primario alle postazioni**. Si apre la finestra con una lista dei gruppi che possono essere assegnati come primari 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** → **1. Imposta questo gruppo come primario**.

Inserimento in gruppi custom

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

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

7.2.3.1. Inserimento manuale delle postazioni in gruppi

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

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



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 di una postazione.
2. Si apre la barra delle proprietà della postazione. Inoltre, si può aprire la sezione delle proprietà della postazione selezionando nel [menu di gestione](#) la voce **Proprietà**.
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 è possibile assegnare il gruppo primario alla postazione (per maggiori informazioni v. [Ereditarietà della configurazione della postazione](#)).

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 ed espandere la lista gerarchica dei gruppi e delle postazioni.
2. Per aggiungere la postazione a un gruppo custom, premere e tenere premuto il tasto CTRL e trascinare la postazione con il mouse nel gruppo richiesto.
3. Per spostare la postazione da un gruppo custom in un altro, trascinarla con il mouse 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.



7.2.3.2. Configurazione dell'appartenenza automatica a un gruppo

Dr.Web Enterprise Security Suite fornisce 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:
 - Nella barra 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 **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 con cui le postazioni verranno inserite in questo gruppo:
 - a) Se per un gruppo prima non sono state impostate le regole di appartenenza, premere **Aggiungi regola**.
 - b) Spuntare il flag **Imposta il gruppo come primario** affinché il gruppo per cui viene creata la regola venga impostato automaticamente come il gruppo primario per tutte le postazioni che verranno trasferite in questo gruppo in base a questa regola.
 - c) Selezionare una delle opzioni che determinano come verranno applicate le regole: **Applica le regole dopo il salvataggio** o **Applica le regole dopo la connessione delle postazioni**.
 - d) Per ciascun blocco delle regole definire 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 condizioni selezionare: uno dei parametri della postazione che verrà controllato per la corrispondenza alle condizioni; il principio di corrispondenza a questa condizione e, se il parametro della postazione lo sottintende, inserire la stringa della condizione.
Le postazioni possono essere unite in gruppi in base alle seguenti condizioni:
 - **Indirizzo IP della postazione** (set di caratteri che sono contenuti nell'indirizzo IP, sottorete a cui esso appartiene o espressione regolare);
 - **descrizione** (set di caratteri che sono contenuti nella descrizione o espressione regolare);



- **ID della postazione** (set di caratteri che sono contenuti nell'ID o espressione regolare);
- **nuovo arrivo** (le postazioni vengono aggiunte a un gruppo in base alla presenza o all'assenza dello stato di nuovo arrivo);
- **LDAP DN da Active Directory** (set di caratteri che sono contenuti in LDAP DN o espressione regolare);



Se viene impostato il parametro **LDAP DN da Active Directory**, è necessario:

1. Attivare il task **Sincronizzazione con Active Directory** nel calendario di Server Dr.Web (sezione **Amministrazione** → **Scheduler di Server Dr.Web**).
2. Nelle regole di appartenenza come la stringa della condizione per il parametro **LDAP DN da Active Directory** impostare il valore DN richiesto, per esempio:
`OU=OrgUnit,DC=Department,DC=domain,DC=com`



Espressioni regolari possono essere impostate solo per la variante **corrisponde all'espressione regolare**. Per tutti gli altri tipi viene utilizzata la ricerca per corrispondenza esatta alla stringa inserita.

L'utilizzo delle espressioni regolari è brevemente descritto in documento **Allegati, Allegato J. Utilizzo delle espressioni regolari in Dr.Web Enterprise Security Suite**.

- **sistema operativo** installato sulla postazione (Windows, UNIX, MacOS, Android e altri; c'è anche il parametro "Sconosciuto");
 - **numero di build del sistema operativo** (set di caratteri che sono contenuti nel numero o espressione regolare);
 - **piattaforma della postazione** (versione del sistema operativo installato sulla postazione; solo per Android, Windows e MacOS);
 - **protocollo di connessione** (TCP IP, TCP IPv6, UNIX);
 - **ID del Server Dr.Web** (set di caratteri che sono contenuti nell'ID o espressione regolare);
 - **nome della postazione** (set di caratteri che sono contenuti nel nome o espressione regolare);
 - **tipo di postazione** (agent completo, agent virtuale, server di scansione).
- Per aggiungere un'altra condizione a questo blocco, premere **+** a destra della stringa della condizione.
- e) 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 applicare queste regole allo stesso tempo a tutte le postazioni registrate su questo Server Dr.Web. In caso






di un grande numero di postazioni connesse al Server Dr.Web, l'esecuzione di questa azione può richiedere del tempo. Le regole di nuovo raggruppamento di postazioni vengono applicate a tutte le postazioni già registrate immediatamente quando viene impostata l'azione e verranno applicate a tutte le postazioni, anche a quelle che verranno registrate sul Server Dr.Web per la prima volta al momento della loro connessione.

- **Applica al momento della connessione delle postazioni** — per salvare le regole di appartenenza impostate e applicare queste regole alle postazioni al momento in cui si connettono al Server Dr.Web. Le regole di nuovo raggruppamento di postazioni vengono applicate a tutte le postazioni già registrate al momento della loro successiva connessione al Server Dr.Web e verranno applicate a tutte le postazioni che vengono registrate sul Server Dr.Web 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 icona delle regole di appartenenza** nella lista  **Impostazioni della vista albero** nella barra degli strumenti.



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

Per rimuovere 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**.
 - Nella barra 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**.

7.2.4. Confronto delle postazioni e dei gruppi

È possibile confrontare le postazioni e i gruppi secondo i parametri principali.








Per confrontare più 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:
 - selezione di più postazioni — per confrontare le postazioni selezionate;
 - selezione di più gruppi — per confrontare i gruppi selezionati e tutti i gruppi nidificati;
 - selezione di più postazioni e gruppi — per confrontare tutte le postazioni: sia quelle selezionate direttamente nella lista gerarchica che quelle che fanno parte dei gruppi selezionati e dei relativi gruppi nidificati.
2. Nel [menu di gestione](#) premere la voce **Confronto**.
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 questo gruppo è primario.
 - **Configurazione individuale** — 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** — lista dei componenti che hanno le impostazioni individuali, non ereditate dal gruppo primario.
 - **Componenti installati** — lista dei componenti antivirus installati sulla postazione.

7.2.5. 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 apportare le modifiche alla configurazione di questi gruppi, premere il pulsante **Salva**.

7.3. Criteri

Criterio è la totalità di tutte le impostazioni esistenti di una postazione: permessi, calendario dei task, chiavi di licenza, limitazioni degli aggiornamenti, lista dei componenti da installare, configurazione dei componenti antivirus.



Un criterio può essere assegnato solo a postazioni.

Per consentire l'uso di criteri per la configurazione delle postazioni

1. Selezionare la voce **Amministrazione** nel menu principale del Pannello di controllo, nella finestra che si è aperta selezionare la voce del menu di gestione **Configurazione del Server Dr.Web**.
2. Nella scheda **Generali**:
 - a) Spuntare il flag **Usa criteri**.
 - b) Nel campo **Numero di versioni del criterio** impostare il numero massimo di versioni che possono essere create per ciascun criterio. Se con la creazione di una nuova versione di un criterio questo numero viene superato, la versione più vecchia del criterio verrà rimossa.
3. Premere **Salva** e riavviare il Server Dr.Web.
4. Dopo che è stato consentito l'uso di criteri, viene creato un criterio predefinito **Default policy**. Questo criterio non può essere rimosso, ma può essere modificato e assegnato alle postazioni.



Dimodoché un amministratore possa gestire criteri e le relative impostazioni, gli devono essere assegnati i [permessi](#) **Visualizzazione delle proprietà e della configurazione dei criteri** e **Modifica delle proprietà e della configurazione dei criteri**.

Se non sono assegnati permessi, i criteri verranno visualizzati nell'albero della rete antivirus e nella Gestione licenze, ma non sarà possibile visualizzare i loro contenuti e gestirli.



7.3.1. Gestione dei criteri

Creazione di un criterio

Per creare un nuovo criterio

1. Selezionare la voce **Rete antivirus** nel menu principale del Pannello di controllo.
2. Selezionare la voce **+ Aggiungi oggetto della rete** nella barra degli strumenti, quindi dal sottomenu selezionare la voce **+ Crea criterio**.
Si apre la finestra di creazione del criterio.
3. Il campo di input **Identificatore** viene compilato in modo automatico. Se necessario, è possibile modificarlo durante la creazione. L'identificatore non deve includere spazi. In seguito l'identificatore del criterio non può essere modificato.
4. Nel campo **Nome** impostare il nome del criterio.
5. Quando viene configurato un criterio, le sue impostazioni vengono copiate di default dal criterio **Default policy**. Per modificare l'oggetto da cui verranno copiate le impostazioni, fare clic sul link **Seleziona un altro oggetto**. Nella finestra che si è aperta selezionare un oggetto dalla lista proposta. Questo può essere un gruppo, una postazione, un altro criterio o una versione di un criterio. È possibile selezionare solo un oggetto. Premere il pulsante **Salva**. L'oggetto selezionato verrà visualizzato nella finestra di creazione del criterio.
6. Per creare il criterio con le impostazioni definite, premere il pulsante **Salva**.
7. A creazione di un criterio viene creata automaticamente una versione del criterio corrispondente alla data di aggiunta del criterio stesso.

Versioni di un criterio

Un criterio può contenere diverse versioni, ma non più di quante sono indicate nelle impostazioni della configurazione del Server Dr.Web. Il nome di una versione di un criterio corrisponde al momento della sua creazione.

Per creare una nuova versione di un criterio

1. Selezionare la voce **Rete antivirus** nel menu principale del Pannello di controllo.
2. Alle impostazioni dei criteri si accede tramite la lista gerarchica della rete antivirus. Modificare la configurazione del criterio per cui si desidera creare una nuova versione. È possibile farlo manualmente o importando/propagando la configurazione da un altro oggetto della rete antivirus (postazione, gruppo, criterio).
3. Quando si salvano le modifiche, verrà creata automaticamente una nuova versione del criterio sulla base delle impostazioni del criterio specificate. La versione creata verrà nominata corrente.



Solo una versione di un criterio è corrente e può essere assegnata alle postazioni.

Le impostazioni della versione di un criterio sono di sola lettura.

Per modificare la versione corrente di un criterio



1. Selezionare la voce **Rete antivirus** nel menu principale del Pannello di controllo.
2. Nella lista gerarchica selezionare un criterio, la cui versione corrente si vuole modificare.
3. Nel pannello delle proprietà che si è aperto nella sezione **Generali** nella lista a cascata **Versione corrente** selezionare la versione richiesta.
4. Premere il pulsante **Salva**.

Rimozione di un criterio



È possibile rimuovere criteri sia per intero che per versione.

Per rimuovere un criterio o una versione di un criterio

1. Selezionare la voce **Rete antivirus** nel menu principale del Pannello di controllo.
2. Selezionare un criterio o una versione di un criterio nella lista gerarchica.
3. Nella barra degli strumenti premere  **Generali** →  **Rimuovi gli oggetti selezionati**.



Quando si rimuove un criterio, prestare attenzione alle seguenti caratteristiche:

- Se viene rimossa la versione ultima rimasta di un criterio, il criterio stesso anche viene rimosso.
- Se viene rimossa la versione corrente di un criterio, diventa corrente la versione più recente (quella con la data più recente).
- A tutte le postazioni cui era assegnata la versione rimossa del criterio verrà assegnata la versione corrente di questo criterio.

7.3.2. Assegnazione di un criterio alle postazioni



A una postazione può essere assegnato solo un criterio.

Alle postazioni può essere assegnato solo quel criterio per cui [è impostata una chiave di licenza](#).



Per assegnare o modificare il criterio della postazione

1. Selezionare la voce **Rete antivirus** nel menu principale del Pannello di controllo.
2. Nella lista gerarchica selezionare una postazione cui si vuole assegnare un criterio o di cui il criterio si vuole modificare.
3. Nel pannello delle proprietà della postazione che si è aperto nella sezione **Gruppi** nella lista **Criteri** spuntare il flag di fronte al criterio che si vuole assegnare.

Se in precedenza è stato già assegnato un criterio, il relativo flag verrà tolto automaticamente in quanto a una postazione può essere assegnato solo un criterio.

Inoltre, è possibile togliere i flag a tutti i criteri. In questo caso le impostazioni della postazione torneranno al loro stato precedente che era prima dell'assegnazione di un criterio.

4. Premere il pulsante **Salva**.

7.4. Profili

I *profili* definiscono le impostazioni del componente [Controllo delle applicazioni](#) in conformità alle quali sulle postazioni possono essere avviati o bloccati applicazioni, moduli, interpreti di script, driver e pacchetti MSI.

I profili vengono creati dall'amministratore e vengono assegnati a criteri, postazioni e utenti, inclusi gruppi di postazioni e utenti. I profili determinano la [modalità di funzionamento](#) di Controllo delle applicazioni.

I profili vengono configurati attraverso l'albero della rete antivirus:

- Tutti i profili sono collocati in un gruppo predefinito **Profiles**.
- Gli oggetti cui è assegnato un profilo specifico sono collocati nell'albero della rete antivirus come elementi figlio di questo profilo.

Per configurare Controllo delle applicazioni

1. [Creare un nuovo profilo](#).
2. [Configurare le impostazioni del profilo](#).
3. [Assegnare il profilo a tutti gli oggetti richiesti](#).



Si consiglia di configurare il funzionamento dei profili in modalità test.

Ci sono le seguenti modalità di funzionamento dei profili:

- **Disattivato** — il profilo non è attivo, le impostazioni del profilo non vengono applicate.



- **Attivo** — il profilo è attivo, le impostazioni vengono applicate agli oggetti su cui questo profilo è propagato.
- **Test globale** — il profilo è attivo, ma funziona in modalità test globale. La modalità test simula il funzionamento di Controllo delle applicazioni con la registrazione del log delle attività completo (v. [Eventi di Controllo delle applicazioni](#)), tuttavia, nessun blocco delle applicazioni effettivo viene eseguito.
- **Test per le regole** — il profilo è attivo, e agli oggetti vengono applicate le impostazioni di analisi funzionale e delle regole. Tuttavia, le regole messe in modalità test non influiscono sul blocco delle applicazioni. Il risultato del funzionamento da esse simulato viene registrato nel log delle attività (v. [Eventi di Controllo delle applicazioni](#)). La modalità test per le regole viene attivata e disattivata nella sezione delle impostazioni delle regole di permesso e divieto.

La tabella seguente mostra quali impostazioni definiscono una particolare modalità di funzionamento del profilo.

Modalità	Disattivato	Attivo	Test globale	Test per le regole
Impostazione				
Generali → Attiva profilo	–	+	+	+
Generali → Metti il profilo in modalità test globale	inattiva	–	+	–
<Modalità> → <Regola> → Attiva regola	inattiva	+/-	+/-	+
<Modalità> → <Regola> → Metti la regola in modalità test	inattiva	–	+/-	+

Segni convenzionali

+	l'impostazione deve essere attivata
–	l'impostazione deve essere disattivata
+/-	l'impostazione non ha importanza
inattiva	l'impostazione non è modificabile

7.4.1. Creazione e assegnazione di profili



Per creare un nuovo profilo

1. Selezionare la voce **Rete antivirus** nel menu principale del Pannello di controllo.
2. Nella finestra che si è aperta, nella barra degli strumenti selezionare la voce **+ Aggiungi oggetto della rete** → **+ Crea profilo**.



3. Nel pannello che si è aperto impostare il **Nome del profilo**. In seguito sarà possibile modificarlo, se necessario, nella sezione delle impostazioni [Generali](#).
4. Premere il pulsante **Salva**.
5. Il nuovo profilo verrà creato e inserito nel gruppo **Profiles**.

Per assegnare un profilo a un oggetto

1. Selezionare la voce **Rete antivirus** nel menu principale del Pannello di controllo.
2. Nella finestra che si è aperta, nella lista gerarchica selezionare il profilo che si vuole assegnare.
3. Nella barra degli strumenti premere  **Dati e configurazione** →  **Assegna profilo**.

Nella finestra che si è aperta selezionare un oggetto su cui propagare le impostazioni:

- Nella scheda **Active Directory** sono presentate liste analoghe alla lista nell'albero della rete antivirus, aggiornata tramite il task **Sincronizzazione con Active Directory** dal [calendario](#) del Server Dr.Web. Queste liste contengono oggetti identici, ma differiscono nel tipo di oggetti cui verrà assegnato il profilo:
 - Nella lista **Postazioni di Active Directory** è possibile selezionare gruppi di postazioni o singole postazioni registrate nel dominio Active Directory.
 - Nella lista **Utenti di Active Directory** è possibile selezionare gruppi di utenti e singoli utenti registrati nel dominio Active Directory.



Gli stessi oggetti non devono essere selezionati in liste diverse.



- Nella scheda **Rete antivirus** è possibile selezionare i seguenti oggetti:
 - Gruppi di postazioni. In questo caso le impostazioni verranno propagate su tutti gli account utente di tutte le postazioni incluse in questi gruppi.
 - Singole postazioni in gruppi. In questo caso le impostazioni verranno propagate su tutti gli account utente delle postazioni selezionate.
 - Criteri nel gruppo **Policies**. In questo caso le impostazioni verranno propagate su tutti gli account utente delle postazioni cui è assegnato il criterio selezionato.
- Nella scheda **Utenti locali** è possibile selezionare un gruppo di utenti o singoli utenti su postazioni. In questo caso le impostazioni verranno propagate solo sugli account utente selezionati su queste postazioni.

Per maggiori informazioni sulle priorità nell'assegnazione di profili v. sezione [Ereditarietà della configurazione della postazione](#).

4. Premere il pulsante **Salva**. Tutti gli oggetti selezionati verranno aggiunti alla lista a cui si applica il profilo che viene configurato (sono visualizzati nell'albero come oggetti nidificati di questo profilo).



Per interrompere la propagazione delle impostazioni del profilo su un oggetto

1. Selezionare la voce **Rete antivirus** nel menu principale del Pannello di controllo.
2. Nella finestra che si è aperta, nella lista gerarchica espandere la lista di oggetti nidificati del profilo e selezionare l'oggetto per cui si vuole annullare l'assegnazione del profilo.
3. Nella barra degli strumenti premere  **Generali** →  **Annulla l'assegnazione del profilo agli oggetti**.

7.4.2. Configurazione dei profili

Per modificare le impostazioni di un profilo

1. Selezionare la voce **Rete antivirus** nel menu principale del Pannello di controllo.
2. Aprire la sezione delle impostazioni di un profilo in uno dei seguenti modi:
 - a) Premere il nome di un profilo nella lista gerarchica della rete antivirus. Nella parte destra della finestra Pannello di controllo si apre automaticamente un pannello con le proprietà del profilo.
 - b) Premere l'icona di un profilo nell'albero della rete antivirus o selezionare un profilo e quindi selezionare la voce **Proprietà [del menu di gestione](#)**. Si apre una finestra con le proprietà del profilo.
3. Nella sezione **Generali** vengono impostati i principi di funzionamento del profilo:
 - Nel campo **Nome del profilo** può essere modificato il nome del profilo.
 - Spuntare il flag **Attiva profilo** per iniziare a utilizzare questo profilo.
 - Se è impostato il flag **Metti il profilo in modalità test globale**, solo il log delle attività verrà registrato come se le impostazioni fossero attivate. È possibile utilizzare questa modalità per mettere a punto il funzionamento del profilo.
 - Nella sezione [Analisi funzionale](#) impostare set di regole predefinite in base a cui l'avvio delle applicazioni verrà consentito o vietato.
4. Per applicare le impostazioni configurate nella sezione **Generali**, premere **Salva** nelle impostazioni del profilo.
5. Nella sezione **Modalità di permesso** è riportato un riassunto generale delle impostazioni della modalità: numero di regole di permesso creati e di gruppi di applicazioni affidabili assegnati a questo profilo. Per attivare o disattivare la modalità, nonché per configurare le regole e le applicazioni affidabili, premere sul link [Modalità di permesso](#) per passare alla sezione corrispondente.
6. Nella sezione **Modalità di divieto** è riportato un riassunto generale delle impostazioni della modalità: numero di regole di divieto creati. Per attivare o disattivare la modalità, nonché per configurare le regole, premere sul link [Modalità di divieto](#) per passare alla sezione corrispondente.



Prestare attenzione alle seguenti caratteristiche del funzionamento del profilo Controllo delle applicazioni:

- Se nessun criterio è attivato nella sezione **Criteri di analisi funzionale**, il profilo stesso sarà disattivato.
- Se quando vengono definite le impostazioni del profilo, non vengono definite le impostazioni avanzate per nessuno criterio nella sezione **Criteri di analisi funzionale**, e sono disattivate le modalità di divieto e di permesso, questa configurazione delle impostazioni non sarà salvata.
- Se non sono impostate né le regole di permesso né le applicazioni affidabili, la modalità di permesso sarà disattivata.
- Se non sono impostate regole di divieto, la modalità di divieto sarà disattivata.

7.4.2.1. Analisi funzionale

Analisi funzionale imposta un set di condizioni predefinite in base a cui l'avvio delle applicazioni viene consentito o vietato in base alle funzionalità eseguite.

Le impostazioni di analisi funzionale vengono modificate nella sezione delle [proprietà](#) del profilo **Generali** → **Criteri di analisi funzionale**.



Se nessun criterio è attivato nella sezione **Criteri di analisi funzionale**, il profilo stesso sarà disattivato.

Se nessuno dei criteri nella sezione **Criteri di analisi funzionale** ha impostazioni avanzate, e sono disattivate le modalità di divieto e di permesso, il profilo stesso sarà disattivato.

Per configurare l'analisi funzionale

1. Nella sezione **Criteri di analisi funzionale** impostare i flag per le categorie che si desidera utilizzare:
 - **Avvio di applicazioni,**
 - **Caricamento ed esecuzione di moduli,**
 - **Avvio di interpreti di script,**
 - **Caricamento dei driver,**
 - **Installazione di pacchetti MSI,**
 - **Integrità di file eseguibili.**




Se un profilo viene impostato per la prima volta, all'attivazione di ciascuno dei criteri le rispettive categorie di permesso vengono automaticamente attivate nelle impostazioni avanzate.



Questo strumento viene usato come misura di sicurezza per il caso se, dopo che vengono applicate le impostazioni delle modalità di permesso o di divieto, saranno bloccati oggetti del sistema operativo necessari per il funzionamento della postazione.

In seguito, se necessario, è possibile disattivare queste categorie di permesso nelle impostazioni avanzate.

2. Per configurare le impostazioni avanzate di un criterio selezionato, premere  **Modifica** di fronte al criterio. Si apre una finestra con la lista delle impostazioni.

Le impostazioni di analisi funzionale possono essere sia quelle che vietano e sia quelle che consentono l'avvio di applicazioni.

Spuntare i flag per le impostazioni da eseguire.

3. Se si attiva l'utilizzo di uno dei criteri, ma non si configurano le relative impostazioni avanzate, il controllo dell'avvio verrà eseguito per tutti gli oggetti in base a questo criterio in conformità alle impostazioni delle modalità di permesso o di divieto.

Per esempio:

- Se è impostato il criterio **Avvio di interpreti di script**, ma non sono configurate le sue impostazioni avanzate, verrà controllato l'avvio di tutti gli interpreti di script in conformità alle impostazioni configurate per le modalità di permesso o di divieto.
- Se è impostato il criterio **Avvio di interpreti di script** ed è configurata la sua impostazione avanzata **Proibisci l'avvio di script da supporti rimovibili**, sarà vietato solo l'avvio di script da supporti rimovibili.

4. Se si configurano le impostazioni avanzate, ma non si attiva l'uso del criterio stesso, non verranno eseguiti né le impostazioni avanzate né il criterio stesso.
5. Per salvare le impostazioni avanzate, premere **Salva** nella finestra con la lista delle impostazioni avanzate.
6. Per salvare le impostazioni di analisi funzionale, premere **Salva** nella finestra delle impostazioni del profilo.

7.4.2.2. Modalità di permesso

Modalità di permesso significa che su tutte le postazioni controllate è consentito solo l'avvio delle applicazioni dalla lista **Applicazioni affidabili** e/o delle applicazioni che corrispondono alle regole di permesso. Tutte le altre applicazioni vengono bloccate con la considerazione dei criteri dell'analisi funzionale.

La modalità di permesso può essere attivata persino nel caso in cui funzionano solo le regole di permesso. In questo caso la modalità di permesso funzionerà come aggiunta all'analisi funzionale permettendo di consentire l'avvio di singole applicazioni dalla lista di quelle vietate. Per esempio, se nei criteri di analisi funzionale è impostato il divieto di avvio di applicazioni da rete e risorse condivise, ma allo stesso tempo, nelle regole di permesso è impostato il permesso di avvio di un'applicazione specifica, questa applicazione verrà avviata, mentre viene mantenuto il blocco di altre applicazioni.



Le regole di permesso e le applicazioni affidabili vengono modificate nelle [proprietà](#) del profilo, scheda **Modalità di permesso**.

Per utilizzare la modalità di permesso

1. Spuntare il flag **Utilizza la modalità di permesso** nella scheda **Modalità di permesso**.
2. Configurare le impostazioni in almeno una delle sue sezioni:
 - [Regole di permesso](#).
 - [Applicazioni affidabili](#).
3. Premere **Salva**.



Se non sono impostate né le regole di permesso né le applicazioni affidabili, la modalità di permesso sarà disattivata.

Regole di permesso

Le regole di permesso vengono modificate nella sezione delle [proprietà](#) del profilo **Modalità di permesso** → **Regole di permesso**.

Per creare una nuova regola di permesso

1. Nella sezione **Regole di permesso** nella barra degli strumenti premere il pulsante **+ Crea regola**.
2. Nella finestra **Aggiunta della regola** impostare il **Nome della regola** e premere **Salva**.
3. Dalla lista delle regole selezionare la regola creata e configurarne le impostazioni nel pannello delle proprietà che si è aperto:
 - a) Spuntare il flag **Attiva regola** per iniziare a utilizzare questa regola.
 - b) Se si vuole testare la regola, spuntare il flag **Metti la regola in modalità test**. Le applicazioni non verranno controllate sulle postazioni, tuttavia, la registrazione del log delle attività verrà eseguita come con le impostazioni attivate. I risultati degli avvisi e dei blocchi delle applicazioni in modalità test di funzionamento della regola verranno visualizzati nella sezione [Eventi di Controllo delle applicazioni](#).
Se il flag **Metti la regola in modalità test** è deselezionato, la regola funzionerà in modalità attiva in cui le applicazioni sulle postazioni vengono avviate in base alle impostazioni della regola specificate (vedi inoltre [modalità di funzionamento dei profili](#)).
 - c) Nella sezione **Consenti l'avvio di applicazioni secondo i seguenti criteri** selezionare le opzioni in base alle quali sarà consentito l'avvio di applicazioni sulle postazioni. Nel campo **Nome del file** indicare il nome del file o la directory.
Sono supportate le variabili di ambiente e le maschere. È possibile:
 - Indicare un file o una cartella.



- per indicare una cartella o un file specifico al suo interno, inserire il percorso completo del file o della cartella nel campo di input.
- per aggiungere un file con un nome specifico, inserire il nome del file inclusa l'estensione nel campo di input. Se il percorso non è impostato, il parametro verrà interpretato come file con il nome indicato indipendentemente dalla posizione.
 - `C:\folder\file.exe` — aggiunge ai consentiti il file `file.exe` nella cartella `C:\folder`.
 - `C:\folder` — aggiunge ai consentiti tutte le sottocartelle e i file nella cartella `C:\folder`.
 - `file.exe` — aggiunge ai consentiti tutti i file con il nome `file` e l'estensione `.exe` in tutte le cartelle.
 - `file` — aggiunge ai consentiti tutti i file con il nome `file` senza estensione in tutte le cartelle.
- Utilizzare una maschera che imposta la parte generale del nome di un oggetto, in particolare:
 - il carattere "*" sostituisce qualsiasi sequenza di caratteri, anche una vuota;
 - il carattere "?" sostituisce qualsiasi carattere, ma uno solo.
 - `C:\Program Files\folder*.exe` — aggiunge alle consentite le applicazioni nella cartella `C:\Program Files\folder`.
 - `C:\Program Files**.exe` — aggiunge alle consentite le applicazioni solo nelle sottocartelle di primo livello di nidificazione della cartella `C:\Program Files`.
 - `C:\Program Files***.exe` — aggiunge alle consentite le applicazioni nelle sottocartelle di qualsiasi livello di nidificazione della cartella `C:\Program Files`.
 - `C:\Program Files\folder\exam*.exe` — aggiunge alle consentite qualsiasi applicazione nella cartella `C:\Program Files\folder`, di cui il nome inizi con `exam`.
 - `example.exe` — aggiunge alle consentite tutte le applicazioni con il nome `example` e l'estensione `.exe` in tutte le cartelle.
 - `example*` — aggiunge alle consentite le applicazioni di qualsiasi tipo, di cui i nomi iniziano con `example`, in tutte le cartelle.
 - `example.*` — aggiunge alle consentite tutte le applicazioni con il nome `example` e qualsiasi estensione in tutte le cartelle.
- Impostare un'applicazione consentita per l'avvio in base al nome di una variabile, se nelle impostazioni delle variabili di sistema sono definiti il nome e il valore di questa variabile.
 - `%EXAMPLE_PATH%\example.exe` — imposta un'applicazione in base al nome di una variabile di sistema. Il nome e il valore della variabile di sistema possono essere definiti nelle impostazioni del sistema operativo (in caso di sistema operativo Windows: **Pannello di controllo** → **Sistema** → **Impostazioni di sistema avanzate** → **Avanzate** → **Variabili d'ambiente** → **Variabili di sistema**).



Il nome della variabile nell'esempio: `EXAMPLE_PATH`.


Il valore della variabile nell'esempio: `C:\Program Files\folder`.




È inoltre possibile creare regole di permesso dalle sezioni [Eventi di Controllo delle applicazioni](#) e [Prontuario applicazioni](#) in base ai dati ottenuti dalle postazioni. In questo caso i parametri applicazione nelle impostazioni della regola verranno automaticamente compilati in base all'applicazione selezionata.

4. Premere **Salva**.

Per creare un duplicato di una regola di permesso

1. Nella sezione **Regole di permesso** nella tabella delle regole selezionare la regola che si vuole duplicare per questo profilo.
2. Nella barra degli strumenti premere il pulsante  **Duplica regola**.
3. Nella tabella delle regole apparirà una nuova regola le cui impostazioni verranno completamente copiate dalla regola selezionata nel passaggio 1. Al nome della regola verrà aggiunta la cifra **1**.

Per rimuovere una regola di permesso

1. Nella sezione **Regole di permesso** nella tabella delle regole selezionare la regola che si vuole rimuovere dal profilo.
2. Nella barra degli strumenti premere il pulsante  **Rimuovi regola**.

Applicazioni affidabili

Per utilizzare le applicazioni affidabili, eseguire una delle seguenti azioni:

- Se la raccolta delle applicazioni affidabili verrà effettuata sul Server Dr.Web corrente (v. inoltre [Applicazioni affidabili](#)), attivare la raccolta delle applicazioni affidabili nella sezione del Pannello di controllo **Amministrazione** → **Controllo delle applicazioni** → **Applicazioni affidabili**.
- Se le applicazioni affidabili verranno trasmesse sul Server Dr.Web corrente attraverso la comunicazione tra i server da un Server Dr.Web adiacente, configurare le [impostazioni corrispondenti](#) nei repository dei Server Dr.Web che inviano e ricevono il prodotto **Applicazioni affidabili**.

Le applicazioni affidabili per un profilo specifico vengono modificate nella sezione delle [proprietà](#) del profilo **Modalità di permesso** → **Applicazioni affidabili**.

La tabella della sezione contiene la lista di tutti i gruppi di applicazioni affidabili assegnati per in questo profilo.



Gruppo di applicazioni affidabili (o white list di applicazioni) è una lista di applicazioni raccolte in base a criteri specificati da una postazione selezionata o un gruppo di postazioni. L'avvio di queste applicazioni è consentito sulle postazioni della rete antivirus a cui è assegnato questo profilo nel caso di funzionamento in modalità di permesso.



Se il Server Dr.Web corrente riceve le applicazioni affidabili attraverso la comunicazione tra i server da un Server Dr.Web adiacente (v. [Applicazioni affidabili](#)), la tabella dei gruppi può contenere record con l'icona **Gruppo di applicazioni affidabili non è presente nel repository del Server**. Questi record indicano i gruppi di applicazioni provenienti da una revisione precedente del prodotto **Applicazioni affidabili**, dopo di che è stata ricevuta una nuova revisione in cui questo gruppo non è incluso. In tal caso, le applicazioni possono continuare a essere operative sulle postazioni corrispondenti, ma per evitare errori di funzionamento del profilo, si consiglia di [rimuovere](#) tali gruppi dalle sue impostazioni.

Per aggiungere un gruppo di applicazioni affidabili al profilo

1. Nella sezione **Applicazioni affidabili** nella barra degli strumenti premere il pulsante **Aggiungi il gruppo di applicazioni affidabili al profilo**.
2. Si apre una finestra con la lista di tutti i gruppi di applicazioni affidabili.



Quando viene configurata la modalità di permesso, i gruppi di applicazioni affidabili vengono selezionati dalla lista dei gruppi disponibili nel [repository](#) per il prodotto **Applicazioni affidabili**.

3. Spuntare i flag di fronte ai gruppi di applicazioni che si desidera aggiungere al profilo.
4. Premere **Salva**.

Per rimuovere un gruppo di applicazioni affidabili dal profilo

1. Nella sezione **Applicazioni affidabili** nella tabella spuntare i flag di fronte ai gruppi che si desidera rimuovere dal profilo.
2. Nella barra degli strumenti premere il pulsante **Rimuovi il gruppo di applicazioni affidabili**.
3. Le applicazioni di questo gruppo verranno rimosse dalla lista di quelle il cui avvio è consentito sulle postazioni cui è assegnato questo profilo.



Alla rimozione dal profilo il gruppo stesso di applicazioni affidabili non viene rimosso. Il gruppo rimane disponibile nel repository e può essere aggiunto sia a questo che ad altri profili.



7.4.2.3. Modalità di divieto

Modalità di divieto significa che su tutte le postazioni controllate è vietato l'avvio solo delle applicazioni che corrispondono alle regole di divieto. Tutte le altre applicazioni vengono consentite.

Le regole di divieto vengono modificate nelle [proprietà](#) del profilo, scheda **Modalità di divieto**.

Per utilizzare la modalità di divieto

1. Spuntare il flag **Utilizza la modalità di divieto** nella scheda **Modalità di divieto**.
2. Creare regole di divieto come descritto [di seguito](#).
3. Premere **Salva**.



Se non sono impostate regole di divieto, la modalità di divieto sarà disattivata.

Per creare una nuova regola di divieto

1. Nella sezione **Regole di divieto** nella barra degli strumenti premere il pulsante **+ Crea regola**.
2. Nella finestra **Aggiunta della regola** impostare il **Nome della regola** e premere **Salva**.
3. Dalla lista delle regole selezionare la regola creata e configurarne le impostazioni nel pannello delle proprietà che si è aperto:
 - a) Spuntare il flag **Attiva regola** per iniziare a utilizzare questa regola.
 - b) Se si vuole testare la regola, spuntare il flag **Metti la regola in modalità test**. Le applicazioni non verranno controllate sulle postazioni, tuttavia, la registrazione del log delle attività verrà eseguita come con le impostazioni attivate. I risultati degli avvisi e dei blocchi delle applicazioni in modalità test di funzionamento della regola verranno visualizzati nella sezione [Eventi di Controllo delle applicazioni](#).
Se il flag **Metti la regola in modalità test** è deselezionato, la regola funzionerà in modalità attiva in cui le applicazioni sulle postazioni vengono bloccate in base alle impostazioni della regola specificate (vedi inoltre [modalità di funzionamento dei profili](#)).
 - c) Nella sezione **Proibisci l'avvio di applicazioni secondo i seguenti criteri** selezionare le opzioni in base alle quali sarà vietato l'avvio di applicazioni sulle postazioni.




Nel campo **Nome del file** indicare un nome di file o una directory. Sono supportate le variabili di ambiente e le maschere. Se il percorso non è impostato, il parametro verrà interpretato come file con il nome indicato indipendentemente dalla posizione. Una descrizione più dettagliata è riportata in sezione [Modalità di permesso](#).




È inoltre possibile creare regole di divieto dalle sezioni [Eventi di Controllo delle applicazioni](#) e [Prontuario applicazioni](#) in base ai dati ottenuti dalle postazioni. In questo caso i parametri applicazione nelle impostazioni della regola verranno automaticamente compilati in base all'applicazione selezionata.

4. Premere **Salva**.

Per creare un duplicato di una regola di divieto

1. Nella sezione **Regole di divieto** nella tabella delle regole selezionare la regola che si vuole duplicare per questo profilo.
2. Nella barra degli strumenti premere il pulsante  **Duplica regola**.
3. Nella tabella delle regole apparirà una nuova regola le cui impostazioni verranno completamente copiate dalla regola selezionata nel passaggio 1. Al nome della regola verrà aggiunta la cifra **1**.

Per rimuovere una regola di divieto

1. Nella sezione **Regole di divieto** nella tabella delle regole selezionare la regola che si vuole rimuovere dal profilo.
2. Nella barra degli strumenti premere il pulsante  **Rimuovi regola**.



Capitolo 8: Gestione delle postazioni

La rete antivirus gestita tramite Dr.Web Enterprise Security Suite consente di configurare in maniera centralizzata i pacchetti antivirus sulle 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 persino quando la postazione non è disponibile per il Server Dr.Web. Queste modifiche verranno accettate dalla postazione non appena si riconnetterà al Server Dr.Web.

8.1. Gestione degli account di postazioni

8.1.1. 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 un nuovo account di postazione](#).

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

1. Se durante l'installazione di Agent Dr.Web su postazione, il flag **Autenticazione manuale sul server** era deselezionato, la modalità di accesso delle postazioni al Server Dr.Web viene determinata in base alle impostazioni definite sul Server Dr.Web (si usa di default), v. [sotto](#).
2. Se durante l'installazione di Agent Dr.Web 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 Dr.Web, viene autenticata automaticamente a prescindere dalle impostazioni del Server Dr.Web (si usa di default nell'installazione di Agent Dr.Web mediante il pacchetto di installazione `drweb_es_<SO>_<postazione>.exe` — v. **Guida all'installazione**, p. [File di installazione](#)).



La configurazione del tipo di autenticazione di Agent Dr.Web durante l'installazione è descritta in **Manuale dell'utente**.



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

1. Aprire le impostazioni di Server Dr.Web. 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 **Modalità di registrazione dei nuovi arrivi** selezionare uno dei seguenti valori:
 - **Conferma l'accesso manualmente** (modalità predefinita, se non modificata durante l'installazione del Server Dr.Web),
 - **Sempre nega l'accesso,**
 - **Consenti l'accesso automaticamente.**

Conferma manuale dell'accesso

In modalità **Conferma l'accesso manualmente** le nuove postazioni vengono inserite nel sottogruppo di sistema **Newbies** del gruppo **Status** e ci restano fino a quando non verranno considerate dall'amministratore.





Per modificare la modalità di accesso delle postazioni non confermate

1. Selezionare la voce **Rete antivirus** nel menu principale del Pannello di controllo. Selezionare postazioni nell'albero di rete antivirus nel gruppo **Status** → **Newbies**.



Il gruppo **Status** → **Newbies** è disponibile nell'albero di rete antivirus soltanto se sono soddisfatte le seguenti condizioni:

1. Nella sezione **Amministrazione** → **Configurazione del Server Dr.Web** → **Generali** per il parametro **Modalità di registrazione dei nuovi arrivi** è impostato il valore **Conferma l'accesso manualmente**.
2. All'amministratore è concesso il [permesso Approvazione dei nuovi arrivi](#).

2. Per configurare l'accesso al Server Dr.Web, nella barra degli strumenti nella sezione  **Postazioni non confermate** impostare l'azione che verrà applicata alle postazioni selezionate:
 -  **Consenti l'accesso delle postazioni selezionate e assegna gruppo primario** — per confermare l'accesso della postazione al Server Dr.Web e assegnarle un gruppo primario dalla lista proposta.
 -  **Annulla l'azione impostata per l'esecuzione al momento della connessione** — per annullare l'azione sulla postazione non confermata, che è stata precedentemente impostata per l'esecuzione al momento della connessione della postazione al Server Dr.Web.
 -  **Nega l'accesso delle postazioni selezionate** — per negare l'accesso della postazione al Server Dr.Web.



Negazione di accesso automatica

In modalità **Sempre nega l'accesso** il Server Dr.Web nega l'accesso quando riceve richieste da nuove postazioni. L'amministratore deve creare gli account di postazioni manualmente e assegnare loro le password di accesso.



Consenti l'accesso automaticamente

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

8.1.2. Rimozione e recupero della postazione

Rimozione di postazioni

Per rimuovere l'account di una postazione

1. Selezionare la voce del menu principale **Rete antivirus**.
2. Nella finestra che si è aperta, nella lista gerarchica selezionare una o più postazioni che si vuole rimuovere.
3. Nella barra degli strumenti premere  **Generali** →  **Rimuovi gli oggetti selezionati**.
4. 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 vuole 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** è possibile modificare l'elenco dei gruppi di cui farà parte la postazione. 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 può essere inclusa 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 **Ripristina**.

8.1.3. 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 rimuovere i nomi di postazioni duplicati

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



8.2. Impostazioni generali della postazione

8.2.1. Proprietà della postazione

Per visualizzare e 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 il nome della postazione nella lista gerarchica della rete antivirus. Nella parte destra della finestra del Pannello di controllo si apre automaticamente una sezione con le proprietà della postazione.
 - b) Selezionare la voce **Proprietà [del menu di gestione](#)**. Si apre la finestra con le proprietà della postazione.
3. 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**.

Per rimuovere 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 impostazioni individuali**. Si apre l'elenco delle impostazioni di questa postazione, le impostazioni individuali sono contrassegnate con dei flag.
2. Lasciare le spunte ai flag accanto alle impostazioni individuali che si vuole rimuovere. Togliere le spunte ai flag accanto alle impostazioni che si vuole lasciare individuali. Premere **Rimuovi**. Per le impostazioni contrassegnate con i flag verrà ripristinata l'ereditarietà dal gruppo primario.

8.2.1.1. Generali

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

- **Identificatore della postazione** — identificatore della postazione univoco. Viene impostato durante la creazione dell'account postazione e in seguito non può essere modificato.
- **Nome** — nome della postazione. Viene impostato durante la creazione dell'account postazione e verrà automaticamente sostituito con il nome del computer dopo la connessione dell'Agent Dr.Web.
- **Data di creazione** — data di creazione dell'account postazione sul Server Dr.Web.



- **Identificatore di sicurezza** — identificatore di sicurezza univoco (SID — security identifier) di un account utente di Windows. Il campo viene compilato automaticamente dopo la connessione al Server Dr.Web di una postazione con il sistema operativo Windows.
- **LDAP DN** — nome distinto (distinguished name) di una postazione con il sistema operativo Windows. Viene utilizzato per le postazioni che rientrano in un dominio ADS/LDAP. Il campo viene compilato automaticamente dopo la connessione della postazione al Server Dr.Web.
- **Indirizzo MAC** — indirizzo MAC della postazione. Il campo viene compilato automaticamente dopo la connessione della postazione al Server Dr.Web.
- **Data del primo download di Agent Dr.Web** — data del primo download del pacchetto di installazione di Agent Dr.Web attraverso il link dalla voce **File di installazione** (v. sotto).
- **Data dell'ultima connessione** — data dell'ultima connessione di questa postazione al Server Dr.Web.
- **Indirizzo di rete** — indirizzo di rete della postazione.
- **Numero di build del sistema operativo** — numero di build del sistema operativo Windows installato 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 Dr.Web (è necessario ripetere la stessa password nel campo **Confermare la password**). Affinché l'Agent Dr.Web possa connettersi nel caso di cambio della password, una procedura analoga deve essere eseguita nelle impostazioni di connessione dell'Agent Dr.Web sulla postazione.
- Nei campi **Inizio del periodo di blocco** e **Fine del periodo di blocco** indicare un periodo (da una data e a una data) durante cui la postazione verrà bloccata sul Server Dr.Web. I campi sono progettati per una sospensione temporanea dell'accesso della postazione al Server Dr.Web. In caso di indicazione di un valore solo nel campo **Inizio del periodo di blocco** la postazione verrà bloccata a tempo indeterminato a partire dalla data impostata.
- Nel campo **Descrizione** si possono inserire le informazioni supplementari circa la postazione.



I valori dei campi contrassegnati con il carattere * sono da impostare.







Inoltre, in questa sezione sono riportati i seguenti link:

- Nella voce **File di installazione** — un link per il download del pacchetto di installazione di Agent Dr.Web per questa postazione.
Nel periodo tra la creazione della postazione e il momento quando verrà impostato il suo sistema operativo, vengono forniti i link per il download dei pacchetti per tutti i sistemi operativi supportati da Dr.Web Enterprise Security Suite.
- Nella voce **File di configurazione** — un link per il download del file con le impostazioni di connessione al Server Dr.Web per le postazioni con Android, macOS e SO Linux.




8.2.1.2. 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	Chiavi di licenza
	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 impostazioni individuali**, le impostazioni dell'altro componente anche verranno rimosse (viene impostata l'ereditarietà delle impostazioni dal gruppo padre).

8.2.1.3. 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 configurare l'appartenenza di una postazione

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**.



8.2.1.4. Sicurezza

Nella sezione **Sicurezza** vengono impostate limitazioni agli indirizzi di rete da cui l'Agent Dr.Web installato su questa postazione può accedere al Server Dr.Web.

Per impostare le limitazioni di accesso

1. Spuntare il flag **Usa questa lista di controllo di accesso** per impostare liste di indirizzi consentiti o proibiti. Se il flag è deselezionato, tutte le connessioni saranno consentite.
2. Per consentire l'accesso da un determinato indirizzo TCP, includerlo nella lista **TCP: consentito** o **TCPv6: consentito**.
3. Per proibire un indirizzo TCP, includerlo nella lista **TCP: negato** o **TCPv6: negato**.
4. 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**.

Per modificare una lista di indirizzi:

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**.



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 indica reti con una maschera: 255.255.255.0
Contiene 254 indirizzi.
Gli indirizzi di host in queste reti sono di tipo: 195.136.12.*
2. Il prefisso 8 indica reti con una maschera 255.0.0.0



Contiene fino a 16777214 indirizzi (256*256*256-2).

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


8.2.1.5. Server proxy

Nella sezione **Server proxy** vengono configurate le impostazioni del Server proxy Dr.Web installato su questa postazione.



Informazioni dettagliate sull'installazione del Server proxy e sulla connessione al Server Dr.Web sono riportate nella **Guida all'installazione**, p. [Installazione del Server proxy](#).

Se il Server proxy è installato sulla postazione:

1. Nel campo **Identificatore** viene riportato l'identificatore dell'account di Server proxy creato nel Pannello di controllo. Una volta che un account è stato creato, l'identificatore non può essere modificato.
2. Nel campo **Nome** è possibile modificare il nome dell'account di Server proxy creato nel Pannello di controllo.
3. Nei campi **Password** e **Confermare la password** è possibile modificare la password dell'account di Server proxy creato nel Pannello di controllo. La password viene utilizzata per la connessione del Server proxy al Server Dr.Web. Se la password è stata cambiata nel Pannello di controllo, è necessario assicurarsi che la password nelle impostazioni di connessione sul Server proxy coincida con la password modificata nel Pannello di controllo. Se le password non coincidono, il Server proxy non potrà connettersi al Server Dr.Web per la gestione della configurazione in remoto attraverso il Pannello di controllo.
4. Nella sezione **Appartenenza** viene impostato il gruppo in cui è incluso il Server proxy. Per modificare il gruppo, spuntare il flag di fronte al gruppo richiesto nella lista riportata. Un Server proxy può rientrare in solo un gruppo. È possibile selezionare il gruppo predefinito **Proxies** e i relativi sottogruppi.
5. È possibile rimuovere il Server proxy associato all'Agent Dr.Web sulla postazione che viene modificata. Per farlo, premere  **Rimuovi Server proxy**. Dopo che si fa clic su **Salva**, il Server proxy verrà disinstallato dalla postazione. L'account del Server proxy verrà rimosso dal Server Dr.Web.

Se il Server proxy non è installato sulla postazione:

1. Se si vuole installare il Server proxy sulla postazione selezionata, spuntare il flag **Crea un Server proxy associato** ed impostare i parametri del Server proxy che viene creato. I parametri sono analoghi ai parametri di creazione del Server proxy.
2. Dopo che si fa clic su **Salva**, verrà creato un account di Server proxy nel Pannello di controllo. Dopo la trasmissione delle impostazioni sulla postazione il Server proxy verrà installato su questa postazione in modalità background. L'Agent Dr.Web si conatterà al



Server Dr.Web solo attraverso il Server proxy installato. L'uso del Server proxy sarà trasparente per l'utente.

8.2.1.6. 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 OpenStreetMap 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**.



Per le postazioni con SO Android è possibile configurare il rilevamento automatico della posizione.

Informazioni dettagliate sull'utilizzo e sulla configurazione di questa funzionalità sono ritrovabili nel documento **Allegati**, nella sezione [Rilevamento automatico della posizione di una postazione con SO Android](#).

8.2.2. Componenti di protezione

Componenti

Per scoprire quali componenti del pacchetto antivirus sono installati su una postazione e inoltre per avviare o arrestare il funzionamento dei componenti

1. Selezionare la voce **Rete antivirus** nel menu principale del Pannello di controllo, nella finestra che si è aperta nella lista gerarchica fare clic sul nome di una postazione o di un gruppo.
2. Dal [menu di gestione](#) che si è aperto selezionare dalla sottosezione **Generali** la voce **Componenti di protezione**.
3. Si apre una finestra con informazioni sui componenti installati sulle postazioni selezionate.



L'elenco dei componenti installati dipende da:

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

4. Se necessario, è possibile modificare lo stato di funzionamento dei componenti direttamente dal Pannello di controllo. Per farlo, spuntare i flag per i componenti di cui lo stato di funzionamento si vuole modificare e premere il pulsante corrispondente nella barra degli strumenti:

- — arresta il funzionamento dei componenti selezionati sulle postazioni.
- — avvia i componenti selezionati sulle postazioni.



Quando viene arrestato il funzionamento dei componenti, le scansioni in corso vengono interrotte, Scanner viene arrestato, il funzionamento dei monitor in esecuzione viene sospeso.

Inoltre, è possibile arrestare il funzionamento dei componenti a seconda del tipo di avvio, come viene descritto nella sezione [Interruzione di componenti in esecuzione per tipo](#).

5. Se necessario, è possibile esportare in file i dati sullo stato di funzionamento dei componenti delle postazioni. Per farlo, premere uno dei seguenti pulsanti 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.

Database dei virus

Per scoprire quali database dei virus sono installati su una postazione

1. Selezionare la voce **Rete antivirus** nel menu principale del Pannello di controllo, nella finestra che si è aperta nella lista gerarchica fare clic sul nome di una postazione.
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 delle postazioni** e **Stato dei database dei virus**, dopodiché riavviare il Server Dr.Web.

La voce **Database dei virus** è disponibile soltanto se vengono selezionate singole postazioni.

8.2.3. Hardware e software sulle postazioni SO Windows

Dr.Web Enterprise Security Suite consente di accumulare e di visualizzare informazioni circa gli hardware e i software delle postazioni SO Windows protette.







Per raccogliere informazioni sugli hardware e sui software delle postazioni

1. Attivare la raccolta delle statistiche sul Server Dr.Web:
 - 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 di Server Dr.Web aprire la scheda **Statistiche** e spuntare il flag **Elenco di hardware e software**, se la spunta è tolta.
 - d) Per accettare le modifiche apportate, premere **Salva** e riavviare il Server Dr.Web.
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 di Agent Dr.Web nella scheda **Generali** spuntare il flag **Raccogli le informazioni sulle postazioni**, se è deselezionato. Se in precedenza la raccolta delle statistiche non è stata consentita nelle impostazioni di Server Dr.Web, questa impostazione non sarà disponibile. 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'elenco hardware e software su una o più postazioni

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



2. Nella lista gerarchica della rete antivirus selezionare una postazione o un gruppo di postazioni.
3. Nel menu di gestione, nella sezione **Generali** selezionare la voce **Hardware e software**.
4. La tabella contiene le seguenti schede di informazioni sugli hardware e sui software delle postazioni selezionate:
 - **Hardware** — elenco dei componenti hardware installati sulle postazioni.
 - **Programmi** — elenco dei prodotti software installati sulle postazioni.
 - **Aggiornamenti di Windows** — elenco dei pacchetti di aggiornamento di SO Windows installati sulle postazioni.
5. La colonna **Postazione** in ciascuna delle schede contiene il nome della postazione per cui sono riportate le informazioni.
6. Per modificare la visualizzazione dei dati nella tabella:
 - Attraverso l'icona  selezionare quali colonne verranno visualizzate nella tabella.
 - Attraverso l'icona  impostare una stringa arbitraria per la ricerca in tutte le sezioni della tabella.
7. Se necessario, è possibile esportare in file i dati sugli hardware e sui software di una postazione. Per farlo, premere uno dei seguenti pulsanti 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.**

8.3. Configurazione delle impostazioni della postazione



8.3.1. Permessi dell'utente della postazione

Per configurare i permessi degli utenti della 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, macOS, Linux e Android vengono modificati nelle seguenti sottosezioni:
 - **Componenti** — configurazione dei permessi per la gestione dei componenti antivirus. Di default, l'utente ha i permessi per avviare ciascun componente, ma gli è vietato modificare la configurazione dei componenti e arrestarli.



- **Generali** — configurazione nei permessi per la gestione dell'Agent Dr.Web e delle sue funzionalità:

Flag della sezione Permessi	Azione del flag	Il risultato sulla postazione se il flag è deselezionato
Postazioni SO Windows		
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 Dr.Web, nella sezione Generali non sono disponibili le impostazioni delle seguenti sottosezioni: <ul style="list-style-type: none">• Avvisi: tutte le impostazioni non sono disponibili.• Server: non sono disponibili le impostazioni di connessione al Server Dr.Web, il flag Sincronizza l'ora del sistema con l'ora del server e l'impostazione Utilizza Modalità mobile, se non è disponibile la connessione al 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.
Disattivazione dell'auto-protezione	Spuntare il flag per permettere agli utenti su postazione di arrestare l'auto-protezione.	Nelle impostazioni di Agent Dr.Web, nella sezione Principali → Autoprotezione non è disponibile l'impostazione Attiva l'autoprotezione e l'impostazione Attiva il supporto di virtualizzazione hardware .
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 Dr.Web su postazione sia tramite l'installer che tramite i mezzi standard di SO Windows. In questo caso, la rimozione dell'Agent Dr.Web è possibile solo tramite la voce  Generali →  Disinstalla Agent Dr.Web nella barra degli strumenti del Pannello di controllo.
Postazioni macOS		
Avvio in modalità mobile	Spuntare il flag per permettere agli utenti su postazione di passare alla modalità mobile e di ricevere aggiornamenti direttamente	Nella finestra principale dell'applicazione la sezione Aggiornamento non è disponibile.



Flag della sezione Permessi	Azione del flag	Il risultato sulla postazione se il flag è deselezionato
	dal Sistema d'aggiornamento mondiale Dr.Web se non è disponibile una connessione con il Server Dr.Web.	
Postazioni SO famiglia Linux		
Avvio in 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 in 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, avviata su un dispositivo mobile, la sezione Aggiornamento non è disponibile.



Quando viene disattivata una delle voci responsabili della modifica della configurazione di Agent Dr.Web, verrà utilizzato il valore definito per questa impostazione l'ultima volta prima della disattivazione.

Le azioni eseguite dalle relative voci del menu sono descritte in **Manuale dell'utente** dei prodotti Dr.Web per il sistema operativo corrispondente.

- È possibile inoltre propagare queste impostazioni su un altro oggetto, premendo il pulsante **Propaga queste impostazioni verso un altro oggetto.**
- Per esportare queste impostazioni in file, fare clic su **Esporta impostazioni da questa sezione in file.**
- Per importare queste impostazioni da file, fare clic su **Importa impostazioni in questa sezione da file.**
- Per accettare le modifiche fatte, premere il pulsante **Salva.**



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

8.3.2. Calendario dei task della postazione

Dr.Web Enterprise Security Suite fornisce la possibilità di avere un *calendario dei task centralizzato* che viene creato dall'amministratore della rete antivirus e che rispetta tutte le regole di ereditarietà delle configurazioni.

Calendario dei task — un elenco delle attività 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 di Scanner. Inoltre, 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 postazioni e gruppi specifici viene modificato tramite il Pannello di controllo della sicurezza Dr.Web.



Agli utenti sulla postazione non è disponibile la possibilità di visualizzare e modificare i task del calendario centralizzato.

Di default per le postazioni con SO Windows il calendario contiene il task Daily scan — scansione di postazione giornaliera.


I risultati di esecuzione dei task del calendario centralizzato non vengono registrati nei dati statistici sul lato Agent Dr.Web, ma vengono inviati al Server Dr.Web e conservati nei dati statistici del Server Dr.Web.

Per modificare un calendario centralizzato


1. Selezionare la voce **Rete antivirus** nel menu principale del Pannello di controllo, nella finestra che si è aperta nella lista gerarchica fare clic sul nome di una postazione o di un gruppo. Nel [menu di gestione](#) che si è aperto selezionare la voce **Scheduler**. Si apre una lista dei task per le postazioni.



La maggior parte degli strumenti di questa sezione non sarà disponibile se per la postazione o il gruppo selezionato è impostata l'ereditarietà delle impostazioni dal gruppo padre. Se necessario, tramite i seguenti elementi nella barra degli strumenti è possibile modificare le impostazioni di ereditarietà nei limiti del calendario dei task:


 **Imposta l'ereditarietà delle impostazioni dal criterio o dal gruppo primario** — per eliminare le impostazioni individuali del calendario dei task e impostare l'ereditarietà delle impostazioni di questa sezione dal gruppo padre.



 **Copia le impostazioni dal criterio o dal gruppo primario e impostale come individuali** — per copiare le impostazioni del calendario dei task dal gruppo padre e assegnarle alle postazioni selezionate. In questo caso, l'ereditarietà verrà interrotta, e tutte le ulteriori modifiche al calendario dei task saranno considerate individuali.


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.

 **Crea task** — per aggiungere un nuovo task. Questa azione viene descritta in dettaglio qui sotto nella sottosezione [Editor dei task](#).

 **Propaga queste impostazioni verso un altro oggetto** — per copiare i task dal calendario in altri oggetti — postazioni o gruppi. Per maggiori informazioni v. sezione [Copiatura delle impostazioni in altri gruppi/postazioni](#).



 **Esporta impostazioni da questa sezione in file** — per esportare il calendario in un file di formato specifico.

 **Importa impostazioni in questa sezione da file** — per importare il calendario da un file di formato specifico.











Non è possibile importare una lista dei task del Server Dr.Web nello Scheduler dei task delle postazioni e viceversa.

b) Per gestire i task esistenti, spuntare i flag di fronte ai task richiesti o nell'intestazione della tabella per selezionare tutti i task nella lista. A condizione che l'ereditarietà delle impostazioni del calendario dei task dal gruppo padre non sia impostata per il gruppo o la postazione selezionata, saranno disponibili i seguenti elementi della barra degli strumenti per la gestione dei task selezionati:

Impostazione		Azione
 Tipo di avvio	Sincrono	Imposta il tipo di avvio sincrono di tutti i task contrassegnati sotto. Un task con una periodicità impostata verrà collocato nella coda generale dei task di Scheduler eseguiti in sequenza.
	Asincrono	Imposta il tipo di avvio asincrono di tutti i task contrassegnati sotto. Un task con una periodicità impostata verrà eseguito in modo parallelo ad altri task, fuori coda.
 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.



Impostazione	Azione
 L'impostazione simile viene definita nell'editor del task nella scheda Generali tramite il flag Permetti l'esecuzione .	
 Gravità	Rendi critico Eeguire 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 non critico Eeguire il task solo nell'ora programmata, indipendentemente dall'omissione o dall'esecuzione del task.
 L'impostazione simile viene definita nell'editor del task nella scheda Generali tramite il 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 (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.
 Esegui task	Eeguire immediatamente i task selezionati nella lista. In tale caso il task verrà avviato anche se esso è vietato per l'esecuzione secondo il calendario.
 Modifica task	Modificare i parametri del task. Si apre la finestra Editor dei task descritta sotto .



Se non si ha bisogno del calendario ereditato dal gruppo padre, è necessario disattivare l'ereditarietà per la postazione e lasciare almeno un task disattivandolo.

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 il nome della postazione nella lista gerarchica della rete antivirus. Nella parte destra della finestra del Pannello di controllo si apre automaticamente una sezione con le proprietà della postazione.
 - b) Selezionare la voce **Proprietà** del menu di gestione. Si apre la finestra con le proprietà della postazione.



3. Nella sezione con le proprietà della postazione selezionare la voce **Configurazione - > Scheduler**.
4. Premere l'icona **Copia le impostazioni dal criterio o dal gruppo primario e impostale come individuali** e confermare l'azione selezionata.
5. Lasciare almeno un task e disattivarne l'esecuzione premendo l'icona **Stato -> Proibisci l'esecuzione**.

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 campi nell'interfaccia contrassegnati con il carattere * devono essere obbligatoriamente compilati.

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.
- Spuntare il flag **Permetti l'esecuzione** per attivare l'esecuzione del task. Se il flag non è selezionato, il task sarà presente nella lista ma non verrà eseguito.



L'impostazione simile viene definita nella finestra principale di Scheduler tramite l'elemento della barra degli strumenti **Stato**.

- Spuntare il flag **Task critico** per eseguire il task in modo straordinario al prossimo avvio di Agent Dr.Web, se l'esecuzione di tale task è stata persa nell'ora programmata (Agent Dr.Web è disattivato al momento dell'esecuzione del task). Se al momento dell'avvio il task è stato perso diverse volte, verrà eseguito solo 1 volta.



L'impostazione simile viene definita nella finestra principale di Scheduler tramite l'elemento della barra degli strumenti **Gravità**.



Se in tale caso sono da eseguire diversi task di scansione, ne verrà 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.

- Se il flag **Avvia il task in modo asincrono** è deselezionato, il task verrà messo nella coda generale dei task di Scheduler eseguiti in sequenza. Spuntare il flag per eseguire questo task in modo parallelo al di fuori della coda.
2. Nella scheda **Azione** selezionare il tipo di task dalla lista a cascata **Azione** e configurare i parametri del task, richiesti per l'esecuzione:

Tipo di task	Parametri e descrizione
Registrazione nel file di log	Stringa — testo del messaggio che viene registrato nel file di log.
Avvio del programma	Impostare i seguenti parametri: <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 della riga di comando per il programma da avviare.• Spuntare il flag Attendi che il programma venga completato per l'attesa del completamento del programma avviato da questo task. In questo caso l'Agent Dr.Web registra nel log l'avvio del programma, il codice restituito e l'ora di completamento del programma. Se il flag Attendi che il programma venga completato è deselezionato, il task è considerato completato immediatamente dopo l'avvio del programma, e l'Agent Dr.Web registra nel log solo l'avvio del programma.
Dr.Web Agent Scanner. Scansione rapida	I parametri di configurazione della scansione sono descritti nel p. Configurazione di Scanner .
Dr.Web Agent Scanner. Scansione personalizzata	
Dr.Web Agent Scanner. Scansione completa	




L'avvio remoto dello Scanner è possibile soltanto sulle postazioni SO Windows, SO della famiglia UNIX e macOS.

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



Modalità di avvio	Parametri e descrizione
Iniziale	Il task verrà eseguito all'avvio di Agent Dr.Web. Viene avviato senza parametri aggiuntivi.
Tra N minuti dopo il task iniziale	Dalla lista a cascata Task iniziale è necessario selezionare il task relativamente al quale viene impostato il tempo di esecuzione del task che viene creato. 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.
 - Spuntare il flag **Avvia il task secondo l'UTC** per avviare il task secondo l'ora mondiale (il fuso orario UTC+0). Se il flag è deselezionato, il task verrà avviato secondo l'ora locale sulla postazione.
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.



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

Per configurare la lista dei componenti da installare del pacchetto antivirus

1. Selezionare la voce **Rete antivirus** nel menu principale del Pannello di controllo, nella finestra che si è aperta nella lista gerarchica selezionare una postazione o un gruppo. 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** — imposta 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 installazione del componente antivirus. L'utente decide sull'installazione del componente durante l'installazione di Agent Dr.Web.
 - **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 [8-1](#) 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 Dr.Web.

Tabella 8-1.


Impostato dall'utente	Impostato sul Server Dr.Web		
	Deve	Può	Non può
Installa	+	+	
Non installare	+		

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



8.3.4. Parametri di connessione

Nella scheda **Parametri di connessione** vengono configurati i parametri che definiscono le impostazioni di comunicazione con il Server Dr.Web:

- Nel campo **Certificato** viene impostato il certificato SSL di Server Dr.Web (`drwcsd-certificate.pem`). Per selezionare il file del certificato, premere il pulsante .

Più certificati possono essere memorizzati contemporaneamente su una postazione, per esempio, durante un trasferimento da un Server Dr.Web su un altro. I certificati devono essere univoci, cioè non è possibile impostare due certificati identici.


Per aggiungere un altro certificato, fare clic sul pulsante  e selezionare il file del certificato.

Per rimuovere un certificato esistente, fare clic sul pulsante  di fronte al certificato che deve essere rimosso.



Il certificato deve essere sempre impostato.

- Nel campo **Server** viene impostato l'indirizzo di Server Dr.Web o Server proxy Dr.Web (per maggiori informazioni v. [Server proxy Dr.Web](#)). Questo campo può rimanere vuoto. In questo caso l'Agent Dr.Web utilizza l'indirizzo di Server Dr.Web indicato nelle impostazioni del computer locale dell'utente (l'indirizzo di Server Dr.Web da cui è stata eseguita l'installazione).

È possibile impostare sia un indirizzo di Server Dr.Web che più indirizzi di diversi Server Dr.Web. Per aggiungere un altro indirizzo di Server Dr.Web, fare clic sul pulsante  e inserire l'indirizzo nel campo che è stato aggiunto. Il formato di impostazione degli indirizzi di rete di Server Dr.Web è descritto in documento **Allegati**, [Allegato D. Specifica dell'indirizzo di rete](#).

Esempio di impostazione dell'indirizzo di Server Dr.Web:

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 Dr.Web si disconnettono dal Server Dr.Web e non possono più connettersi ad esso. In questo caso, l'indirizzo di Server Dr.Web 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 in 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 in modalità *Mulicasting*.
- I campi **Modalità di compressione** e **Modalità di cifratura** definiscono le impostazioni corrispondenti della compressione e cifratura del 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 in documento **Allegati**, [Allegato D. Specifica dell'indirizzo di rete](#).


Di default si utilizza **udp/:2193**, il che significa "tutte le interfacce, porta 2193".

8.3.5. Chiavi di licenza

È possibile visualizzare e modificare la lista delle chiavi di licenza di una postazione o di un gruppo nei seguenti modi:

1. Tramite [Gestione licenze](#).
2. Attraverso la configurazione dell'oggetto di licenza (postazione o gruppo) nella rete antivirus.

Per modificare la lista delle chiavi di licenza attraverso la configurazione di un oggetto di licenza

1. Selezionare la voce **Rete antivirus** nel menu principale del Pannello di controllo.
2. Aprire la sezione [Proprietà della postazione](#) o [Modifica dei gruppi](#) per l'oggetto di cui le chiavi di licenza si vuole modificare.
3. Nella sezione configurazione fare clic sull'icona  **Modifica** o sul link **Chiavi di licenza**.
4. La finestra **Chiavi di licenza** che si è aperta contiene la lista delle chiavi dell'oggetto, il loro status corrente (ereditate o impostate individualmente), e inoltre, la lista di tutte le chiavi disponibili su questo Server Dr.Web. Inoltre, se necessario, è possibile passare direttamente alla Gestione licenze.
5. Le azioni applicabili alla lista chiavi dipendono dallo status delle chiavi di licenza correnti dell'oggetto:


Azione	Le chiavi correnti sono ereditate	Le chiavi correnti sono impostate in modo individuale	Nessuna chiave di licenza è impostata
Aggiungi chiave di licenza	L'ereditarietà verrà interrotta. La nuova chiave verrà aggiunta alla lista delle chiavi assegnate e la lista delle chiavi sarà individuale.	La nuova chiave verrà aggiunta alla lista delle chiavi assegnate.	Le chiavi verranno aggiunte alla lista delle chiavi di licenza dell'oggetto come chiavi individuali.
Rimuovi chiave di licenza	L'azione non è disponibile.	Una chiave verrà rimossa dalla lista delle chiavi dell'oggetto.	L'azione non è disponibile.




Azione	Le chiavi correnti sono ereditate	Le chiavi correnti sono impostate in modo individuale	Nessuna chiave di licenza è impostata
Imposta l'ereditarietà	L'azione non è disponibile.	Le chiavi correnti verranno rimosse dalla lista delle chiavi dell'oggetto, viene impostata l'ereditarietà delle chiavi dal gruppo primario/gruppo padre.	L'azione non è disponibile.
Interrompi l'ereditarietà	L'ereditarietà verrà interrotta. La lista delle chiavi rimarrà inalterata, ma sarà individuale.	L'azione non è disponibile.	L'azione non è disponibile.

Le chiavi correnti sono ereditate

Per aggiungere una chiave di licenza

1. Nella finestra **Chiavi di licenza**, nella lista **Tutte le chiavi** selezionare una o più chiavi di licenza che si vuole aggiungere.
2. Premere .
3. Se le liste dei componenti da installare sulle postazioni e nelle chiavi che vengono aggiunte sono diverse, verrà visualizzato l'avviso corrispondente e verrà chiesto di modificare la lista risultante dei componenti.
4. Dopo aver apportato tutte le modifiche necessarie, premere **Salva**.
5. L'ereditarietà verrà interrotta. La nuova chiave verrà aggiunta alla lista delle chiavi assegnate e la lista delle chiavi sarà individuale.


Per interrompere l'ereditarietà senza modificare la lista delle chiavi di licenza

1. Nella finestra **Chiavi di licenza** premere il pulsante  **Copia le impostazioni dal gruppo primario e impostale come individuali**.
2. L'ereditarietà verrà interrotta. La lista delle chiavi verrà copiata dal gruppo primario/gruppo padre e impostata per l'oggetto come una lista individuale.
3. Premere **Salva**.



Le chiavi correnti sono impostate in modo individuale

Per aggiungere una chiave di licenza

1. Nella finestra **Chiavi di licenza**, nella lista **Tutte le chiavi** selezionare una o più chiavi di licenza che si vuole aggiungere.
2. Premere .
3. Se le liste dei componenti da installare sulle postazioni e nelle chiavi che vengono aggiunte sono diverse, verrà visualizzato l'avviso corrispondente e verrà chiesto di modificare la lista dei componenti.
4. Dopo aver apportato tutte le modifiche necessarie, premere **Salva**.
5. La nuova chiave verrà aggiunta alla lista delle chiavi assegnate.

Per rimuovere una chiave di licenza



1. Nella finestra **Chiavi di licenza**, nella lista **Chiavi dell'oggetto** fare clic su  di fronte alle chiavi di licenza che si vuole rimuovere.



Se sono state rimosse tutte le chiavi, verrà impostata l'ereditarietà delle chiavi di licenza dal gruppo primario/gruppo padre (vedi inoltre [Impostazione dell'ereditarietà](#)).

2. Premere **Salva**.
3. Se le liste dei componenti da installare sulle postazioni e nelle chiavi rimanenti sono diverse, verrà visualizzato l'avviso corrispondente e verrà chiesto di modificare la lista risultante dei componenti.

Per impostare l'ereditarietà

1. È possibile impostare l'ereditarietà in uno dei seguenti modi:
 - Aprire la sezione [Proprietà della postazione](#) o [Modifica dei gruppi](#) per l'oggetto per cui si vuole impostare l'ereditarietà. Nella sezione configurazione fare clic sull'icona  **Rimuovi chiave**.
 - Nella finestra **Chiavi di licenza**, nella lista **Chiavi dell'oggetto** fare clic su  di fronte a tutte le chiavi di licenza assegnate. Premere **Salva**.
2. Le chiavi correnti verranno rimosse dalla lista delle chiavi dell'oggetto, viene impostata l'ereditarietà delle chiavi dal gruppo primario/gruppo padre.
3. Se le liste dei componenti da installare sulle postazioni e nelle chiavi ereditate sono diverse, verrà visualizzato l'avviso corrispondente e verrà chiesto di modificare la lista dei componenti.




Nessuna chiave di licenza è impostata



La situazione è possibile solo se nessuna chiave di licenza è stata aggiunta sul Server Dr.Web o se chiavi di licenza sono state aggiunte sul Server Dr.Web, ma non sono state distribuite su nessun oggetto, incluso il gruppo **Everyone**.

Per aggiungere una chiave di licenza

1. Nella finestra **Chiavi di licenza**, nella lista **Tutte le chiavi** selezionare una o più chiavi di licenza che si vuole aggiungere.
2. Premere .
3. Premere **Salva**.
4. Le chiavi verranno aggiunte alla lista delle chiavi di licenza dell'oggetto come chiavi individuali.

8.4. Configurazione dei componenti antivirus



Le impostazioni dei componenti antivirus, configurabili attraverso il Pannello di controllo, sono descritte dettagliatamente nel **Manuale dell'amministratore** per la gestione delle postazioni per il sistema operativo corrispondente.

Componenti

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

Postazioni SO 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 verifica della presenza di rootkit.

SpIDer Guard

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

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).

SplDer 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 a risorse locali e di rete, in particolare, controllo dell'accesso a siti web. Permette di controllare l'integrità dei file importanti, proteggendoli contro le modifiche accidentali o contro l'infezione dai virus, e vieta ai dipendenti l'accesso alle informazioni indesiderate.

Firewall

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

Quarantena

Isolamento di oggetti dannosi e sospetti in una directory speciale.

Auto-protezione

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

Protezione preventiva

Include l'analisi comportamentale, la protezione dagli exploit e la protezione dai ransomware.

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

Controllo delle applicazioni

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



Postazioni con SO della famiglia UNIX

Dr.Web Scanning Engine

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

Dr.Web File Checker

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

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

Dr.Web ICAPD

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

SpIDer Guard per Linux (solo come parte dei pacchetti di distribuzione per i sistemi operativi della famiglia GNU/Linux)

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

SpIDer Guard per SMB

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

SpIDer Guard per NSS (solo come parte dei pacchetti di distribuzione per i sistemi operativi della famiglia GNU/Linux)

Monitor dei volumi NSS (Novell Storage Services). Funziona in background e monitora le operazioni del file system (come per esempio la creazione, l'apertura e la chiusura di un file, nonché le operazioni di scrittura) sui volumi NSS montati in un punto specificato del



file system. Invia il contenuto di file nuovi e modificati per la verifica al componente della scansione file.

SpIDer Gate (solo come parte dei pacchetti di distribuzione per i sistemi operativi della famiglia GNU/Linux)

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

Dr.Web MailD

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

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



Gli altri componenti per le postazioni con i sistemi operativi della famiglia UNIX sono aggiuntivi e servono per la configurazione interna del funzionamento del software antivirus.

Postazioni macOS

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. Controlla tutti i processi che vengono avviati e 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 sospetti in una directory speciale.



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.

SplDer Guard

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

Filtro chiamate ed SMS

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

Antifurto

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

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 applicazioni.

Auditor della sicurezza (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.

8.5. Scansione antivirus delle postazioni



L'utente della postazione può eseguire la scansione antivirus della postazione in modo autonomo utilizzando il componente Scanner Dr.Web.



L'avvio e il corretto funzionamento dello Scanner sono possibili anche se l'Agent Dr.Web non è operativo, tra le altre cose anche in modalità provvisoria del sistema operativo.

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.

8.5.1. Interruzione dei componenti in esecuzione 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.

Per interrompere l'esecuzione di tutti i componenti di un determinato tipo, avviati su postazioni

1. Selezionare la voce **Rete antivirus** nel 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 della directory 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 dallo Scheduler** — per arrestare una scansione attiva Dr.Web Agent Scanner, che è stata avviata secondo i task del calendario centralizzato.
 - **Interrompi Dr.Web Agent Scanner avviato dall'amministratore** — per arrestare una scansione attiva tramite Dr.Web Agent Scanner, che è stata avviata manualmente dall'amministratore tramite il Pannello di controllo.
 - **Interrompi Scanner Dr.Web avviato dall'utente** — per arrestare una scansione attiva tramite Scanner Dr.Web, che è stata avviata dall'utente sulla postazione.
 - **Interrompi SpIDer Guard, SpIDer Mail, SpIDer Gate, Office control, Firewall, Auto-protezione e Protezione preventiva** — per sospendere l'operazione dei rispettivi componenti.


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**.




8.5.2. Avvio della scansione della postazione


Per avviare la scansione antivirus delle postazioni

1. Selezionare la voce **Rete antivirus** nel menu principale del Pannello di controllo.
2. Nella finestra che si è aperta, nella lista gerarchica fare clic sul nome di una postazione o di un gruppo.
3. Nella barra degli strumenti fare clic sulla voce  **Scansiona**. Nella lista che si è aperta nella barra degli strumenti selezionare una delle modalità di scansione:

 **Scansione rapida**. In questa modalità vengono scansionati i seguenti oggetti:

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

 **Scansione completa**. In questa modalità viene eseguita la scansione completa di tutti i dischi rigidi e supporti rimovibili (inclusi i settori di avvio).

 **Scansione personalizzata**. Questa modalità permette di selezionare qualsiasi directory o file per la successiva scansione, nonché configurare le impostazioni di scansione avanzate.

4. Dopo che è stata selezionata una variante di scansione, si apre la finestra delle impostazioni di Dr.Web Agent Scanner. Se necessario, modificare le impostazioni di scansione (v. sezione [Configurazione di Scanner](#)).
5. Premere il pulsante **Scansiona** per avviare il processo di scansione sulle postazioni selezionate.



La scansione della postazione tramite Dr.Web Agent Scanner avviato su remoto viene eseguita in background senza visualizzare gli avvisi all'utente della postazione.

8.5.3. Configurazione di 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 in remoto tramite Pannello di controllo. Tuttavia, l'amministratore



può modificarne le impostazioni in modo centralizzato che successivamente verranno trasmesse e salvate 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 Scanner Dr.Web

1. Selezionare la voce **Rete antivirus** nel menu principale del Pannello di controllo.
2. Nella finestra che si è aperta, nella lista gerarchica fare clic sul nome di 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 Dr.Web.
4. Impostare i parametri di scansione richiesti. La descrizione dei parametri di Scanner Dr.Web è riportata in **Guida alla gestione di postazioni** 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 una scansione delle postazioni, come descritto in p. [Avvio della scansione della postazione](#).

La lista delle sezioni delle impostazioni di Dr.Web Agent Scanner che saranno disponibili (+) o non disponibili (–) dipende dalla variante di avvio della scansione di postazioni ed è riportata nella tabella sotto.

Tabella 8–2. Lista delle sezioni delle impostazioni di Dr.Web Agent Scanner a seconda della variante di avvio

Variante di avvio della scansione	Sezioni delle impostazioni			
	Generali	Azioni	Limitazioni	Eccezioni
 Scansione personalizzata	+	+	+	+
 Scansione rapida	+	+	+	–
 Scansione completa	+	+	+	–



A seconda del sistema operativo della postazione su cui viene avviata la scansione remota, sarà disponibile solo quella parte delle impostazioni di Dr.Web Agent Scanner che è supportata dal sistema operativo della postazione.

8.5.3.1. Generali



Le impostazioni che non sono supportate per la scansione delle postazioni SO della famiglia UNIX e macOS sono racchiuse tra parentesi quadre [].

Le impostazioni che non sono supportate per la scansione delle postazioni con SO Android sono racchiuse tra parentesi tonde ().

Nella sezione **Generali** è possibile configurare le seguenti impostazioni della scansione antivirus tramite Dr.Web Agent Scanner:

- Nella lista a cascata selezionare una delle modalità di scansione:
 - **Scansione di tutti i dischi** — esegui la scansione antivirus su tutti i dischi locali disponibili.
 - **Scansione dei percorsi indicati** — esegui la scansione antivirus solo sui percorsi indicati.
- Nel campo **Percorsi da scansionare** impostare una lista dei percorsi da scansionare (il metodo di impostazione è descritto in p. [Eccezioni](#)).
- Per aggiungere una nuova riga alla lista, fare clic sul pulsante e nella riga che si è aperta inserire il percorso richiesto.
 - Per rimuovere un elemento dalla lista, fare clic sul pulsante di fronte alla riga corrispondente.
- Spuntare il flag **Controlla settori di avvio** affinché Dr.Web Agent Scanner esegua la scansione dei 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 in esecuzione automatica** per scansionare i programmi eseguiti automaticamente alla partenza del sistema operativo.
 - Spuntare il flag **[Controlla programmi e moduli che vengono caricati]** per scansionare i processi in esecuzione nella memoria operativa.
 - Spuntare il flag **[Verifica la presenza di rootkit]** per abilitare la ricerca dei programmi malevoli che nascondono la propria presenza nel sistema operativo.
 - Spuntare il flag **Controlla le unità fisse** per scansionare le unità dischi fissi (hard drive ecc.).
 - Spuntare il flag **Controlla oggetti sui supporti rimovibili** per scansionare tutte le unità dispositivi rimovibili, per esempio unità dischi magnetici (dischetti), CD/DVD, dispositivi flash ecc.
 - Spuntare il flag **Utilizza l'analisi euristica** affinché Dr.Web Agent Scanner cerchi i virus sconosciuti utilizzando l'analisi euristica. In questa modalità sono possibili falsi positivi di Scanner.



- Spuntare il flag **Segui collegamenti simbolici** affinché la scansione segua collegamenti simbolici.
- Spuntare il flag **[(Sospendi la scansione se computer passa all'alimentazione a batteria)]** per sospendere la scansione antivirus se il computer dell'utente passa all'alimentazione a batteria.
- Spuntare il flag **Scollega il computer dalla rete per il tempo della scansione** per scollegare il computer dalla rete locale e da internet per il tempo della scansione.
- Spuntare il flag **Archivi** per cercare virus nei file in archivi compressi.
- Spuntare il flag **File di email** per controllare caselle email.
- Spuntare il flag **Pacchetti di installazione** per controllare pacchetti di installazione di programmi.
- Dalla lista a cascata **[(Priorità di scansione)]** selezionare la priorità del processo di scansione relativamente alle risorse di calcolo disponibili del sistema operativo.
- Dalla lista a cascata **[(Livello di utilizzo delle risorse del computer)]** selezionare l'utilizzo massimo ammissibile delle risorse durante la scansione tramite Dr.Web Agent Scanner. In assenza di altri processi attivi le risorse del computer verranno utilizzate al massimo.



L'opzione **Livello di utilizzo delle risorse del computer** non influisce sul valore effettivo del consumo delle risorse se la scansione viene eseguita in un sistema a singolo processore con un core.

- Nel campo **[(Core del processore utilizzati (numero))]** impostare il numero massimo di core del processore utilizzati da Dr.Web Agent Scanner. Sono ammissibili i valori interi da 0 a 32. Il valore 0 prescrive di utilizzare tutti i core disponibili. Configurando un gruppo di postazioni, è necessario prestare attenzione al fatto che per questo parametro viene impostato il valore assoluto e non il rapporto percentuale del numero totale di core disponibili. Pertanto, l'impostazione dello stesso valore può portare a un carico relativo differente di postazioni con un numero diverso di core di processore.
- Dalla lista a cascata **[(Core del processore utilizzati (%))]** selezionare il rapporto percentuale di core utilizzati rispetto al numero totale di core disponibili.
- Nella lista a cascata **(Azioni dopo la scansione)** selezionare quale azione verrà eseguita immediatamente dopo il completamento del processo di scansione:
 - **non fare nulla** — dopo la fine della scansione non intraprendere alcuna azione con il computer dell'utente.
 - **spegni la postazione** — dopo la fine della scansione spegni il computer dell'utente. Prima di spegnere il computer, Dr.Web Agent Scanner applicherà alle minacce rilevate le azioni impostate.
 - **riavvia la postazione** — dopo la fine della scansione riavvia il computer dell'utente. Prima di riavviare il computer, Dr.Web Agent Scanner applicherà alle minacce rilevate le azioni impostate.
 - **passa la postazione in modalità di sospensione.**
 - **passa la postazione in modalità di ibernazione.**





8.5.3.2. Eccezioni

Nella sezione **Eccezioni** viene impostata una lista delle directory e dei file da escludere dalla scansione antivirus tramite Dr.Web Agent Scanner.



Prima di aggiungere eccezioni, consultare le raccomandazioni sull'utilizzo di programmi antivirus su computer con SO Windows. Un articolo con le informazioni necessarie si trova all'indirizzo <https://support.microsoft.com/en-us/topic/virus-scanning-recommendations-for-enterprise-computers-that-are-running-windows-or-windows-server-kb822158-c067a732-f24a-9079-d240-3733e39b40bc>. Il materiale di questo articolo ha lo scopo di aiutare a ottimizzare le prestazioni del sistema in presenza di software antivirus.

Per modificare la lista dei percorsi e file da escludere

1. Inserire il percorso di un file o di una directory 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 rimuovere 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:
 - Il carattere \ esclude dalla scansione l'intero disco di sistema in SO Windows,
 - Il carattere / esclude dalla scansione l'intero file system radice in SO della famiglia Unix,
 - Percorso che finisce con il carattere \ (o / in caso di SO della famiglia Unix) — questa directory viene esclusa dalla scansione,
 - Percorso che non finisce con il carattere \ (o / in caso di SO della famiglia Unix) — viene esclusa dalla scansione qualsiasi sottodirectory il cui percorso inizia con la stringa indicata.

Esempio per SO Windows: `C:\Windows` — non scansionare i file della directory `C:\Windows` e tutte le sue sottodirectory.

Esempio per SO della famiglia Unix: `/etc` — non scansionare i file della directory `/etc` e tutte le sue sottodirectory.

2. Maschere di oggetti esclusi dalla scansione. Per impostare le maschere si possono utilizzare i caratteri ? e *.

Esempio per SO Windows: `C:\Windows**.dll` — non scansionare tutti i file con estensione `dll` che si trovano in tutte le sottodirectory della directory `C:\Windows`.

Esempio per SO della famiglia Unix: `/etc/*/*.pub` — non scansionare tutti i file con estensione `pub` che si trovano in tutte le sottodirectory della directory `/etc`.



3. Variabili di ambiente impostate nel sistema operativo come parte del percorso degli oggetti esclusi dalla scansione.

Esempio per SO Windows: %WINDIR%\SysWOW64\ — non scansionare i file nella sottodirectory SysWOW64 della directory C:\Windows.

Esempio per SO della famiglia Unix: /home/*/network — non scansionare i file nella sottodirectory network della directory /home.

4. 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.

La sintassi delle espressioni regolari utilizzate per trascrivere percorsi esclusi è la seguente:

```
qr{ <espressione> } <flag>
```

Il più spesso come flag si utilizza il carattere `i`; questo flag significa "non prendere in considerazione differenza di maiuscole e minuscole".

Esempi di trascrizione in espressioni regolari di percorsi e file da escludere

Espressione regolare	Valore
<code>qr{\\pagefile\.sys\$}i</code>	non scansionare file di swap di SO Windows
<code>qr{\\notepad\.exe\$}i</code>	non scansionare file <code>notepad.exe</code>
<code>qr{^C:}i</code>	non scansionare proprio niente sul disco C :
<code>qr{^\.:\WINNT\\}i</code>	non scansionare niente nelle directory WINNT su tutti i dischi
<code>qr{(^C:) (^\.:\WINNT\\)}i</code>	combinazione dei due casi precedenti
<code>qr{^C:\\dir1\\dir2\\file\.ext\$}i</code>	non scansionare il file <code>c:\dir1\dir2\file.ext</code>
<code>qr{^C:\\dir1\\dir2\\(.+\\)?file\.ext\$}i</code>	non scansionare il file <code>file.ext</code> se si trova nella directory <code>c:\dir1\dir2</code> e nelle sottodirectory
<code>qr{^C:\\dir1\\dir2\\}i</code>	non scansionare la directory <code>c:\dir1\dir2</code> e le sottodirectory
<code>qr{dir\\[^\\]+}i</code>	non scansionare la sottodirectory <code>dir</code> che si trova in qualsiasi directory, ma scansiona le sottodirectory
<code>qr{dir\\}i</code>	non scansionare la sottodirectory <code>dir</code> che si trova in qualsiasi directory e le sottodirectory

L'utilizzo delle espressioni regolari è brevemente descritto in documento **Allegati**, [Allegato I. Utilizzo delle espressioni regolari in Dr.Web Enterprise Security Suite.](#)



8.5.3.3. Azioni

Nella sezione **Azioni** viene impostata la reazione di Dr.Web Agent Scanner al rilevamento di file infetti o sospetti, programmi malevoli, nonché archivi infetti.



Dr.Web Agent Scanner applica automaticamente le azioni impostate per gli oggetti malevoli rilevati.

Sono previste le seguenti azioni da applicare alle minacce rilevate:

- **Cura** — per ripristinare l'oggetto infetto allo stato precedente all'infezione. Se l'oggetto è incurabile o se il tentativo di cura 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 rimuovere gli oggetti infetti.
- **Sposta in quarantena** — per trasferire gli oggetti infetti nella directory di Quarantena su postazione.
- **Informa** — per inviare nel Pannello di controllo un avviso di rilevamento di un virus (per la configurazione della modalità di avviso v. p. [Configurazione degli avvisi](#)).
- **Ignora** — per saltare l'oggetto senza eseguire alcuna azione, tra l'altro, non inviare avvisi nelle statistiche di scansione.

Tabella 8-3. Azioni di Dr.Web Agent Scanner sugli oggetti malevoli rilevati

Oggetto	Azione				
	Cura	Rimuovi	Sposta in quarantena	Informa	Ignora
Infetti	+/*	+	+	disponibile se in una delle chiavi c'è l'opzione AllowReportAction=Yes	
Sospetti		+	+/*		+
Incurabili		+	+/*		
Pacchetti di installazione		+	+/*		
Archivi compressi		+	+/*		



Oggetto	Azione				
	Cura	Rimuovi	Sposta in quarantena	Informa	Ignora
File di email			+	+/*	+
Settori di avvio	+/*			+	
Adware		+	+/*		+
Dialer		+	+/*		+
Joke		+	+/*		+
Riskware		+	+/*		+
Hacktool		+	+/*		+

Segni convenzionali

- + azione consentita per questo tipo di oggetti
- +/* azione predefinita per questo tipo di oggetti

Per impostare le azioni sulle minacce rilevate, utilizzare le seguenti impostazioni:

- La lista a cascata **Infetti** imposta la reazione di Dr.Web Agent Scanner al rilevamento di un file infettato da un virus conosciuto.
- La lista a cascata **Sospetti** imposta la reazione di Dr.Web Agent 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 directory di installazione di SO, si consiglia di selezionare per i file sospetti la reazione **Informa**.

- La lista a cascata **Incurabili** imposta la reazione di Dr.Web Agent Scanner al rilevamento di un file infettato da un virus conosciuto incurabile, nonché per i casi in cui il tentativo di cura non è riuscito.
- La lista a cascata **Pacchetti di installazione infetti** imposta la reazione di Dr.Web Agent Scanner al rilevamento di un file infetto o sospetto all'interno di pacchetti di installazione di programmi.
- La lista a cascata **Archivi infetti** imposta la reazione di Dr.Web Agent Scanner al rilevamento di un file infetto o sospetto all'interno di un archivio di file.
- La lista a cascata **File di email infetti** imposta la reazione di Dr.Web Agent Scanner al rilevamento di un file infetto o sospetto in formato 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.

- 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 **Mostra il progresso della scansione** per visualizzare nel Pannello di controllo l'indicatore e la barra di stato del processo di scansione della postazione.

8.5.3.4. Limitazioni



Le impostazioni che non sono supportate per la scansione delle postazioni SO della famiglia UNIX e macOS sono racchiuse tra parentesi quadre [].

Nella sezione **Limitazioni** sono disponibili le seguenti impostazioni della scansione antivirus tramite Dr.Web Agent Scanner:

- **Tempo massimo di scansione (ms)** — tempo massimo in millisecondi di scansione di un oggetto. Dopo il tempo indicato, la scansione dell'oggetto viene arrestata.
- **Livello di annidamento massimo di un archivio** — numero massimo di archivi annidati. Se un archivio ha un livello di annidamento che 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.
- **Rapporto di compressione massimo** — se Dr.Web Agent Scanner determina che il rapporto di compressione di un 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 Dr.Web Agent 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.

8.6. Visualizzazione delle statistiche della postazione

Tramite il menu di gestione della sezione **Rete antivirus** si possono visualizzare le seguenti informazioni:

- **Statistiche** — statistiche sul funzionamento degli elementi antivirus su postazione, sullo stato delle postazioni e degli elementi antivirus, per visualizzare e salvare i report contenenti tutte le statistiche riepilogative o riassunti selezionati per tipo di tabella.
- **Grafici** — grafici con informazioni sulle infezioni rilevate su postazioni.
- **Quarantena** — accesso remoto ai contenuti della Quarantena su postazione.

8.6.1. Statistiche



È possibile configurare la creazione automatica di un report statistico che includa le tabelle statistiche richieste. Questo report in formato selezionato non solo può essere salvato su Server Dr.Web, ma anche inviato via email.

Per farlo, configurare il task **Creazione del report statistico** nel [calendario](#) di Server Dr.Web.

Per visualizzare le tabelle

1. Selezionare la voce **Rete antivirus** nel menu principale del Pannello di controllo, nella finestra che si è aperta nella lista gerarchica fare clic sul nome di una postazione o di un gruppo.
2. Nel [menu di gestione](#) che si è aperto, selezionare la voce richiesta dalla sottosezione **Statistiche**.

La sezione di menu **Statistiche** contiene le seguenti voci:

- **Minacce** — per visualizzare informazioni sulle minacce rilevate alla sicurezza delle postazioni protette: un elenco degli oggetti infetti, la posizione per postazione, i nomi delle minacce, le azioni dell'antivirus ecc.



In caso di blocco di URL per i virus e miner, nella tabella viene visualizzata l'azione "Segnalati".

- **Errori** — per visualizzare una lista di errori di scansione sulla postazione selezionata per un determinato periodo.



- **Dati riepilogativi** — per visualizzare e salvare i report che contengono tutte le statistiche riepilogative o riassunti selezionati per tipo di tabella. Non è disponibile nel menu se sono nascoste tutte le altre voci di menu nella sezione **Statistiche**.
- **Statistiche di scansione** — per ottenere le statistiche di funzionamento degli elementi antivirus su postazione.
- **Avvio/Arresto** — per visualizzare la lista dei componenti che erano avviati su postazione.
- **Statistiche delle minacce** — per visualizzare informazioni sul rilevamento delle minacce alla sicurezza delle postazioni protette, raggruppate per tipo di minaccia e per quantità di minacce su postazioni.
- **Stato** — per visualizzare informazioni su uno stato insolito delle postazioni, che probabilmente richiede l'intervento.
- **Task** — per visualizzare la lista dei task assegnati alla postazione in un determinato periodo.
- **Dispositivi bloccati** — per visualizzare la lista dei dispositivi bloccati su postazioni dal componente Office control.
- **Prodotti** — per visualizzare informazioni sui prodotti installati su postazioni selezionate. Per prodotti in questo caso si intendono i prodotti del **repository** di Server Dr.Web.
- **Database dei virus** — per visualizzare informazioni sui database dei virus installati: nome del file che contiene un database dei virus specifico; 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 singole postazioni.
- **Moduli** — per visualizzare le informazioni dettagliate su tutti i moduli dell'antivirus Dr.Web: il nome funzionale, l'hash MD5, la versione completa del modulo ecc. Questa voce è disponibile solo se vengono selezionate postazioni.
- **Eventi di Protezione preventiva** — per visualizzare informazioni sugli eventi registrati su postazioni dal componente Protezione preventiva.
- **Eventi di Controllo delle applicazioni** — per visualizzare informazioni sugli eventi registrati su postazioni dal componente Controllo delle applicazioni.
- **Installazioni di Agent** — per visualizzare la lista delle installazioni di Agent Dr.Web su una postazione o un gruppo di postazioni.
- **Disinstallazioni di Agent** — per visualizzare la 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. sotto), dopodiché premere il pulsante **Salva** e riavviare il Server Dr.Web.



Tabella 8-4. Corrispondenza delle voci della sezione Statistiche e dei flag della sezione Statistiche nella configurazione di Server Dr.Web

Voci della sezione Statistiche	Flag della sezione Statistiche nella configurazione di Server Dr.Web
Minacce	Minacce alla sicurezza rilevate
Errori	Errori di scansione
Statistiche di scansione	Statistiche di scansione
Avvio/Arresto	Avvio/arresto dei componenti
Statistiche delle minacce	Minacce alla sicurezza rilevate
Stato	Stato delle postazioni
Task	Log di esecuzione di task su postazioni
Dispositivi bloccati	Dispositivi bloccati
Database dei virus	Stato delle postazioni Stato dei database dei virus
Moduli	Lista dei moduli delle postazioni
Eventi di Protezione preventiva	Minacce alla sicurezza rilevate
Eventi di Controllo delle applicazioni	Statistiche di Controllo applicazioni sull'attività dei processi Statistiche di Controllo applicazioni sul blocco dei processi
Installazioni di Agent	Installazioni di 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.

8.6.1.1. Dati riepilogativi




Per visualizzare i dati riepilogativi

1. Nella lista gerarchica selezionare una postazione o un gruppo.
2. Nel [menu di gestione](#) nella sezione **Statistiche** selezionare la voce **Dati complessivi**.
3. Si apre una finestra che contiene i dati tabulari di report.



Per includere nel report determinate statistiche, premere il pulsante  nella barra degli strumenti e selezionare i tipi richiesti dalla lista a cascata: **Statistiche di scansione, Minacce, 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. Se nel report è inclusa una tabella con le minacce rilevate, nella barra degli strumenti diventano inoltre disponibili le seguenti opzioni:

Opzione	Descrizione
 Escludi file dalla scansione	<p>Permette di aggiungere gli oggetti selezionati alla lista delle eccezioni dalla scansione dai componenti di protezione:</p> <ol style="list-style-type: none">Nella tabella Minacce spuntare il flag di fronte a uno o più oggetti rilevati.Premere il pulsante .Nella finestra che si è aperta definire le seguenti impostazioni:<ul style="list-style-type: none">• Escludi dalla scansione e assegna le impostazioni individuali di SpIDer Guard — per aggiungere gli oggetti selezionati alla lista delle eccezioni dalla scansione dal componente SpIDer Guard. In tal caso, se i nodi della rete per cui verrà modificata la lista delle eccezioni ereditavano le impostazioni del componente SpIDer Guard dai loro gruppi primari, per loro l'ereditarietà verrà interrotta e loro verranno assegnate le impostazioni individuali.• Escludi dalla scansione e assegna le impostazioni individuali di Scanner Dr.Web — per aggiungere gli oggetti selezionati alla lista delle eccezioni dalla scansione dal componente Scanner Dr.Web. In tal caso, se i nodi della rete per cui verrà modificata la lista delle eccezioni ereditavano le impostazioni del componente Scanner Dr.Web dai loro gruppi primari, per loro l'ereditarietà verrà interrotta e loro verranno assegnate le impostazioni individuali.• Nella lista Escludi per i seguenti oggetti selezionare i nodi della rete per cui l'oggetto selezionato verrà aggiunto alla lista delle eccezioni: solo per la posizione su cui l'oggetto è stato rilevato o per le postazioni e i gruppi custom selezionati nella lista proposta.Premere il pulsante Escludi.
 Scansiona	Per scansionare nuovamente gli oggetti selezionati. Nel menu a cascata selezionare il tipo di scansione.

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 le icone del calendario accanto ai campi di date. Per visualizzare le informazioni, premere il pulsante **Aggiorna**.
6. Se occorre salvare un report in modo da stamparlo o 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.

8.6.1.2. Statistiche di scansione

Per ottenere le statistiche di funzionamento degli elementi antivirus su postazione

1. Nella lista gerarchica selezionare una postazione o un gruppo.



Se è necessario visualizzare le statistiche per diverse postazioni o gruppi, si possono selezionare le postazioni richieste utilizzando i tasti MAIUSCOLO 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 ventiquattro ore.
4. Per visualizzare le informazioni per un determinato periodo, indicare un intervallo di tempo relativamente al giorno odierno nella lista a cascata o impostare un intervallo di tempo nella barra degli strumenti. Per impostare un intervallo di tempo arbitrario, inserire le date richieste o fare clic sulle icone di 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. Per visualizzare statistiche dettagliate di funzionamento di specifici strumenti antivirus, fare clic sul nome di una postazione nella tabella. Si apre una finestra (o una sezione della finestra attuale) contenente una tabella con dati statistici dettagliati.
6. Per ordinare i dati di una colonna della tabella, premere la freccia corrispondente (ordine decrescente o crescente) nell'intestazione della colonna corrispondente.
7. 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.

8. 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](#)).



8.6.1.3. Stato

Per visualizzare informazioni sullo stato delle postazioni

1. Nella lista gerarchica selezionare una postazione o un gruppo.
2. Nel [menu di gestione](#) nella sezione **Statistiche** selezionare la voce **Stato**.
3. Le informazioni circa lo stato delle postazioni vengono visualizzate in base alle impostazioni del filtro. Premere l'icona  nell'intestazione della tabella per modificare i seguenti parametri del filtro:
 - Nel campo **Ricerca** impostare una stringa arbitraria per la ricerca in tutte le sezioni della tabella.
 - Nella lista **Gravità** spuntare i flag per i livelli richiesti di importanza dei messaggi: la lista dei messaggi sullo stato includerà solo i messaggi con la gravità selezionata.
 - Nella lista **Fonte** spuntare i flag per le fonti di comparsa di eventi che dovranno essere visualizzate nella lista:
 - **Agent** — per visualizzare gli eventi arrivati dagli Agent Dr.Web connessi a questo Server Dr.Web.
 - **Server** — per visualizzare gli eventi arrivati da questo Server Dr.Web.
 - Nella lista **Postazioni** spuntare i flag per i tipi di status delle postazioni, i messaggi su cui verranno visualizzati nella lista:
 - **Collegati** — per visualizzare gli eventi per le postazioni che sono connesse a questo Server Dr.Web e sono attualmente in rete (online).
 - **Scollegati** — per visualizzare gli eventi per le postazioni che sono connesse a questo Server Dr.Web e non sono attualmente in rete (offline).
 - **Disinstallati** — per visualizzare l'ultimo evento per le postazioni su cui il software antivirus Dr.Web è stato rimosso.

Per gestire le impostazioni del filtro, utilizzare i seguenti pulsanti nella lista del filtro:

- **Di default** — per ripristinare tutte le impostazioni del filtro nei valori predefiniti.
 - **Aggiorna** — per applicare le impostazioni selezionate del filtro.
4. 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.

5. Se occorre salvare un report in modo da stamparlo o elaborarlo in seguito, premere uno dei pulsanti nel pannello di controllo:



Registra le informazioni in file CSV,



Registra le informazioni in file HTML,



Registra le informazioni in file XML,



 Registra le informazioni in file PDF.

8.6.1.4. Eventi di Controllo delle applicazioni

Configurazione dell'ottenimento delle statistiche

Per attivare l'invio di informazioni dalle postazioni per la sezione Eventi di Controllo delle applicazioni

1. Nella sezione **Rete antivirus** selezionare nell'albero la postazione o il gruppo di postazioni con il Controllo applicazioni installato, da cui si desidera ricevere informazioni sull'avvio delle applicazioni.
2. Nel menu di gestione selezionare la voce **Windows** → **Agent Dr.Web**, se è stato selezionato un gruppo, o **Agent Dr.Web**, se è stata selezionata una postazione.
3. Nella scheda **Generali** spuntare il flag **Monitora eventi di Controllo applicazioni** per monitorare l'attività dei processi sulle postazioni, registrata dal Controllo applicazioni, e inviare gli eventi sul Server Dr.Web. Se la connessione al Server Dr.Web non è disponibile, gli eventi vengono accumulati e inviati quando la connessione viene stabilita. Se il flag è tolto, l'attività di processi viene ignorata.
4. Premere **Salva**.

Per attivare la raccolta delle informazioni da parte del Server Dr.Web per la sezione Eventi di Controllo delle applicazioni

1. Nella sezione **Amministrazione** → **Configurazione del Server Dr.Web** andare alla scheda **Statistiche**.
2. Impostare una delle seguenti opzioni:
 - **Statistiche di Controllo applicazioni sull'attività dei processi**, per ricevere e registrare informazioni su qualsiasi attività di tutti i processi: sia quelli il cui avvio è consentito che quelli vietati da Controllo applicazioni. Quando questa opzione è selezionata, le applicazioni verranno inserite nel prontuario a condizione che sia stato creato e assegnato almeno un [profilo](#) con una o più categorie selezionate di [criteri di analisi funzionale](#). Fino a quando profili non vengono creati e assegnati a postazioni della rete antivirus, l'avvio di tutte le applicazioni è consentito.
 - **Statistiche di Controllo applicazioni sul blocco dei processi**, per ricevere e registrare informazioni sull'attività di tutti i processi il cui avvio è vietato da Controllo applicazioni. Quando questa opzione è selezionata, applicazioni verranno inserite nel prontuario solo dopo che vengono creati [profili](#) secondo le cui impostazioni l'avvio delle applicazioni verrà bloccato e vengono assegnati a postazioni della rete antivirus.



Il flag **Statistiche di Controllo applicazioni sull'attività dei processi** può aumentare significativamente l'intensità d'uso delle risorse per la raccolta delle statistiche su tutta la rete antivirus.



3. Premere il pulsante **Salva**.
4. Riavviare il Server Dr.Web.
5. Dopo il riavvio il Server Dr.Web inizierà a registrare tutte le statistiche di avvio applicazioni, che vengono inviate da tutte le postazioni con il Controllo applicazioni installato.

Visualizzazione delle statistiche

Per visualizzare gli eventi registrati sulle postazioni dal componente Controllo delle applicazioni

1. Nella lista gerarchica selezionare una postazione o un gruppo.
2. Nel [menu di gestione](#) nella sezione **Statistiche** selezionare la voce **Eventi di Controllo delle applicazioni**.
3. Si apre una finestra che contiene una lista delle applicazioni il cui avvio è stato consentito o vietato sulle postazioni selezionate.
4. Di default vengono visualizzate le statistiche delle ultime ventiquattro ore. Per visualizzare i dati per un determinato periodo, indicare nella lista a cascata un intervallo di tempo relativo al giorno di oggi o impostare un intervallo di tempo nella barra degli strumenti. Per impostare un intervallo di tempo arbitrario, inserire le date richieste o fare clic sulle icone di calendario accanto ai campi di date. Per caricare i dati, premere il pulsante **Aggiorna**. Nella finestra verrà caricata una tabella con i dati statistici. Le colonne della tabella sono descritte nella tabella seguente.

Tabella 8-5. Descrizione delle colonne della tabella Eventi di Controllo delle applicazioni

Nome di colonna	Descrizione
Identificatore	Identificatore della postazione
Postazione	Nome della postazione
Indirizzo della postazione	Indirizzo della postazione
Identificatore di sicurezza	Identificatore di sicurezza dell'account utente
Utente	Utente della postazione
Tipo di evento	Tipo di evento avviato sulla postazione
Azione applicata	Azione applicata all'applicazione avviata sulla postazione
Criterio di analisi funzionale	Criterio in base a cui l'applicazione viene consentita o vietata
Maschera di analisi funzionale	Parametro del criterio di analisi funzionale che determina se è consentito avviare l'applicazione sulla postazione o meno



Nome di colonna	Descrizione
ID del profilo	Identificatore del profilo
Nome del profilo	Nome del profilo
ID della regola	Identificatore della regola
Nome della regola	Nome della regola
Modalità di funzionamento	Modalità in cui funziona la regola
Percorso del file del processo	Posizione del file del processo
Processo	Processo che è consentito o vietato avviare sulla postazione
Bollettino con l'hash del processo	Bollettino in cui è presente l'hash del file del processo avviato
Percorso del file dello script	Posizione del file dello script
Script	File dello script
Bollettino con l'hash dello script	Bollettino in cui è presente l'hash del file dello script avviato
Comparsa dell'evento	Data e ora di comparsa dell'evento
Avviso di evento	Data e ora dell'avviso di evento
Hash del file (SHA-256)	Valore di hash del file secondo l'algoritmo SHA-256
Descrizione del file	Descrizione del file
Editore	Editore del file
Emittente del certificato	Autorità di certificazione che ha rilasciato il certificato
Impronta del certificato (SHA-1)	Valore di hash del certificato secondo l'algoritmo SHA-1
Data di inizio validità del certificato	Data di inizio validità del certificato
Data di fine validità del certificato	Data di fine validità del certificato



5. 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.**



Con un profilo o una regola presente in [modalità test](#) le applicazioni avviate sulle postazioni specificate vengono controllate per tutto lo [schema di funzionamento di Controllo delle applicazioni](#) dall'inizio alla fine. Nelle statistiche verranno registrati i casi di corrispondenza dell'applicazione a tutti i criteri possibili: impostazioni di analisi funzionale, regole e gruppo di applicazioni affidabili. Pertanto, la stessa applicazione può avere più record nella colonna **Azione applicata** dove verrà indicato che è consentita secondo alcuni criteri e/o bloccata secondo altri.

Creazione delle regole

Per creare una nuova regola basata sulle statistiche di eventi di Controllo delle applicazioni

1. Nella sezione **Statistiche** → **Eventi di Controllo delle applicazioni** selezionare una riga con un evento di tentativo di avvio di un'applicazione per cui si desidera creare una regola che ne controlli l'avvio.
2. Dopo un click su una riga della tabella si aprirà una finestra con informazioni sull'evento selezionato.
3. Premere il pulsante **Crea regola** (sulla base dei dati del processo o dell'applicazione).
4. Si apre una finestra per la creazione di una nuova regola. Configurare le seguenti impostazioni:
 - a) Dalla lista a cascata **Nome del profilo** selezionare un [profilo](#) di Controllo delle applicazioni in cui verrà creata la regola.
 - b) Nel campo **Nome della regola** specificare un nome per la regola che viene creata.
 - c) Nella sezione **Tipo di regola** selezionare il tipo di regola creata: quella [di divieto](#) o [di permesso](#).
 - d) Per l'opzione **Modalità di funzionamento** selezionare in quale modalità funzionerà la regola creata (corrisponde al flag **Metti la regola in modalità test** disponibile durante la creazione di una regola da un profilo):

Se si vuole testare la regola, selezionare la modalità **Test**. Le applicazioni non verranno bloccate sulle postazioni, però la registrazione del log delle attività verrà eseguita come con le impostazioni attivate. I risultati di avvii e blocchi delle applicazioni in modalità test di funzionamento della regola verranno visualizzati nella sezione **Eventi di Controllo delle applicazioni**.

In modalità **Attivo** la regola funzionerà in modalità attiva in cui le applicazioni sulle



postazioni vengono bloccate in base alle impostazioni della regola specificate (vedi inoltre [modalità di funzionamento dei profili](#)).

- e) Nella sezione **Proibisci l'avvio di applicazioni secondo i seguenti criteri/Consenti l'avvio di applicazioni secondo i seguenti criteri** (a seconda del tipo di regola selezionato nel passaggio 4c) i campi verranno automaticamente compilati in conformità all'applicazione sulla base della quale viene creata la regola. Se necessario, è possibile modificare i valori delle impostazioni.
5. Premere **Salva**. La regola verrà creata nel profilo specificato di Controllo applicazioni.

8.6.2. Grafici

Grafici e tabelle delle infezioni

Per visualizzare i grafici e le tabelle generali con informazioni sulle infezioni rilevate

1. Selezionare la voce **Rete antivirus** nel menu principale del Pannello di controllo, nella finestra che si è aperta nella lista gerarchica fare clic sul nome di una postazione o di un gruppo. Nel [menu di gestione](#) che si è aperto nella sezione **Generali** selezionare la voce **Grafici**.
2. Si apre una finestra che contiene i seguenti dati in forma grafica e tabellare:
 - **Attività di virus** — nel grafico viene visualizzato il numero totale di oggetti malevoli trovati all'interno di ciascun intervallo di tempo per tutte le postazioni e i gruppi selezionati.
 - **Le minacce più diffuse** — viene riportata una lista di dieci minacce trovate nel più grande numero di file. Nel grafico vengono visualizzati i dati numerici degli oggetti corrispondenti a una particolare minaccia.
 - **Classi delle minacce** — viene riportata la lista delle minacce in base alla classificazione degli oggetti malevoli. Il diagramma circolare mostra la percentuale di tutte le minacce rilevate.
 - **Azioni eseguite** — viene riportata la lista delle azioni eseguite sugli oggetti malevoli rilevati. Il diagramma circolare mostra la percentuale di tutte le azioni eseguite.
 - **Le postazioni più attaccate** — viene riportata la lista delle postazioni su cui sono state rilevate minacce alla sicurezza. Nella tabella viene visualizzato il numero totale di minacce per ciascuna postazione.
3. Per visualizzare le informazioni per un periodo predefinito, selezionare un intervallo di tempo dalla lista a cascata nella barra degli strumenti: report per un determinato giorno o mese. O è possibile impostare un intervallo di tempo arbitrario, per fare ciò, inserire le date richieste o selezionare le date dai calendari a discesa. Per visualizzare le informazioni, premere il pulsante **Aggiorna**.



Grafici e tabelle delle statistiche riepilogative

Nella voce **Grafici** della sezione **Generali** e in alcune voci della sezione **Statistiche** del menu di gestione vengono riportati i dati in forma grafica e tabellare. Nella tabella di seguito è riportata la lista dei grafici e delle tabelle possibili e delle relative sezioni del menu di gestione in cui vengono visualizzati questi elementi.

Tabella 8-6. Corrispondenza dei grafici e delle tabelle alle sezioni del menu di gestione

Grafici e tabelle	Sezioni
Attività di virus	Grafici
Le minacce più diffuse	Grafici Minacce Statistiche delle minacce
Classi delle minacce	Grafici Statistiche delle minacce
Le postazioni più attaccate	Grafici
Azioni eseguite	Grafici Minacce
Numero di errori per postazione	Errori
Numero di errori per componente	Errori
Minacce per componente	Avvio/Arresto
Errori per componente	Avvio/Arresto

- **Numero di errori per postazione** — viene riportata la lista delle postazioni su cui si verificavano errori di funzionamento dei componenti antivirus. Il grafico mostra il numero totale di errori per ciascuna postazione.
- **Numero di errori per componente** — viene riportata la lista dei componenti antivirus in cui si verificavano errori di funzionamento. Il diagramma circolare mostra la percentuale di errori di tutti i componenti.
- **Minacce per componente** — viene riportata la lista dei componenti antivirus che hanno rilevato minacce. Il grafico mostra il numero totale di minacce rilevate da ciascuno componente.
- **Errori per componente** — viene riportata la lista dei componenti antivirus in cui si verificavano errori di funzionamento. Il grafico mostra il numero totale di errori di ciascuno componente.



8.6.3. Identificatori di protezione

Per visualizzare informazioni sugli identificatori di protezione su postazioni

1. Selezionare la voce **Rete antivirus** nel menu principale del Pannello di controllo, nella finestra che si è aperta nella lista gerarchica fare clic sul nome di una postazione o di un gruppo. Nella sezione **Generali** del menu di gestione nella parte sinistra della finestra selezionare la voce **Identificatori di protezione**.
2. Si apre una finestra che contiene i seguenti dati:
 - **Identificatore** — identificatore della postazione univoco. Viene impostato durante la creazione dell'account postazione e in seguito non può essere modificato.
 - **Postazione** — nome della postazione. Viene impostato durante la creazione dell'account postazione e verrà automaticamente sostituito con il nome del computer dopo la connessione dell'Agent Dr.Web.
 - **Indirizzo** — indirizzo IP della postazione.
 - **Identificatori di protezione** — identificatore di protezione univoco (SID, security identifier) del computer. Il campo viene compilato automaticamente dopo la connessione al Server Dr.Web di una postazione con il sistema operativo Windows.
 - **Data dell'ultima connessione** — data dell'ultimo tentativo di connessione della postazione al Server Dr.Web.
3. Per visualizzare i dati per un periodo predefinito, selezionare un intervallo dalla lista a cascata nella barra degli strumenti: report per un determinato giorno o mese, quindi premere il pulsante **Aggiorna**. Per visualizzare i dati in un intervallo di date personalizzato, inserire le date richieste o selezionare le date dai calendari a cascata e premere il pulsante **Aggiorna**.

8.6.4. Quarantena

Contenuti della quarantena

File possono essere aggiunti alla quarantena da uno dei componenti antivirus, per esempio da Scanner.

L'utente può in autonomo scansionare nuovamente i file che si trovano in quarantena, utilizzano il Pannello di controllo o la Gestione quarantena sulla postazione.

Per visualizzare e modificare i contenuti della quarantena nel Pannello di controllo

1. Selezionare la voce **Rete antivirus** nel menu principale del Pannello di controllo, nella finestra che si è aperta nella lista gerarchica fare clic sul nome di una postazione o di un gruppo. Nel [menu di gestione](#) nella sezione **Generali** selezionare la voce **Quarantena**.
2. Si apre una finestra che contiene i dati tabulari sullo stato corrente della 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 contengono gli oggetti di quarantena separatamente per ciascuna postazione.





Le statistiche di scansione ripetuta di un oggetto in quarantena, riportate nella colonna **Informazioni**, tengono conto solo di una scansione ripetuta avviata attraverso il Pannello di controllo.

Se più di una minaccia sono spostate in quarantena, fare clic nella colonna **Informazioni** sul numero di oggetti spostati in quarantena per visualizzare l'intera lista delle minacce in una finestra popup.

Se per un oggetto in quarantena è dichiarato lo status **non è infetto**, questo significa che dopo lo spostamento in quarantena di un oggetto classificato come minaccia è stata eseguita una scansione ripetuta e all'oggetto è stato attribuito lo status oggetto sicuro.

Il ripristino di oggetti da quarantena viene effettuato solo manualmente.








3. Per visualizzare file spostati in quarantena per un determinato periodo, indicare un periodo relativamente al giorno odierno nella lista a cascata o impostare un intervallo di date nella barra degli strumenti. Per impostare un intervallo, inserire le date richieste o premere le icone del calendario accanto ai campi di date. Per visualizzare le informazioni, premere il pulsante **Aggiorna**.
4. Per modificare la visualizzazione dei dati, fare clic sull'icona  nell'intestazione della tabella:
 - Definire le impostazioni di visualizzazione delle righe (utile in caso di righe lunghe).
 - Selezionare quali colonne verranno visualizzate nella tabella.
5. Per filtrare i file di quarantena, premere il pulsante  nell'intestazione della tabella e configurare i seguenti parametri di filtraggio:
 - **Ricerca** — impostare una stringa arbitraria per la ricerca in tutte le sezioni della tabella. Nella tabella verranno visualizzate solo le righe che corrispondono ai risultati della ricerca.
 - **Spostato dal componente** — selezionare il componente di protezione Dr.Web che ha spostato i file in quarantena.
 - **Minaccia** — selezionare il nome della minaccia rilevata secondo la classificazione di Doctor Web.
 - **Nome originale** — inserire il nome originale dell'oggetto prima dello spostamento in quarantena.
 - **Dimensione del file, B** — tramite il pulsante a scorrimento impostare l'intervallo delle dimensioni in byte degli oggetti rilevati.

Premere il pulsante **Applica** per visualizzare i file di quarantena secondo i parametri di filtro impostati.




Premere il pulsante **Di default** per ripristinare tutte le impostazioni di filtraggio ai valori iniziali.



6. Per gestire i file in quarantena, spuntare un flag che corrisponde a un file, un gruppo di file o a tutti i file nella pagina aperta di quarantena (nell'intestazione della tabella). Nella barra degli strumenti selezionare una delle seguenti azioni:

Opzione	Descrizione
 Rimuovi i file	
	 Rimuovi i file selezionati Per rimuovere i file selezionati dalla quarantena e dal sistema.
	 Rimuovi tutti i file Per rimuovere dalla quarantena e dal sistema tutti i file che soddisfano i parametri di filtraggio selezionati, cioè tutti i file visualizzati nella finestra di quarantena.
 Esportazione Per copiare e salvare il file selezionato. Dopo lo spostamento dei file sospetti in quarantena locale sul computer dell'utente, è possibile copiare e salvare questi file attraverso il Pannello di controllo. Per esempio, per il successivo invio per l'analisi al laboratorio antivirus dell'azienda Doctor Web. Durante l'esportazione il file viene inserito all'interno di un archivio a cui viene assegnato un nome che corrisponde all'hash del file esportato. Oltre all'oggetto esportato, l'archivio contiene anche un file CSV con informazioni generali sull'oggetto. L'archivio di default è protetto dalla password <code>virus</code> .	
 Ripristina i file	
 Utilizzare la funzione di ripristino di file da quarantena solo se si è sicuri che un oggetto è innocuo.	
	 Ripristina i file selezionati Per ripristinare la posizione originale dei file selezionati nella finestra, cioè ripristinare i file nelle directory in cui erano prima dello spostamento in quarantena.



Opzione	Descrizione
	<p data-bbox="379 309 861 344"> Ripristina i file secondo i parametri</p> <p data-bbox="507 371 1236 407">Nella finestra che si è aperta definire le seguenti impostazioni:</p> <ul data-bbox="507 421 1444 1982" style="list-style-type: none"><li data-bbox="507 421 1444 1433">• Se è selezionato un oggetto:<ul data-bbox="545 465 1444 1433" style="list-style-type: none"><li data-bbox="545 465 1444 728">▫ Ripristina il file come — per ripristinare dalla quarantena il file selezionato e collocarlo nel percorso impostato e con il nome impostato. Nel campo Ripristina il file nel seguente percorso impostare il completo percorso su postazione in cui verrà ripristinato il file selezionato. Il nome del file deve essere obbligatoriamente impostato. Di default viene proposto il percorso e nome di file originale (quello prima dello spostamento). Se necessario, è possibile modificare questo parametro.<li data-bbox="545 745 1444 884">▫ Ripristina i file secondo il tipo di minaccia — per ripristinare dalla quarantena tutti i file cui è stato attribuito un tipo di minaccia uguale a quello del file selezionato. Il tipo di minaccia viene riportato nel campo Ripristina i file che contengono la seguente minaccia.<li data-bbox="545 902 1444 1164">▫ Ripristina i file in base al percorso — per ripristinare dalla quarantena tutti i file spostati da una determinata directory. Nel campo Ripristina tutti i file che sono stati spostati in quarantena dalla seguente directory impostare il percorso di una directory su postazione. Verranno ripristinati tutti i file spostati in Quarantena da questa directory. Di default viene proposto il percorso della directory in cui era il file selezionato. Se necessario, è possibile modificare questo parametro.<li data-bbox="507 1182 1444 1433">• Se sono selezionati diversi oggetti:<ul data-bbox="545 1227 1444 1433" style="list-style-type: none"><li data-bbox="545 1227 1444 1321">▫ Ripristina i file — per ripristinare la posizione originale dei file sul computer, cioè ripristinare i file nelle directory in cui si trovavano prima dello spostamento in Quarantena.<li data-bbox="545 1339 1444 1433">▫ Ripristina i file secondo il tipo di minaccia — per ripristinare dalla quarantena tutti i file cui sono stati attribuiti tipi di minaccia uguali a quelli dei file selezionati.<li data-bbox="507 1451 1444 1579">• Nella lista Ripristina sui seguenti oggetti selezionare i nodi della rete su cui l'oggetto selezionato verrà ripristinato da Quarantena: soltanto per la posizione su cui l'oggetto è stato rilevato o per gruppi custom selezionati nella lista proposta.<li data-bbox="507 1597 1444 1803">• Aggiungi le eccezioni come impostazioni individuali di SplDer Guard — per aggiungere gli oggetti selezionati alla lista delle eccezioni dalla scansione dal componente SplDer Guard. In tal caso, se i nodi della rete per cui verrà modificata la lista delle eccezioni ereditavano le impostazioni del componente SplDer Guard dai loro gruppi primari, per loro l'ereditarietà verrà interrotta e loro verranno assegnate le impostazioni individuali.<li data-bbox="507 1821 1444 1982">• Aggiungi le eccezioni come impostazioni individuali di Scanner Dr.Web — per aggiungere gli oggetti selezionati alla lista delle eccezioni dalla scansione dal componente Scanner Dr.Web. In tal caso, se i nodi della rete per cui verrà modificata la lista delle eccezioni ereditavano le impostazioni del componente Scanner Dr.Web dai loro gruppi primari, per loro



Opzione	Descrizione
	l'ereditarietà verrà interrotta e loro verranno assegnate le impostazioni individuali.
 Ripristina tutti i file	Per ripristinare la posizione originale di tutti i file nella finestra di quarantena, cioè ripristinare i file nelle directory in cui erano prima dello spostamento in quarantena.
 Scansiona i file	
 Scansiona i file selezionati	Per eseguire nuovamente una scansione dei file selezionati in quarantena.
 Scansiona tutti i file	Per eseguire nuovamente una scansione di tutti i file nella finestra di quarantena.



Su postazioni disconnesse la richiesta di ripristino e nuova scansione verrà inviata solo dopo che le postazioni si conatteranno al Server Dr.Web.

7. Esportare i dati sullo stato della 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.

8.6.5. Report di supporto tecnico

Raccolta di informazioni di sistema

1. Selezionare una postazione o un gruppo di postazioni per cui si vuole creare un report.
2. Nella scheda **Generali** nella barra degli strumenti selezionare la voce  **Crea il report per il supporto tecnico.**
3. Confermare l'avvio della creazione del report.



Dopo l'avvio della creazione dei report per la postazione o il gruppo di postazioni, l'icona  rimane attiva, tuttavia, per una postazione non è possibile avviare la creazione di più report contemporaneamente. Per un gruppo, se si fa nuovamente clic sull'icona, la creazione di un nuovo report verrà avviata solo per le postazioni su cui la raccolta del report precedente è stata completata o arrestata, le altre postazioni ignoreranno questo comando.

4. Per visualizzare lo stato del report, premere **Dettagli**. Se l'avvio della raccolta dei report è in esecuzione o differito, comparirà un messaggio con il link a una sezione con una tabella in cui viene visualizzato il processo di creazione dei report e i file dei report già pronti.

Visualizzazione dei report

Le informazioni sullo stato della raccolta dei report, nonché i file dei report già pronti sono disponibili in una tabella nella sezione **Rete antivirus > Generali > Report per il supporto tecnico**.



Nella tabella possono essere conservati diversi report per una stessa postazione.

La tabella contiene i seguenti dati:

- **Identificatore** — ID della postazione.
- **Postazione** — nome della postazione.
- **Indirizzo della postazione** — quello di default.
- **Nome del report** — nome del file del report.
- **Hash SHA-256** — hash SHA-256 del file del report.
- **Avanzamento** — avanzamento dell'esecuzione del compito (creazione del report) in percentuale.
- **Stato** — stato della raccolta (**Creazione in corso/Download in corso/Pronto/Errore**).
- **Errori** — messaggio di errore.
- **Ora di inizio** — ora di inizio della raccolta.
- **Ora di fine** — ora di fine della raccolta.

I pulsanti sopra la tabella consentono di avviare o annullare la creazione del report, rimuovere i report arrestati o già pronti dal server (sulla postazione i report non vengono conservati) o scaricare i report.



Nella tabella non viene conservato lo stato per i report differiti (quando Agent Dr.Web non ha ancora inviato informazioni sullo stato) o i report di postazioni che non supportano questa funzione.



8.7. Invio dei file di installazione

Quando viene creato un nuovo account di postazione, nel Pannello di controllo viene generato un pacchetto di installazione di Agent Dr.Web individuale. Il pacchetto di installazione include l'installer di Agent Dr.Web e un set di parametri di connessione al Server Dr.Web e di autenticazione della postazione sul Server Dr.Web (il pacchetto di installazione e il relativo processo di installazione di Agent Dr.Web sono descritti in **Guida all'installazione**, sezione [Installazione locale di Agent Dr.Web](#)).

Dopo aver creato i pacchetti di installazione, per la comodità della loro distribuzione, si possono inviare pacchetti di installazione specifici sugli indirizzi email degli utenti.

Quando i pacchetti di installazione vengono inviati via email, i contenuti dell'email vengono formati nel seguente modo:



1. Nelle impostazioni sono vietati gli allegati (è selezionato il flag **Invia solo un link**, v. sotto): nell'email vengono inviati solo i link per il download dei pacchetti.
2. Il sistema operativo della postazione è conosciuto (gli allegati sono consentiti):
 - a) SO Windows: all'email viene allegato il pacchetto di installazione di Agent Dr.Web per Windows.
 - b) Linux, macOS, Android: vengono allegati all'email il file di 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.
3. Il sistema operativo della postazione non è conosciuto — un nuovo account di postazione, l'Agent Dr.Web non è ancora installato (gli allegati sono consentiti):
 - a) Se sul Server Dr.Web non ci sono pacchetti per le postazioni Linux, macOS, Android (in particolare, sul Server Dr.Web non sono caricati i **Prodotti aziendali Dr.Web**): vengono allegati all'email il pacchetto di installazione di Agent Dr.Web per Windows, nonché il file di configurazione con le impostazioni per la connessione al Server Dr.Web per le postazioni Linux, macOS, Android.
 - b) Se sul Server Dr.Web c'è almeno un pacchetto oltre al pacchetto per le postazioni SO Windows: vengono allegati all'email il pacchetto di installazione di Agent Dr.Web per Windows, il file di configurazione con le impostazioni per la connessione al Server Dr.Web per le postazioni Linux, macOS, Android, nonché un link al download dei file di installazione per le postazioni Linux, macOS, Android.

Per distribuire i pacchetti di 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 di installazione generato per questa postazione.
 - selezionare un gruppo di postazioni per inviare via email i pacchetti di installazione generati per le postazioni di questo gruppo.



Per selezionare più oggetti alla volta, utilizzare i tasti CTRL o MAIUSCOLO.

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 **Generali**:
 - Spuntare il flag **Comprimi in archivio zip** per comprimere i file dei pacchetti di installazione in un archivio zip. La compressione in archivio può essere utile se sul lato utente ci sono filtri email che bloccano la trasmissione di file eseguibili in allegati ai messaggi email.
 - Spuntare il flag **Invia solo un link** per inviare in un'email solo un link per il download del pacchetto. Il file stesso del pacchetto di installazione non verrà allegato all'email. Questa opzione può essere utile se il server di posta del cliente elimina automaticamente gli allegati dai messaggi email.
 - Nella sezione **Indirizzi e-mail dei destinatari** impostare l'indirizzo email su cui verrà inviato il pacchetto di installazione. Se sono state selezionate diverse postazioni o gruppi, impostare per ciascuna postazione separatamente di fronte al nome di questa postazione gli indirizzi email per l'invio del pacchetto di installazione.



I parametri di invio di email vengono configurati nel menu **Amministrazione**, nella sezione **Configurazione del Server Dr.Web**, nella scheda **Rete**, nella scheda interna [E-mail](#).

4. Premere il pulsante **Invia**.

8.8. Invio di messaggi alle postazioni

L'amministratore di sistema può inviare agli utenti messaggi informativi con qualsiasi contenuto che includono:

- testo del messaggio;
- link alle risorse Internet;
- logo aziendale (o qualsiasi immagine grafica).

Nell'intestazione della finestra inoltre viene indicata la data precisa di ricezione del messaggio.

Tali messaggi vengono visualizzati sul lato utente come finestre pop-up (vedi [immagine 8-1](#)).

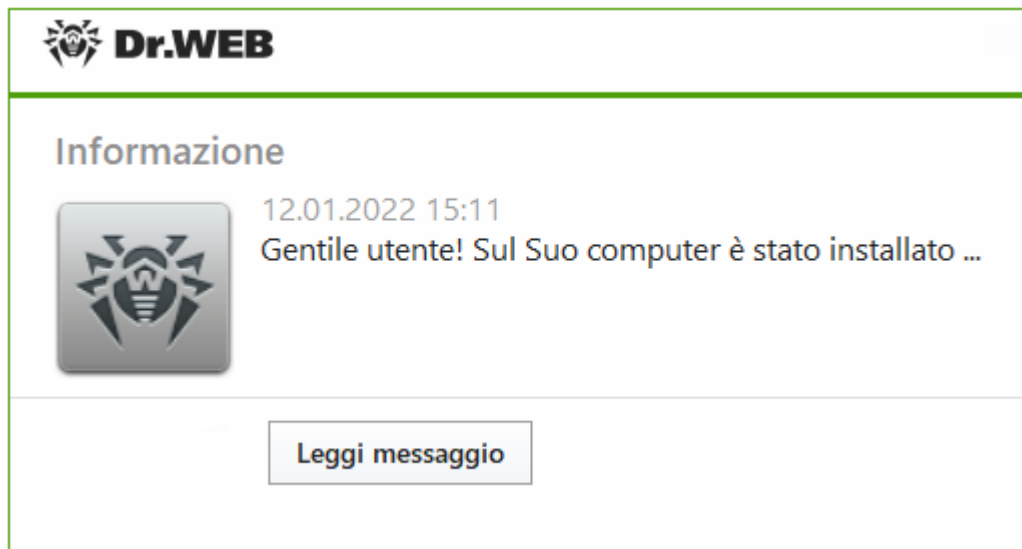


Immagine 8-1. Una finestra di messaggio su una postazione SO Windows

Per inviare il messaggio all'utente

1. Selezionare la voce **Rete antivirus** nel 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 messaggio su postazioni**.
3. Nella finestra che si è aperta, riempire i seguenti campi:
 - 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.
 - **Testo del messaggio** — campo obbligatorio.
 - 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:
 - A destra del campo **File del logo** premere il pulsante  per caricare il file di logo da risorsa locale e selezionare l'oggetto desiderato in esplora risorse di file system (v. [Formato del file di logo](#)).
 - Spuntare il flag **Mostra link nel messaggio** per includere nel messaggio un link a risorse web.

Per aggiungere un link:

- a) Nel campo **Nome del link** indicare il nome del link — il testo che verrà visualizzato nella posizione del link nel messaggio.
- b) Nel campo **Indirizzo URL per il link** impostare l'indirizzo URL della pagina web che si apre quando si fa clic sul link.
- c) Nel campo **Testo del messaggio** aggiungere il marcatore `{link}` ovunque sia necessario aggiungere il link. Nel messaggio risultante, nella sua posizione viene inserito il link con i parametri indicati. Il numero di tag `{link}` nel testo non è



limitato, ma tutti essi conterranno gli stessi parametri dai campi **Indirizzo URL per il link** e **Nome del link**. Se sono presenti uno o più marcatori {link}, il link verrà inserito solo nelle posizioni dei marcatori.

d) Se il marcatore {link} non è indicato nel campo **Testo del messaggio**, il link verrà inserito una volta alla fine del messaggio in una riga separata.

- 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 di 72x72 pixel. Le immagini di altre dimensioni verranno ridimensionate all'invio 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 un messaggio all'utente (soprattutto a molteplici indirizzi), si consiglia di inviarlo preliminarmente a qualsiasi computer con l'Agent Dr.Web installato per controllare la correttezza del risultato.



Esempio di invio di un messaggio

Per inviare il messaggio riportato nella [immagine 8-1](#), sono stati impostati i seguenti parametri:

Testo del messaggio:

Gentile utente!

Sul suo computer è stato installato il componente Firewall Dr.Web.

Le informazioni dettagliate sulle funzionalità di questo componente possono essere ottenute {link}.

Cordiali saluti,

Amministrazione

Indirizzo URL per il link: <http://drweb.com/>

Nome del link: qui



Capitolo 9. Gestione delle postazioni in ambienti virtuali

Dr.Web Enterprise Security Suite può essere utilizzato per la protezione dell'infrastruttura virtuale — cluster di macchine virtuali che forniscono servizi a clienti (qui di seguito denominati *MV client*): hosting virtuale, sistema di postazioni di lavoro remote, cloud aziendali ecc.

Una o più macchine virtuali del cluster ottengono il ruolo di quelle *di servizio*; su di esse viene installato un software specializzato (Server di scansione Dr.Web) tramite cui esse elaborano le richieste di scansione antivirus provenienti dalle macchine virtuali client.

Server di scansione include:

- motore di scansione che controlla i dati ricevuti per la presenza di minacce;
- database dei virus e database dei filtri incorporati per Office control.

Sulle MV client viene installato Agent virtuale Dr.Web il quale funziona sotto la gestione di Server Dr.Web e trasmette alla MV di servizio le richieste di scansione, nonché i file stessi da controllare. Tale schema di funzionamento riduce significativamente il carico sulle macchine virtuali client grazie ai seguenti fattori:

- la scansione è spostata al di fuori delle MV client;
- è assente la necessità di mantenere aggiornati i database dei virus e i database dei filtri incorporati su ciascuna delle MV client.

La configurazione con Server di scansione consente di:

- risparmiare memoria operativa;
- ridurre il carico sul sottosistema disco delle macchine virtuali;
- ridurre il carico sulla rete.

L'approccio utilizzato comporterà a un elevato carico del processore. Le configurazioni con Server di scansione sono le più efficaci in caso di collocamento della rete virtuale nei limiti di un singolo server fisico. L'utilizzo di una rete virtuale (invece di quella fisica) per il trasferimento di dati tra le MV situate sullo stesso server (hypervisor) può assicurare un'alta velocità di scambio di dati e un'alta velocità di scansione.

Server di scansione può essere parte di qualsiasi gruppo. È anche possibile unire i Server di scansione in un gruppo separato, tra l'altro anche automaticamente in base alle [regole di appartenenza impostate](#).



L'aggiunta di Server di scansione a gruppi e la configurazione delle regole di appartenenza vengono effettuate allo stesso modo che per tutte le altre postazioni. Le informazioni dettagliate sulla gestione dei gruppi sono contenute nella sezione [Inserimento delle postazioni in gruppi](#).

Le postazioni interagiscono con Server di scansione tramite un Agent Dr.Web che funziona in modalità virtuale (Agent virtuale Dr.Web). L'Agent Dr.Web funziona sotto la gestione di Server



Dr.Web e trasmette le richieste di scansione di file e URL a Server di scansione. Passando alla modalità virtuale, l'Agent Dr.Web smette di utilizzare i database dei virus, e senza connessione a Server di scansione rimane senza protezione. Pertanto, gli Agent virtuali non possono essere utilizzati senza installare e configurare un Server di scansione.

9.1. Connessione delle postazioni a Server di scansione

Server di scansione — macchina virtuale che ha uno stato speciale e su cui è installato un software specializzato per l'elaborazione delle richieste di scansione antivirus provenienti dalle altre macchine virtuali.

Per informazioni dettagliate sull'installazione e la configurazione iniziale di Server di scansione v. **Guida all'installazione**, p. [Installazione di Server di scansione Dr.Web.](#)








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

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



La possibilità di connettere postazioni a Server di scansione è disponibile solo se è prevista dalle condizioni della licenza in uso.

Per connettere una postazione al Server di scansione

1. Selezionare la voce **Rete antivirus** (icona ) nel menu principale del Pannello di controllo.
2. Nell'albero della rete antivirus selezionare una postazione (icona  o  se la postazione è spenta) o un gruppo di postazioni (icona ) che si vogliono connettere a Server di scansione (icona ). Le postazioni connesse a Server di scansione sono presentate nell'albero come elementi nidificati.
3. Nella sezione **Configurazione** selezionare **Agent virtuale**.
4. Spuntare il flag **Utilizza Server di scansione** e indicare l'indirizzo di Server di scansione nel campo **Indirizzo di rete del Server di scansione**.



Per un solo Agent virtuale può essere indicato l'indirizzo di un solo Server di scansione.

Se non è necessario indicare un indirizzo specifico, utilizzare l'impostazione di default `udp://:18008` — in questo caso il Server di scansione verrà determinato automaticamente indipendentemente dall'indirizzo ad esso assegnato — IPv4 o IPv6.



L'indirizzo può essere indicato in uno dei seguenti formati:

- `tcp://<indirizzo_IP>:<porta>` (è possibile indicare sia gli indirizzi IPv4 che quelli IPv6; l'indirizzo IPv6 viene indicato tra parentesi quadre, per esempio `tcp://[fd15:4ba5:5a2b:1008:edc8:733e:1dd7:789c]:7777`);
- `udp://:<porta>` (in questo formato vengono indicati solo il protocollo e la porta su cui le postazioni cercheranno Server di scansione);
- `srv://service@<domain>` (l'indirizzo e la porta del server di servizio vengono determinati tramite la ricerca del record SRV del dominio DNS `<domain>`; se il dominio non è indicato, verrà preso dal file di configurazione DNS dal campo `search` o `domain` — dipende da quale di essi viene per ultimo nel file di configurazione).

5. Premere il pulsante **Salva**.

Permessi

Per gli utenti delle postazioni con SO della famiglia UNIX sono disponibili i seguenti permessi:

- avvio di Server di scansione,
- interruzione del funzionamento di Server di scansione,
- modifica della configurazione di Server di scansione.

Di default è concesso solo il permesso di avvio di Server di scansione.

Il set di permessi concessi, se necessario, può essere modificato dall'amministratore della rete antivirus. Per maggiori informazioni sui permessi v. sezione [Permessi dell'utente della postazione](#).

Impostazioni aggiuntive

Sia su Server di scansione che sulle postazioni con SO UNIX ad esso connesse possono essere definite le impostazioni aggiuntive che vengono indicate nel file di configurazione `drweb.ini` (sezione `[MeshD]`). Modifiche al file `drweb.ini` possono essere apportate attraverso il Pannello di controllo (nelle impostazioni della postazione selezionare **UNIX** → **Agent Dr.Web** → **Configurazione**).

La descrizione dettagliata di queste impostazioni è riportata nella tabella seguente.



Per le postazioni con SO Windows può essere impostato solo l'indirizzo di Server di scansione. Tutte le altre impostazioni descritte nella tabella non sono supportate.

Parametro	Descrizione
<code>LogLevel</code> <i>{livello di dettaglio}</i>	Livello di dettaglio del log. Può assumere uno dei seguenti valori:



Parametro	Descrizione
	<ul style="list-style-type: none">• <code>DEBUG</code> — il livello più dettagliato (di debug). Vengono registrati tutti i messaggi, nonché le informazioni di debug.• <code>INFO</code> — vengono registrati tutti i messaggi.• <code>NOTICE</code> — vengono registrati i messaggi di errore, le avvertenze, gli avvisi.• <code>WARNING</code> — vengono registrati i messaggi di errore e le avvertenze.• <code>ERROR</code> — vengono registrati solo i messaggi di errore. <p>Il valore di default è: <code>Notice</code></p>
<code>Log</code> <i>{tipo di log}</i>	<p>Metodo di registrazione del log. Può assumere uno dei seguenti valori:</p> <ul style="list-style-type: none">• <code>Stderr[:ShowTimestamp]</code> — i messaggi verranno registrati nel flusso di errori standard <code>stderr</code>.• <code>Auto</code> — i messaggi da salvare nel log vengono passati al daemon di gestione della configurazione <code>Dr.Web ConfigD</code> sulla postazione, il quale li salva in un unico luogo secondo le proprie impostazioni.• <code>Syslog[:<facility>]</code> — i messaggi verranno trasmessi dal componente al servizio di registrazione del log di sistema <code>syslog</code>.• L'opzione aggiuntiva <code><facility></code> viene utilizzata per specificare il tipo di log in cui <code>syslog</code> salverà i messaggi. I valori possibili sono:<ul style="list-style-type: none">▫ <code>DAEMON</code> — messaggi dei daemon;▫ <code>USER</code> — messaggi dei processi utente;▫ <code>MAIL</code> — messaggi dei programmi di posta;▫ <code>LOCAL0</code> — messaggi dei processi locali 0;...▫ <code>LOCAL7</code> — messaggi dei processi locali 7.▫ <code><percorso></code> — i messaggi verranno salvati direttamente nel file di log su postazione specificato. <p>Il valore di default è: <code>Auto</code></p>
<code>IdleTimeLimit</code> <i>{intervallo di tempo}</i>	<p>Tempo massimo di inattività di Agent virtuale o di Server di scansione trascorso il quale esso finisce di funzionare.</p> <p>Il parametro può essere impostato sia su Server di scansione che su Agent virtuale.</p>



Parametro	Descrizione
	<p>Se è impostato il valore <code>None</code>, Agent virtuale/Server di scansione sarà in continua esecuzione; nel caso di assenza dell'attività ad esso non verrà inviato il segnale <code>SIGTERM</code>.</p> <p>Il valore minimo è 10s.</p> <p>Il valore di default è: 30s</p>
<code>DebugSsh</code> <i>{logico}</i>	<p>Indica se è necessario registrare nel log i messaggi del protocollo SSH sulla postazione se è impostato il livello di dettaglio del log <code>LogLevel = Debug</code>.</p> <p>Il valore di default è: No</p>
<code>ListenAddress</code> <i>{<indirizzo_IP>:<porta>}</i>	<p>Socket di rete (indirizzo e porta) della connessione client su cui Server di scansione è in attesa di connessioni dalle postazioni client.</p> <p>Il parametro può essere impostato solo su Server di scansione.</p> <p>Il parametro deve essere obbligatoriamente impostato affinché Server di scansione sia in ascolto sull'interfaccia IPv6 e possa rilevare Agent virtuali tramite IPv6.</p> <p>Gli indirizzi IPv6 vengono indicati tra parentesi quadre.</p> <p>Se come valore di questo parametro è indicata una stringa vuota, Server di scansione finisce di funzionare.</p> <p>Per attribuire a questo parametro il valore '' (cioè stringa vuota), è necessario possedere contemporaneamente i permessi di arresto e di modifica della configurazione di Server di scansione</p>
<code>DnsResolverConfPath</code> <i>{percorso}</i>	<p>Percorso del file di configurazione del sottosistema per la risoluzione dei nomi a dominio (DNS resolver).</p> <p>Il parametro viene impostato per Agent virtuale se come indirizzo di Server di scansione è impostato un record SRV.</p> <p>Il valore di default è: <code>/etc/resolv.conf</code></p>
<code>DiscoveryResponderPort</code> <i>{porta}</i>	<p>Porta su cui Server di scansione risponde alle richieste dei client tramite il protocollo UDP.</p> <p>Il valore di default è: 18008</p>
<code>EngineChannel</code> <i>{On Off}</i>	<p>Attivazione o disattivazione della possibilità da parte di server di fornire i servizi di motore di scansione.</p> <p>Il parametro può essere impostato solo su Server di scansione.</p> <p>Il valore di default è: On</p>



Parametro	Descrizione
	Per cambiare il valore di questo parametro in <code>Off</code> , è necessario possedere contemporaneamente i permessi di arresto e di modifica della configurazione di Server di scansione.
EngineUplink {indirizzo}	Indirizzo di Server di scansione (viene indicato nello stesso formato della configurazione attraverso il Pannello di controllo). Il parametro può essere impostato solo su Agent virtuale. Il valore di default è: <i>Non impostato</i>
EngineDebugIpc {logico}	Registra nel log le informazioni di debug per il servizio di scansione se è impostato il livello di dettaglio del log <code>LogLevel = Debug</code> . Il valore di default è: <code>No</code>
UrlChannel {On Off}	Attivazione o disattivazione della possibilità da parte di server di fornire i servizi di controllo URL. Il valore di default è: <code>On</code> Per cambiare il valore di questo parametro in <code>Off</code> , è necessario possedere contemporaneamente i permessi di arresto e di modifica della configurazione di Server di scansione.
UrlUplink {indirizzo}	Indirizzo del nodo superiore utilizzato per il controllo URL. Il parametro può essere impostato solo su Agent virtuale. Il valore di default è: <i>Non impostato</i>
UrlDebugIpc {logico}	Registra nel log le informazioni di debug per il servizio di controllo URL se è impostato il livello di dettaglio del log <code>LogLevel = Debug</code> . Il valore di default è: <code>No</code>



Maggiori informazioni sulla configurazione dei parametri di Server di scansione e di Agent virtuali sono riportate in **Manuali dell'amministratore Dr.Web per UNIX**, sezione **Dr.Web MeshD**.

9.2. Integrazione con l'infrastruttura dei desktop virtuali

Dr.Web Enterprise Security Suite supporta l'integrazione con l'infrastruttura dei desktop virtuali (VDI). Questa possibilità è utile quando si utilizzano *thin client* che supportano il funzionamento in modalità terminale tramite il protocollo RDP.



Il funzionamento della rete antivirus in tale caso viene organizzato come segue:

1. L'amministratore della rete antivirus crea *un'immagine modello della postazione virtuale* con il software e l'Agent Dr.Web preinstallati, dopodiché connette il modello al Server Dr.Web.
2. Dal modello creato vengono clonate le postazioni virtuali necessarie.
3. Dopo il periodo impostato le postazioni virtuali vengono rimosse. In seguito le postazioni virtuali vengono create nuovamente dall'immagine modello secondo necessità.

Per preparare la rete antivirus per l'utilizzo della VDI

1. Selezionare la voce **Rete antivirus** nel menu principale del Pannello di controllo e creare una nuova postazione che fungerà da immagine modello.
2. Installare sulla postazione creata Agent Dr.Web e tutto il software necessario. [Connettere la postazione](#) al Server Dr.Web.
3. Nominare una delle postazioni Server di scansione e [installare il software necessario su di essa](#).
4. Nelle impostazioni delle postazioni create indicare che esse devono utilizzare [Server di scansione](#). Indicare l'indirizzo del Server di scansione a cui si conetteranno le postazioni.
5. Nella stessa sezione [creare un nuovo gruppo](#) in cui saranno collocate le postazioni virtuali.
6. Configurare il procedimento di registrazione delle postazioni virtuali. Andare alla sezione **Amministrazione** → [Procedure personalizzate](#). Aggiungere una nuova procedura basata sull'evento **Nuovo arrivo si connette al Server Dr.Web**. Nel campo **Testo della procedura personalizzata** indicare:

```
local args = ... -- args.id, args.address, args.station

if args.id == '<identificatore_postazione_modello>' then

    return { "id", dwcore.get_uuid(), "pgroup", "<identificatore_gruppo_primario>" }

end
```

Come *<identificatore_postazione_modello>* è necessario indicare l'ID della postazione modello creata nel [passaggio 1](#). Come *<identificatore_gruppo_primario>* indicare l'ID del gruppo creato nel [passaggio 5](#). Queste informazioni sono sempre disponibili nelle proprietà degli oggetti nell'albero della **Rete antivirus**.

Alla clonazione ciascuna nuova postazione virtuale riceverà un identificatore che coincide con l'identificatore della postazione modello. Secondo le condizioni della procedura, quando la postazione viene connessa al Server Dr.Web, per essa viene generato un nuovo UUID, dopodiché la postazione viene registrata nel gruppo primario con l'identificatore specificato.

Quando si scrive la procedura, si consiglia di consultare il modello di procedura incorporato **Nuovo arrivo si connette al Server Dr.Web**. Per verificare le informazioni, inclusi i possibili parametri alternativi e i valori di ritorno, nel Pannello di controllo nell'albero delle procedure




personalizzate selezionare **Examples of the hooks** → **Nuovi arrivi** → **Nuovo arrivo si connette al Server Dr.Web.**

Rimozione pianificata delle postazioni virtuali inattive

Per una distribuzione razionale delle licenze, nonché per prevenire l'accumulo di informazioni sulle postazioni virtuali rimosse nel database, è necessario configurare un task di rimozione automatica delle postazioni inattive. Per postazioni inattive si intendono le postazioni che non si connettevano al Server Dr.Web durante il periodo specificato.

Per preparare un task di rimozione automatica delle postazioni inattive

1. Nel Pannello di controllo andare alla sezione **Amministrazione** → **Scheduler di Server Dr.Web.**
2. Creare un nuovo task premendo il pulsante  **Crea task** nella barra degli strumenti.



3. Nella scheda **Azione** dalla lista a cascata selezionare **Esecuzione dello script**, dopodiché importare da un file separato o inserire manualmente il seguente script Lua nel campo sottostante:

```
local adminName = 'admin'
-- indichiamo l'ID del gruppo
local gid      = '<identificatore_gruppo_primario>'
-- impostiamo il periodo di inattività (in secondi)
local interval = 86400

require('st-db-state')
require('core/datetime')
require('core/admins/admins')

local lastseen = Datetime.timeUnixstampToDBFormat(Datetime.nowTimestamp()
- interval)

local stations = {}
-- eseguiamo una query al database
local res, err1 = DBuilder()
    :select('id, lastseenat')
    :from('stations')
    :where('gid', gid)
    :where('lastseenat '..dwcore.base64_decode('PA=='), lastseen)
    :where('state !=', st_db_state.st_db_state_logged_in)
    :get()

if res and next(res) then
    for i = 1, #res do
        table.insert(stations, res[i][1])
    end
end

-- rimuoviamo le postazioni inattive
local function delete_stations(ids)
    local admin, err = Admin:initWithLogin(adminName)
    require 'core/admins/admins'
    require('core/stations/stations')
    local status, results_stations = Stations:delete(ids, admin)
    return ''
end

return delete_stations(stations)
```

Come <identificatore_gruppo_primario> indicare l'ID del gruppo creato nel [passaggio 5](#) della preparazione per l'utilizzo della VDI.



Questo script accede al database, ottiene gli ID delle postazioni che non si connettevano al Server Dr.Web nelle ultime 24 ore (86400 secondi) e rimuove queste postazioni dal gruppo con l'ID specificato.



Si consiglia di aggiornare l'immagine modello ogni volta che viene effettuato un aggiornamento dei componenti antivirus che richiede il riavvio del sistema operativo. Dopo l'aggiornamento controllare e, se necessario, correggere l'identificatore della postazione modello nel testo della procedura.



Capitolo 10: Configurazione del Server Dr.Web

In questo capitolo vengono descritte le seguenti possibilità di gestione dei parametri di funzionamento della rete antivirus e del Server Dr.Web:

- [Gestione delle licenze](#) — parametri delle licenze;
- [Logging](#) — visualizzazione e gestione dei log di funzionamento del Server Dr.Web, visualizzazione di statistiche dettagliate sul funzionamento del Server Dr.Web;
- [Configurazione del Server Dr.Web](#) — configurazione dei parametri di funzionamento del Server Dr.Web;
- [Configurazione del calendario di Server Dr.Web](#) — configurazione di un calendario di task per la manutenzione del Server Dr.Web;
- [Configurazione del web server](#) — per configurare i parametri di funzionamento del web server;
- [Procedure personalizzate](#) — per connettere e configurare procedure personalizzate;
- [Configurazione degli avvisi](#) — per configurare il sistema di avviso dell'amministratore sugli eventi della rete antivirus con diversi modi di consegna dei 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 la successiva distribuzione degli aggiornamenti su postazioni;
- [Gestione del database](#) — manutenzione diretta del database di Server Dr.Web;
- [Caratteristiche di una rete con diversi Server Dr.Web](#) — per configurare una rete antivirus con diversi server e le reazioni tra i server;
- [Integrazione con l'infrastruttura dei desktop virtuali](#) — configurazione del Server Dr.Web per il funzionamento con l'infrastruttura di desktop virtuali (VDI).

10.1. Gestione delle licenze

10.1.1. Gestione licenze



Per maggiori informazioni circa i principi e le caratteristiche della concessione delle licenze Dr.Web Enterprise Security Suite consultare la sezione [Concessione delle licenze](#).

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 nel [menu di gestione](#) selezionare la voce **Gestione licenze**.


Lista gerarchica delle chiavi

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

La barra degli strumenti contiene i seguenti elementi di gestione:

Opzione	Descrizione	A seconda degli oggetti nell'albero delle chiavi
 Aggiungi chiave di licenza	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, gruppo o criterio) o una chiave di licenza.
 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.	
 Controlla disponibilità degli aggiornamenti e sostituisci chiavi di licenza	Controlla la disponibilità degli aggiornamenti su SAM per tutte le chiavi. Se sono disponibili gli aggiornamenti, scarica le chiavi ed effettua la sostituzione (v. Aggiornamento automatico delle licenze).	L'opzione è sempre disponibile. L'azione si applica a tutte le chiavi di licenza nell'albero.
 Propaga la chiave verso i Server Dr.Web adiacenti	Per trasferire licenze dalla chiave selezionata ai Server Dr.Web adiacenti.	L'opzione è disponibile se nell'albero è selezionata una chiave di licenza.



 **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 di licenza.
- 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, postazioni e criteri a cui queste chiavi sono state assegnate. Questa vista ad albero è la principale 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 gruppi contenenti gli oggetti a cui sono state assegnate direttamente le chiavi di licenza. Elementi nidificati dei gruppi sono le postazioni e i criteri inclusi in questi gruppi e le chiavi di licenza assegnate a questi oggetti. Questa vista ad albero si utilizza per visualizzare informazioni sulle licenze in un modo più comodo e non consente di gestire gli oggetti dell'albero.
- Per modificare l'aspetto dell'albero, utilizzare le seguenti opzioni:
 - **Mostra identificatori dei client** — attiva/disattiva la visualizzazione degli identificatori delle postazioni univoci.
 - **Mostra nomi dei client** — attiva/disattiva la visualizzazione dei nomi delle postazioni.
 - **Mostra indirizzi dei client** — attiva/disattiva la visualizzazione degli indirizzi IP delle postazioni.
 - **Mostra descrizioni** — attiva/disattiva la visualizzazione delle descrizioni delle postazioni e dei gruppi di postazioni.

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 Dr.Web adiacente.](#)
8. [Modificare le licenze trasferite su un Server Dr.Web adiacente.](#)



Visualizzare le informazioni sulla licenza

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

- Il numero di licenze concesse e utilizzate da questo file della chiave di licenza.
- Utente della licenza.
- Venditore da cui è stata acquistata la licenza.
- Identificatore e numero di serie della licenza.
- Data di scadenza della licenza.
- Viene indicato se la licenza comprende il supporto del modulo Antispam.
- Hash MD5 della chiave di licenza.
- Liste consentite dei bollettini degli hash per l'informazione sull'appartenenza delle minacce rilevate. Se le funzionalità non sono concesse in licenza, questo parametro è assente.




L'assenza della licenza per i bollettini degli hash non riduce il livello di protezione antivirus. Questa licenza consente di aggiungere un avviso all'amministratore su quello che la minaccia rilevata è presente nei bollettini specializzati degli hash di minacce conosciuti.

- Lista dei componenti antivirus che questa 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 di licenza** nella barra degli strumenti.
2. Nel pannello che si è aperto, fare clic sul pulsante  e selezionare un file della chiave di licenza.
3. Spuntare il flag:
 - **Assegna chiave di licenza al gruppo Everyone**, se questa è la prima chiave di licenza nella rete antivirus. La chiave che viene aggiunta verrà automaticamente assegnata al gruppo **Everyone**.
 - **Sostituisci la chiave di licenza del gruppo Everyone**, se questa non è la prima chiave di licenza nella rete antivirus. La chiave di licenza corrente del gruppo **Everyone** verrà sostituita con la chiave di licenza che viene aggiunta.



Se al gruppo **Everyone** sono assegnate più chiavi di licenza, verrà sostituita la prima chiave nella lista.

Se si vuole sostituire una determinata chiave di licenza del gruppo **Everyone**, utilizzare la procedura [Aggiornare una chiave di licenza](#).

4. Premere il pulsante **Salva**.
5. La chiave di licenza verrà aggiunta all'albero delle chiavi.


Se al passaggio 3 non è stato selezionato il flag corrispondente, la chiave di licenza aggiunta non verrà associata a nessuno degli oggetti. In questo caso per impostare gli oggetti di licenza, eseguire le procedure personalizzate [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 di Gestione licenze nell'albero delle chiavi selezionare la chiave che si vuole assegnare a un oggetto di licenza: gruppo di postazioni, postazione o criterio.
2. Nella barra degli strumenti fare clic sul pulsante  **Propaga la chiave verso i gruppi e le postazioni**. Si apre una finestra con la lista gerarchica della rete antivirus.



3. Selezionare gli oggetti di licenza dalla lista. Per selezionare più oggetti, utilizzare i tasti CTRL e MAIUSCOLO.



Per assegnare una chiave a un criterio, è necessario selezionare il criterio stesso o la versione corrente di questo criterio (una chiave viene automaticamente assegnata a un criterio quando si seleziona la sua versione corrente e viceversa).

Una chiave di licenza può anche essere assegnata a qualsiasi versione di un criterio, che non è corrente. In questo caso, la chiave verrà assegnata solo a questa versione e non al criterio stesso. Tale chiave non verrà applicata alle postazioni fino a quando la versione corrente del criterio non verrà sostituita con quella a cui è assegnata questa chiave.


Una chiave di licenza deve essere assegnata direttamente a criteri o alle loro versioni.

4. Fare clic sul pulsante **Sostituisci chiave di licenza**. 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 alla lista delle chiavi di licenza dell'oggetto

1. Nella finestra principale di Gestione licenze nell'albero delle chiavi selezionare la chiave che si vuole aggiungere all'elenco delle chiavi dell'oggetto: gruppo di postazioni, postazione o criterio.
2. Nella barra degli strumenti fare clic sul pulsante  **Propaga la chiave verso i gruppi e le postazioni**. Si apre una finestra con la lista gerarchica della rete antivirus.
3. Selezionare gli oggetti di licenza dalla lista. Per selezionare più oggetti, utilizzare i tasti CTRL e MAIUSCOLO.



Per assegnare una chiave a un criterio, è necessario selezionare il criterio stesso o la versione corrente di questo criterio (una chiave viene automaticamente assegnata a un criterio quando si seleziona la sua versione corrente e viceversa).

Una chiave di licenza può anche essere assegnata a qualsiasi versione di un criterio, che non è corrente. In questo caso, la chiave verrà assegnata solo a questa versione e non al criterio stesso. Tale chiave non verrà applicata alle postazioni fino a quando la versione corrente del criterio non verrà sostituita con quella a cui è assegnata questa chiave.

Una chiave di licenza deve essere assegnata direttamente a criteri o alle loro versioni.

4. Fare clic sul pulsante **Aggiungi chiave di licenza**. 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 i criteri assegnati a postazioni che non hanno impostazioni individuali della chiave di licenza è necessario impostare una chiave di licenza.


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

1. Nella finestra principale di Gestione licenze selezionare la chiave di licenza che si vuole cancellare o selezionare l'oggetto (postazione, gruppo o criterio) a cui è assegnata questa chiave e fare clic sul pulsante  **Rimuovi gli oggetti selezionati** nella barra degli strumenti. Tenere presente che:
 - Se sono stati selezionati un gruppo o una postazione, vengono cancellati dalla lista degli oggetti a cui è assegnata questa chiave. Per il gruppo o la postazione per cui viene rimossa una chiave impostata come individuale, viene impostata l'ereditarietà della chiave di licenza.
 - Se è stato selezionato un criterio, dalla lista degli oggetti a cui è assegnata la chiave di licenza viene inoltre cancellata la versione corrente del criterio. Se è stata selezionata la versione corrente di un criterio, anche il criterio stesso verrà eliminato. Tuttavia, quando viene eliminata una versione di un criterio che non è corrente, il criterio stesso e la sua versione corrente non verranno eliminati.
 - Se è stata selezionata una chiave di licenza, l'account della chiave viene rimosso dalla rete antivirus. Per tutti i gruppi e postazioni a cui è stata assegnata questa chiave di licenza verrà impostata l'ereditarietà della chiave di licenza.
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 rimuovere l'oggetto selezionato.

Trasferire licenze su un Server Dr.Web adiacente

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

Per trasferire licenze su un Server Dr.Web adiacente

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



3. Selezionare dalla lista i Server Dr.Web su cui si vogliono distribuire le licenze.
4. Di fronte a ciascuno dei Server Dr.Web configurare i seguenti parametri:
 - **Numero di licenze** — numero di licenze disponibili che si vuole trasferire da questa chiave su un Server Dr.Web adiacente.
 - **Data di scadenza della licenza** — periodo per cui vengono trasferite le licenze. Dopo il periodo indicato tutte le licenze verranno revocate dal Server Dr.Web adiacente e torneranno nella lista delle licenze disponibili di questa chiave di licenza.
5. Fare clic su uno dei pulsanti:
 - **Aggiungi chiave di licenza** — per aggiungere le licenze alla lista delle licenze disponibili dei Server Dr.Web 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 delle chiavi](#).
 - **Sostituisci chiave di licenza** — per rimuovere le licenze correnti dei Server Dr.Web adiacenti e assegnare solo 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](#).

Modificare le licenze trasferite su un Server Dr.Web adiacente

Per modificare le licenze distribuite su un Server Dr.Web adiacente

1. Nella finestra principale Gestione licenze nell'albero delle chiavi selezionare il Server Dr.Web 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 disponibili trasferite dalla chiave di questo Server Dr.Web sul Server Dr.Web adiacente.
 - **Data di scadenza della licenza** — periodo per cui vengono trasferite le licenze. Dopo il periodo indicato tutte le licenze verranno revocate da questo Server Dr.Web adiacente e torneranno nella lista delle licenze disponibili della chiave di licenza corrispondente.
3. Fare clic sul pulsante **Salva** per aggiornare 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 Dr.Web adiacente sostituendone la chiave.

Per configurare i componenti da installare per l'esecuzione di queste procedure

1. Nella finestra di configurazione dei componenti da installare nella lista degli oggetti sono riportati:
 - Postazioni, gruppi e criteri con le loro liste 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.
 - 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.
2. Per configurare la lista dei componenti da installare:
 - a) Nella colonna **Chiave che viene assegnata** è possibile configurare la lista risultante 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
+	+	+
-	+	+
+	-	-
-	-	-

- È possibile modificare le impostazioni dei componenti da installare (abbassare i permessi di installazione) solo se nelle impostazioni ottenute nella colonna **Chiave che viene assegnata** l'utilizzo di questo componente è consentito.
- b) Spuntare i flag per gli oggetti (postazioni, gruppi e criteri) per cui l'ereditarietà delle impostazioni verrà disattivata e verranno definite come individuali le impostazioni dei componenti da installare dalla colonna **Chiave che viene assegnata**. Per gli altri oggetti (per cui i flag non sono selezionati) verrà definita l'ereditarietà delle impostazioni originali 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 Dr.Web adiacente aggiungendo la chiave.

Per configurare i componenti da installare per l'esecuzione di queste procedure

1. Nella finestra di configurazione dei componenti da installare nella lista degli oggetti sono riportati:
 - Postazioni, gruppi e criteri con le loro liste 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**, invece delle impostazioni stesse della chiave che viene assegnata, sono riportate le impostazioni risultanti dei componenti da installare.
3. Per configurare la lista dei componenti da installare:
 - a) Nella colonna **Chiave che viene assegnata** è possibile configurare la lista risultante 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
+	+	+
-	+	-
+	-	-
-	-	-

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



- b) Spuntare i flag per gli oggetti (postazioni, gruppi e criteri) per cui l'ereditarietà delle impostazioni verrà disattivata e verranno definite come individuali le impostazioni dei componenti da installare dalla colonna **Chiave che viene assegnata**. Per gli altri oggetti (per cui i flag non sono selezionati) verrà definita l'ereditarietà delle impostazioni dalla colonna **Chiave che viene assegnata**.

10.1.2. Report sull'utilizzo delle licenze

Il report sull'utilizzo delle licenze contiene informazioni su tutte le licenze che sono utilizzate sia da questo Server Dr.Web che dai Server Dr.Web adiacenti, anche nel caso di trasferimento di una licenza attraverso una relazione tra i server.



I report vengono creati (e inviati nel caso di Server Dr.Web adiacenti) in base alle impostazioni definite nella sezione **Configurazione del Server Dr.Web** → **Licenze**, sezione **Impostazioni per il report sull'utilizzo delle licenze**.

Per visualizzare un report, nel menu principale del Pannello di controllo selezionare la voce **Amministrazione**, nella finestra che si è aperta nel [menu di gestione](#) selezionare la voce **Report sull'utilizzo delle licenze**.

In questa sezione sono riportate le seguenti informazioni:

- Report su tutte le licenze di cui dispone questo Server Dr.Web. Il report sarà presente anche nel caso in cui nessuna relazione con Server Dr.Web adiacenti è configurata sul Server Dr.Web.
- Report sulle licenze di cui dispongono i Server Dr.Web adiacenti che sono subordinati a questo Server Dr.Web, in particolare, ricevono licenze da esso attraverso le relazioni tra i server. Saranno presenti i report da tutti i Server Dr.Web adiacenti giù nell'albero delle relazioni tra i server.

Ogni report è visualizzato sotto forma di tabella separata e contiene informazioni sulle licenze di un solo Server Dr.Web — l'autore del report.

L'intestazione della tabella contiene le seguenti informazioni:

- **Server Dr.Web** — nome del Server Dr.Web — autore del report.
- **Totale licenze ricevute tramite le relazioni** — numero totale di licenze che il Server Dr.Web ha ricevuto attraverso le relazioni tra i server.

La tabella del report contiene le seguenti informazioni:

- **Utente** — utente della chiave di licenza, le informazioni sulle licenze della quale vengono riportate nella riga del report.
- **Totale licenze** — numero totale di licenze fornite da questa chiave di licenza su questo Server Dr.Web.
- **Disponibile** — numero di licenze disponibili, non utilizzate in questa chiave.



- **Totale licenze utilizzate** — numero totale di licenze utilizzate (rilasciate alle postazioni o ai Server Dr.Web adiacenti) al momento della creazione del report.
- **Utilizzate dalle postazioni** — numero di licenze utilizzate dalle postazioni connesse al Server Dr.Web — autore del report.
- **In attesa** — numero di licenze che l'autore del report si aspetta di ricevere. In particolare, se un Server Dr.Web che ha utilizzato un certo numero di licenze (o le ha già assegnate alle sue postazioni, o le ha trasmesse tramite le relazioni tra i server), ha perso una parte di queste licenze. Per esempio, la chiave di licenza è stata sostituita con una chiave con un minor numero di licenze, o è stato ridotto il numero di licenze ottenute dal Server Dr.Web padre.
- **Riservate** — numero di licenze che sono state date tramite le relazioni tra i server, ma il destinatario non ha ancora preso le licenze ad esso assegnate: i Server Dr.Web adiacenti ancora non si connettevano per ricevere le licenze. Queste licenze sono riservate dalla chiave di licenza e non possono essere date ad altre postazioni o Server Dr.Web.
- **Rilasciate tramite le relazioni** — numero di licenze che il Server Dr.Web — autore del report ha rilasciato ai suoi Server Dr.Web adiacenti attraverso le relazioni tra i server.
- **Ricevute tramite le relazioni** — numero di licenze che il Server Dr.Web — autore del report ha ricevuto dai suoi Server Dr.Web adiacenti attraverso le relazioni tra i server.
- **Data del report** — data di creazione del report.

Per le licenze utilizzate dalle postazioni del Server Dr.Web stesso — autore del report sono disponibili informazioni aggiuntive. Per visualizzarle, fare clic sul numero di licenze nella colonna **Utilizzate dalle postazioni** (il numero di licenze non deve essere pari a zero). Nella tabella che si è aperta **Utilizzo delle licenze dai gruppi** sono fornite le seguenti informazioni:

- **Nome del gruppo** — il nome del gruppo di postazioni su cui sono state propagate le licenze.
- **Licenze propagate** — il numero totale di licenze propagate sul gruppo di postazioni.
- **Postazioni attive** — numero di postazioni attive nel gruppo. Per postazioni attive si intendono le postazioni che sono state nella rete durante il periodo specificato nelle impostazioni per la creazione del report sul Server Dr.Web — proprietario della chiave di licenza.

10.2. Log

10.2.1. Log in tempo reale

Il log in tempo reale consente di visualizzare una lista di eventi e modifiche relativi al funzionamento di Server Dr.Web che vengono restituiti immediatamente al momento del verificarsi di un evento.





Il log in tempo reale solo visualizza informazioni nel Pannello di controllo e non registra eventi in file. Il file di [log di Server Dr.Web](#) viene registrato separatamente con le sue impostazioni e non dipende dal log in tempo reale e dalle sue impostazioni.

Quando si passa a un'altra sezione, vengono cancellate tutte le informazioni visualizzate nel log in tempo reale.

La tabella del log contiene le seguenti informazioni:


- **n.** — numero progressivo del record. Il numero viene assegnato in base all'ordine in cui i messaggi arrivano dal Server Dr.Web.
- **Tempo nel formato del log** — tempo del verificarsi dell'evento rappresentato nel formato del log di Server Dr.Web. Può essere utilizzato durante la ricerca di un evento nel file di log di Server Dr.Web.
- **Tempo** — tempo del verificarsi dell'evento rappresentato in una forma conveniente per l'utente.
- **Livello** — livello di registrazione del log secondo cui si è verificato l'evento.
- **PID** — identificatore del processo in cui si è verificato l'evento.
- **TID** — identificatore del flusso in cui si è verificato l'evento.
- **Flusso** — nome del flusso in cui si è verificato l'evento.
- **Sottosistema** — nome del sottosistema in cui si è verificato l'evento.
- **Messaggio** — testo del messaggio sull'evento. Fare clic su un messaggio nella tabella per aprire la finestra con il testo completo del messaggio. Se il testo è un codice HTML, spuntare il flag **Formatta come testo HTML** per la corretta visualizzazione delle informazioni. Notare che se nel testo del messaggio c'è JavaScript, esso verrà eseguito.


Per cambiare la visualizzazione dei dati nella tabella

- Tramite l'icona :
 - Definire le impostazioni di visualizzazione delle righe (utile in caso di righe lunghe).
 - Selezionare quali colonne verranno visualizzate nella tabella.
- Tramite l'icona :
 - Impostare una stringa arbitraria per la ricerca in tutte le sezioni della tabella. Nella tabella verranno visualizzate solo le righe che corrispondono ai risultati della ricerca.
 - Per visualizzare solo livelli specifici, spuntare i flag di fronte ai livelli richiesti.
 - Per visualizzare solo sottosistemi specifici, spuntare i flag di fronte ai sottosistemi richiesti.

Affinché nel log vengano registrati solo messaggi di livelli specifici e da sottosistemi specifici, definire le [impostazioni di registrazione del log](#).

Nella barra degli strumenti sono riportati i seguenti elementi di gestione del log:

 **Configura la visualizzazione dei dati** — per aprire la finestra di [configurazione di registrazione del log](#).

 **Pulisci tabella** — per cancellare tutti i dati visualizzati nella tabella. L'operazione è irreversibile.



- **Arresta la raccolta dati** — per arrestare l'output di informazioni su eventi nella tabella. Il pulsante è attivo quando viene eseguita la raccolta dei dati. Se viene premuto, il pulsante cambia in ● **Avvia la raccolta dati**.
- **Avvia la raccolta dati** — per iniziare l'output di informazioni su eventi nella tabella. Il pulsante è attivo quando la raccolta dei dati è arrestata. Se viene premuto, il pulsante cambia in ● **Arresta la raccolta dati**.

Configurazione di registrazione del log in tempo reale

1. Nel pannello di controllo premere **Configura la visualizzazione dei dati**. Si apre la finestra **Impostazioni di visualizzazione dei dati**.
2. Il campo **Numero massimo di record** imposta una limitazione al numero di record visualizzati nella tabella del log. Quando viene raggiunto il numero impostato, i record vecchi vengono cancellati alla comparsa di record nuovi.
3. Il campo **Frequenza di aggiornamento, s** definisce la frequenza in secondi con cui i nuovi record verranno visualizzati nel log.
4. Il campo **Ricerca per sottosistema** consente di effettuare una ricerca per nome dei sottosistemi riportati sotto. Può essere usato quando è necessario impostare il livello di dettaglio del log di un determinato sottosistema nel caso di un numero elevato di sottosistemi nella lista.
5. La tabella dei sottosistemi consente di configurare la lista dei dati visualizzati e il livello di dettaglio dei dati:
 - a) Spuntare i flag di fronte ai sottosistemi di cui i messaggi verranno visualizzati nella tabella.
 - b) Selezionare il livello di dettaglio del log per i sottosistemi selezionati.
 - c) Per visualizzare tutti i sottosistemi, spuntare il file nell'intestazione della tabella.
 - d) Per impostare un livello di dettaglio del log uguale per tutti i sottosistemi, selezionare dalla lista a cascata il valore **all** di fronte a un sottosistema. In tale caso nella tabella verranno restituiti solo messaggi dai sottosistemi per cui i flag sono spuntati.
6. Premere il pulsante **Applica** per iniziare a visualizzare dati secondo le impostazioni definite.
7. Premere **Chiudi** per chiudere la finestra senza alcuna modifica nelle impostazioni di visualizzazione del log.


10.2.2. Log di verifica

Il log di verifica consente di visualizzare la lista degli eventi e delle modifiche apportate tramite i sottosistemi di gestione di Dr.Web Enterprise Security Suite.

Per visualizzare il log di verifica

1. Selezionare la voce **Amministrazione** nel menu principale del Pannello di controllo.
2. Nella finestra che si è aperta, selezionare la voce del menu di gestione **Log di verifica**.



3. Si apre una finestra con una tabella delle azioni registrate. Per configurare la visualizzazione del log, impostare nella barra degli strumenti un periodo durante cui sono state eseguite le azioni. Per farlo, si può selezionare dalla lista a discesa uno dei periodi proposti o impostare qualsiasi data nei calendari che vengono aperti quando si fa clic sui campi delle date. Premere **Aggiorna** per visualizzare il log per le date selezionate.
4. Per configurare l'aspetto della tabella, fare clic sull'icona  nell'angolo destro dell'intestazione della tabella. Nella lista a cascata è possibile configurare le seguenti opzioni:
 - Attivare o disattivare la continuazione in nuove righe per messaggi lunghi.
 - Selezionare colonne che verranno visualizzate nella tabella (sono contrassegnate da un flag accanto al nome). Per attivare/disattivare una colonna, fare clic sulla riga con il suo nome.
 - Selezionare l'ordine delle colonne nella tabella. Per modificare l'ordine, trascinare nella lista la colonna desiderata sul posto richiesto.
5. La tabella del log contiene le seguenti informazioni:
 - **Tempo** — la data e l'ora quando è stata eseguita l'azione.
 - **Stato** — il breve risultato dell'esecuzione dell'azione:
 - **OK** — l'operazione è stata eseguita con successo.
 - **non riuscito** — un errore è occorso durante l'esecuzione dell'operazione. L'operazione non è stata eseguita.
 - **avviato** — l'esecuzione dell'operazione è stata avviata. Il risultato dell'esecuzione dell'operazione sarà noto solo dopo il suo completamento.
 - **nessun permesso** — l'amministratore che ha avviato l'esecuzione dell'operazione non ha i permessi per la sua esecuzione.
 - **differito** — l'esecuzione dell'azione è stata rinviata fino al verificarsi di un determinato termine o evento.
 - **vietato** — l'esecuzione dell'azione richiesta è vietata. Per esempio, l'eliminazione dei gruppi di sistema.



Per le azioni terminate con un errore (il valore **non riuscito** nella colonna **Stato**) le righe vengono marcate in rosso.

- **Messaggio / Errore** — descrizione dettagliata dell'operazione eseguita o dell'errore occorso.
- **Nome utente** — il nome utente dell'amministratore di Server Dr.Web. Viene specificato se l'azione è stata avviata direttamente dall'amministratore o in caso di una connessione al Server Dr.Web in base alle credenziali dell'amministratore.
- **Indirizzo** — l'indirizzo IP da cui è stata avviata l'esecuzione di questa azione. Viene specificato solo nel caso di una connessione esterna al Server Dr.Web, in particolare attraverso il Pannello di controllo o attraverso Web API.



- **Sottosistema** — il nome del sottosistema da cui o attraverso cui è stata avviata l'azione. Il log di verifica viene registrato per i seguenti sottosistemi:
 - **Pannello di controllo** — l'azione è stata eseguita attraverso il Pannello di controllo della sicurezza Dr.Web, in particolare dall'amministratore.
 - **Web API** — l'azione è stata eseguita attraverso Web API, per esempio, da un'applicazione esterna connessa in base alle credenziali dell'amministratore (v. inoltre documento **Allegati**, p. [Allegato K. Integrazione di Web API e Dr.Web Enterprise Security Suite](#)).
 - **Server** — l'azione è stata eseguita dal Server Dr.Web, per esempio secondo il suo calendario.
 - **Utility** — l'azione è stata avviata attraverso le utility esterne, in particolare attraverso l'utility di diagnostica remota del Server Dr.Web.
- 6. Se necessario, è possibile esportare in file le informazioni per un periodo selezionato. Per farlo, nella barra degli strumenti premere uno dei seguenti 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.

10.2.3. Log del Server Dr.Web

Il Server Dr.Web registra in un log gli eventi relativi al suo funzionamento.



Il log di Server Dr.Web viene utilizzato per il debugging, nonché per la risoluzione dei problemi in caso di funzionamento anomalo dei componenti della rete antivirus.

Di default, il file di log si chiama `drwcsd.log` e si trova in:

- In SO **UNIX**:
 - in caso di SO Linux: `/var/opt/drwcs/log/drwcsd.log`;
 - in caso di SO FreeBSD: `/var/drwcs/log/drwcsd.log`.
- In SO **Windows**: nella sottodirectory `var` della directory di installazione di Server Dr.Web.

Il file è in formato di testo semplice (v. documento **Allegati**, [Allegato J. Formato dei file di log](#)).

Per visualizzare il log di funzionamento di Server Dr.Web tramite il Pannello di controllo


1. Selezionare la voce **Amministrazione** nel menu principale del Pannello di controllo.
2. Nella finestra che si è aperta, selezionare la voce del menu di gestione **Log del Server Dr.Web**.
3. Si apre una finestra con l'elenco dei log di funzionamento del Server Dr.Web. Secondo le impostazioni della modalità di rotazione, viene utilizzato il seguente formato dei nomi dei




file di log di Server Dr.Web: `<file_name>.<N>.log` o `<file_name>.<N>.log.gz`, dove `<N>` è 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 — maggiore 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** — per salvare una copia locale dei file di log selezionati. Il salvataggio della copia del log può essere usato, per esempio per visualizzare i contenuti del file di log da un computer remoto.

 **Rimuovi i file di log selezionati** — per rimuovere i file di log selezionati senza possibilità di recupero.



Per cambiare la modalità di registrazione del log di Server Dr.Web attraverso il Pannello di controllo, utilizzare la sezione [Log](#).

Gestione del livello di dettaglio del log

A seconda delle impostazioni configurate, il log di Server Dr.Web può essere riempito con diversi livelli di dettaglio. L'attivazione di una modalità più dettagliata per una singola fonte di messaggi o per tutte le fonti contemporaneamente può aiutare ad effettuare il debug e la risoluzione di problemi, e inoltre, può essere richiesta quando si contatta il supporto tecnico dell'azienda Doctor Web. Esistono diversi modi per configurare questo parametro:

- Tramite il Pannello di controllo nella sezione **Amministrazione** → **Configurazione del Server Dr.Web** → **Log**. In questo modo è possibile impostare il livello di dettaglio dei messaggi del log per tutte le possibili fonti.
- Tramite l'opzione `-verbosity` all'avvio di Server Dr.Web dalla riga di comando. Questo metodo è più flessibile e consente, se necessario, di impostare il livello di dettaglio per una o più fonti separate. Il formato dell'opzione è descritto in documento **Allegati**, [G3.8. Descrizione delle opzioni](#).
- Tramite un file di configurazione separato `logging.conf`. Per questo scopo è necessario creare un file con tale nome nella directory `etc` all'interno della directory di installazione di Server Dr.Web, dopodiché indicare nel file le fonti di messaggi e i livelli di dettaglio richiesti nel formato `<fonte_messaggio> : <livello>`. L'opzione formato `-verbosity=all:all` equivale all'opzione `-verbosity=all`. I livelli di dettaglio impostati tramite `logging.conf` hanno la precedenza sui livelli impostati in qualsiasi altro modo.

Esempio del contenuto del file `logging.conf`:

```
Alert:all, Server:err, SQLite3:inf
```



Oltre alla virgola, come separatore è ammissibile qualsiasi carattere di spazio, inclusi lo spazio normale, la tabulazione, la nuova riga, ecc. È possibile precisare la lista delle fonti di messaggi direttamente nel file di log di Server Dr.Web, o tramite il Pannello di controllo eseguendo il comando `drwcs.log_subsystems()` nella sezione **Amministrazione** → **Console Lua**. I possibili livelli di dettaglio sono riportati in documento **Allegati**, [Allegato J. Formato dei file di log](#).



I livelli di dettaglio impostati in questo modo vengono ereditati da parte dei sottosistemi. Cioè, per esempio, se vengono indicati contemporaneamente i parametri `Socket/Client:inf` e `Socket:all`, il sottosistema `Socket/Client`, seguendo l'istruzione a livello di padre, registrerà nel log informazioni su tutti gli eventi correlati, e non solo messaggi di carattere informativo.

- Per i Server Dr.Web che funzionano sui sistemi operativi della famiglia UNIX — tramite un'opzione speciale nel file di configurazione `local.conf`. La procedura per l'utilizzo di questo file è descritta di seguito.

Configurazione del log di funzionamento per UNIX

I Server Dr.Web sotto gli SO della famiglia UNIX includono la possibilità di configurare la registrazione del log di funzionamento di Server Dr.Web attraverso un file di configurazione separato:

- in caso di SO Linux: `/var/opt/drwcs/etc/local.conf`;
- in caso di SO FreeBSD: `/var/drwcs/etc/local.conf`.

Contenuti del file `local.conf`:

```
# Log level.  
DRWCS_LEV=info  
  
# Log rotation.  
DRWCS_ROT=10z,10m
```

I valori dei parametri corrispondono ai valori delle opzioni della riga di comando per l'avvio di Server Dr.Web:

- `-verbosity=<livello_di_dettaglio>` — livello di dettaglio del log di funzionamento di Server Dr.Web.
- `-rotate=<N><f>, <M><u>` — modalità di rotazione del log di funzionamento di Server Dr.Web.

La descrizione dettagliata delle opzioni è riportata in documento **Allegati**, sezione [G3.8. Descrizione delle opzioni](#).




Se il file `local.conf` è stato modificato nel processo di funzionamento di Server Dr.Web, è necessario riavviare Server Dr.Web affinché le modifiche alle impostazioni di registrazione del log abbiano effetto. Il riavvio deve essere eseguito tramite gli strumenti del sistema operativo.

Se Server Dr.Web viene aggiornato o rimosso, viene eseguito il backup del file `local.conf`, il che consente di gestire il livello di registrazione del log in caso di aggiornamento batch di Server Dr.Web.

10.2.4. Log di aggiornamento del repository

Il log di aggiornamento del repository contiene un elenco degli aggiornamenti da SAM che include informazioni dettagliate sulle revisioni dei prodotti aggiornate.

Per visualizzare il log di aggiornamento del repository

1. Selezionare la voce **Amministrazione** nel menu principale del Pannello di controllo.
2. Nella finestra che si è aperta, selezionare la voce del menu di gestione **Log di aggiornamento del repository**.
3. Si apre una finestra con una tabella delle azioni registrate. Per configurare la visualizzazione del log, impostare nella barra degli strumenti un periodo durante cui sono state eseguite le azioni. Per farlo, si può selezionare dalla lista a discesa uno dei periodi proposti o impostare qualsiasi data nei calendari che vengono aperti quando si fa clic sui campi delle date. Premere **Aggiorna** per visualizzare il log per le date selezionate.
4. Per visualizzare nella tabella solo gli eventi di un determinato tipo, fare clic sull'icona  nella barra degli strumenti. Nella lista a cascata è possibile selezionare i parametri di filtraggio richiesti:
 - **Nome del prodotto** — nella tabella del log verranno visualizzati tutti gli eventi relativi ai prodotti selezionati dalla lista.
 - **Risultato dell'aggiornamento** — nella tabella del log verranno visualizzate tutte le sessioni di aggiornamento e i loro risultati. Le sessioni possono essere filtrate in base ai seguenti risultati:
 - **Il prodotto richiesto non è stato trovato sui server SAM;**
 - **La chiave di licenza non è stata trovata sui server SAM;**
 - **Aggiornamento è disattivato;**
 - **Aggiornamento completato con successo.**
 - **Iniziatore** — nella tabella del log verranno visualizzate le sessioni di aggiornamento avviate dai seguenti sistemi:
 - **Avviato dalla riga di comando** — l'aggiornamento è stato avviato dall'amministratore tramite il comando di console corrispondente.



- **Avviato dallo Scheduler** — l'aggiornamento è stato avviato secondo un task nel [calendario del Server Dr.Web](#).
- **Aggiornamento tra i server** — l'aggiornamento è stato ricevuto attraverso la comunicazione tra i server da Server Dr.Web principale. Questo tipo di iniziatore è presente solo nel caso di una [configurazione di rete antivirus con diversi server](#) con la distribuzione degli aggiornamenti attraverso la comunicazione tra i server.
- **Avviato dal Pannello di controllo** — l'aggiornamento è stato avviato dall'amministratore tramite il Pannello di controllo della sicurezza Dr.Web, nella sezione [Stato del repository](#).
- **Importazione del repository** — l'aggiornamento è stato caricato dall'amministratore attraverso la sezione [Contenuti del repository](#) del Pannello di controllo.

5. La tabella del log contiene le seguenti informazioni:

- **Amministratore** — il nome utente dell'amministratore di Server Dr.Web. Viene specificato se l'azione è stata avviata direttamente dall'amministratore.
- **Indirizzo di rete** — l'indirizzo IP da cui è stata avviata l'esecuzione di questa azione. Viene specificato solo nel caso di una connessione esterna al Server Dr.Web, in particolare attraverso il Pannello di controllo o attraverso Web API.
- **Iniziatore** — il sistema che ha avviato il processo di aggiornamento.
- **Directory nel repository** — il nome della directory di repository di Server Dr.Web che è stata modificata secondo il processo di aggiornamento.
- **Nome del prodotto** — il nome del prodotto di repository che è stato caricato o di cui il caricamento è stato richiesto.
- **Inizio** — la data e l'ora di inizio del caricamento degli aggiornamenti di un prodotto specifico da SAM.
- **Fine** — la data e l'ora di fine del caricamento degli aggiornamenti di un prodotto specifico da SAM.
- **Risultato dell'aggiornamento** — il risultato dell'aggiornamento del repository. Contiene brevi informazioni sul completamento di aggiornamento riuscito o la causa di errore.







Per le azioni fallite le celle **Risultato dell'aggiornamento** vengono marcate in rosso.

- **Revisione iniziale** — il numero della revisione (le revisioni vengono numerate in base alla data di creazione) che era l'ultima per questo prodotto prima dell'inizio del processo di aggiornamento.
- **Revisione ricevuta** — il numero della revisione (le revisioni vengono numerate in base alla data di creazione) che è stata caricata nel processo di aggiornamento.
- **File aggiornati** — un riepilogo dei file modificati. Viene riportato nel formato: *<numero di file> - <azione eseguita con i file>*.

6. Se necessario, è possibile esportare in file le informazioni per un periodo selezionato. Per farlo, nella barra degli strumenti premere uno dei seguenti 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.**

10.2.5. Log dei messaggi


Nel log dei messaggi vengono visualizzati tutti i messaggi di testo che sono stati inviati dall'amministratore sulle postazioni della rete antivirus (v. [Invio di messaggi alle postazioni](#)).


Il log dei messaggi inviati contiene le seguenti informazioni:

- **Data di invio.**
- **Mittente** — il nome utente dell'amministratore autenticato nel Pannello di controllo per l'invio del messaggio.
- **Stato** — numero di messaggi inviati dall'amministratore e numero di messaggi consegnati con successo sulle postazioni. Se il numero di messaggi inviati e consegnati coincide, le informazioni su questi messaggi sono evidenziate in grigio.
- **Messaggio** — testo del messaggio inviato. Vengono visualizzate opzionalmente informazioni su altre impostazioni definite per l'invio.

Quando si fa clic su un messaggio specifico nella tabella, si apre una finestra con i dettagli sulla consegna: la lista di tutti i destinatari e la data di consegna del messaggio in caso di un'operazione riuscita o messaggio **Non consegnato** — in caso di un'operazione non riuscita.


Per gestire il log dei messaggi, utilizzare le seguenti opzioni nella barra degli strumenti:

 **Invia di nuovo i messaggi selezionati** — l'opzione è disponibile se viene selezionato uno o più messaggi inviati nel log (vedi le procedure sotto).

 **Salva il messaggio selezionato come modello** — per creare in base al messaggio inviato un modello da utilizzare nuovamente in seguito. L'opzione è disponibile se viene selezionato un messaggio nel log. I modelli salvati vengono gestiti nella sezione [Modelli di messaggio](#).

Dalla lista a cascata selezionare un periodo durante cui sono stati inviati i messaggi che si vuole visualizzare. Lo stesso periodo può essere selezionato nei campi con le date che vengono impostate attraverso un calendario a discesa. Per applicare il periodo selezionato, premere il pulsante **Aggiorna**.


Per inviare nuovamente un messaggio

1. Spuntare il flag di fronte al messaggio che si vuole inviare.
2. Premere il pulsante  **Invia di nuovo i messaggi selezionati**.
3. Si apre la finestra **Invio del messaggio**. Configurare le seguenti impostazioni:



- a) Nell'albero **Rete antivirus** saranno selezionate postazioni su cui deve essere inviato questo messaggio. È possibile lasciare i destinatari precedenti o selezionare destinatari arbitrari dall'elenco proposto: possono essere sia singole postazioni che gruppi di postazioni.
 - b) Le impostazioni del messaggio sono simili alle impostazioni dalla sezione [Invio di messaggi alle postazioni](#).
4. Premere il pulsante **Invia**.

Per inviare nuovamente più messaggi

1. Spuntare i flag di fronte ai messaggi che si vuole inviare.
2. Premere il pulsante  **Invia di nuovo i messaggi selezionati**.
3. Si apre la finestra **Invio di più messaggi**. Nella sezione **Elenco dei messaggi** sono riportati tutti i messaggi che sono stati selezionati per il nuovo invio. I nomi dei messaggi corrispondono alle date del relativo invio su postazioni precedente.
4. Premere il pulsante **Invia tutto** per inviare tutti i messaggi dalla lista.
5. Per modificare uno dei messaggi, selezionarlo nella sezione **Elenco dei messaggi**. Nella sezione **Impostazioni del messaggio** configurare i seguenti parametri:
 - a) Nell'albero **Rete antivirus** saranno selezionate postazioni su cui deve essere inviato questo messaggio. È possibile lasciare i destinatari precedenti o selezionare destinatari arbitrari dall'elenco proposto: possono essere sia singole postazioni che gruppi di postazioni.
 - b) Le impostazioni del messaggio sono simili alle impostazioni dalla sezione [Invio di messaggi alle postazioni](#).
 - c) Per eliminare il messaggio selezionato dalla lista dei messaggi da inviare, premere il pulsante **Rimuovi**.

10.3. Configurazione del Server Dr.Web



Ogni volta che si salvano modifiche della sezione **Configurazione del Server Dr.Web**, viene automaticamente salvato un backup della versione precedente del file di configurazione del Server Dr.Web. Vengono conservati gli ultimi 10 backup.

I backup si trovano nella stessa directory del file di configurazione e vengono denominati nel seguente formato:

```
drwcsd.conf_<ora_di_creazione>
```

È possibile utilizzare i backup creati, in particolare, per ripristinare il file di configurazione se l'interfaccia del Pannello di controllo non è disponibile.

Per definire i parametri di configurazione di Server Dr.Web






1. Selezionare la voce **Amministrazione** nel menu principale del Pannello di controllo.



2. Nella finestra che si è aperta selezionare la voce del menu di gestione **Configurazione del Server Dr.Web**. Si apre la finestra delle impostazioni di Server Dr.Web.



I valori dei campi contrassegnati con il carattere * sono da impostare.

3. Nella barra degli strumenti sono disponibili i seguenti pulsanti per gestire le impostazioni della sezione:
 -  **Riavvia Server Dr.Web** — per riavviare il Server Dr.Web per accettare le modifiche apportate a questa sezione. Il pulsante diventa attivo dopo che si sono apportate modifiche alle 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 è possibile ritornare dopo che si sono apportate modifiche. Il pulsante diventa attivo dopo che si sono apportate modifiche alle 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 di default** — per ripristinare tutti i parametri di questa sezione ai valori di default.
4. Per accettare le modifiche apportate alle impostazioni della sezione, premere il pulsante **Salva**, dopodiché sarà necessario riavviare il Server Dr.Web. Per fare questo, premere il pulsante  **Riavvia Server Dr.Web** nella barra degli strumenti di questa sezione.

10.3.1. Generali

Nella scheda **Generali** vengono configurate le seguenti impostazioni di funzionamento del Server Dr.Web:

- **Nome del Server** — nome di questo Server Dr.Web. Se il valore del campo non è impostato, viene utilizzato il nome del computer su cui è installato il Server Dr.Web.
- **Lingua del Server Dr.Web** — lingua che viene utilizzata di default dai componenti e sistemi di Server Dr.Web, se non è stato possibile ottenere le impostazioni di lingua dal database di Server Dr.Web. In particolare, viene utilizzata per il Pannello di controllo della sicurezza Dr.Web e il sistema di avviso dell'amministratore, se il database è stato danneggiato e non è possibile ottenere le impostazioni di lingua.



Se si seleziona una lingua in cui i testi dell'interfaccia al momento non vengono aggiornati, verrà suggerito di attivare l'aggiornamento per questa lingua. Per fare ciò, andare attraverso il link alla sezione **Amministrazione** → **Configurazione generale del repository** → **Server Dr.Web** → **Lingue del Pannello di controllo della sicurezza Dr.Web**, impostare il flag per la lingua desiderata e premere **Salva**. Al prossimo aggiornamento del repository i testi dell'interfaccia per la lingua selezionata verranno aggiornati. È inoltre possibile avviare manualmente l'aggiornamento nella sezione **Stato del repository**.



- **Numero di richieste parallele dai client** — numero di flussi per l'elaborazione dei dati provenienti dai client: Agent Dr.Web, installer di Agent, Server Dr.Web adiacenti, Server proxy Dr.Web. Questo parametro influisce sulle prestazioni di Server Dr.Web. In caso di utilizzo del database incorporato, non è consigliabile modificare il valore di default. In caso di utilizzo di un database esterno, potrebbe essere necessario un valore di parametro più grande (v. **Allegati**, sezione [Carico su Server Dr.Web e parametri di configurazione raccomandati](#)). In caso di utilizzo di una rete con un numero elevato di connessioni client a Server Dr.Web, prima di modificare il valore, si consiglia di ottenere consulenza nel servizio di supporto tecnico dell'azienda Doctor Web.



A partire dalla versione 10 non è più fornita la possibilità di modificare il parametro **Coda di autenticazione** attraverso il Pannello di controllo.

Di default, quando viene installato nuovo Server Dr.Web, questo parametro viene impostato pari a 50. Se Server Dr.Web viene aggiornato da versione precedente con il salvataggio del file di configurazione, il valore di coda di autenticazione viene salvato dalla configurazione della versione precedente.

Se è necessario modificare la lunghezza della coda di autenticazione, modificare il valore del seguente parametro nel file di configurazione di Server Dr.Web:

```
<!-- Maximum authorization queue length -->  
<maximum-authorization-queue size='50' />
```

- Nella lista a cascata **Modalità di registrazione dei nuovi arrivi** viene impostato il criterio di approvazione delle nuove postazioni (v. [Criteri di approvazione delle postazioni](#)).
 - La lista a cascata **Gruppo primario predefinito** definisce il gruppo primario in cui le postazioni verranno messe con la conferma automatica dell'accesso delle postazioni al Server Dr.Web.
- Spuntare il flag **Trasferisci le postazioni non autenticate in nuovi arrivi** per resettare per le postazioni non autenticate i parametri di ottenimento di accesso a Server Dr.Web. Questa opzione può essere utile in caso di modifica delle impostazioni di Server Dr.Web (come per esempio, la chiave di cifratura pubblica) o in caso di cambio del database. In tali casi le postazioni non potranno connettersi e dovranno nuovamente ricevere i nuovi parametri di accesso a Server Dr.Web.
- Spuntare il flag **Crea automaticamente account di postazioni** affinché nel Pannello di controllo gli account di postazioni mancanti vengano creati automaticamente durante l'installazione degli Agent Dr.Web da un pacchetto di installazione di gruppo. Se il flag è tolto, l'installazione è possibile solo per il numero di account già creati nel gruppo per le cui postazioni viene avviato il pacchetto di installazione.
- Nel campo **Differenza ammissibile tra l'ora del Server Dr.Web 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.
- Nella lista a cascata **Nome della postazione** viene impostato il formato di visualizzazione dei nomi delle postazioni nella directory della rete antivirus del Pannello di controllo.
- Attraverso la lista a cascata **Sostituisci il nome della postazione** è possibile impostare, se necessario, una variante che consente di sostituire i nomi delle postazioni visualizzati con un nome DNS completamente o parzialmente qualificato (se la risoluzione dei nomi DNS non è possibile, vengono visualizzati gli indirizzi IP).



Di default il flag **Sostituisci gli indirizzi IP** è deselezionato, e i nomi delle postazioni non vengono sostituiti. In caso di una configurazione errata del servizio DNS, l'attivazione di queste funzionalità può rallentare notevolmente il Server Dr.Web. Se viene attivata qualsiasi di queste modalità, si consiglia di consentire la memorizzazione dei nomi nella cache sul server DNS.



Se nella lista a cascata **Sostituisci il nome della postazione** è selezionata una delle varianti di sostituzione, e nella rete antivirus viene utilizzato un Server proxy Dr.Web, per tutte le postazioni connesse al Server Dr.Web attraverso il Server proxy Dr.Web come nomi di postazioni nel Pannello di controllo verrà visualizzato il nome del computer su cui è installato il Server proxy Dr.Web.

- Spuntare il flag **Sincronizza le descrizioni delle postazioni** per sincronizzare la descrizione del computer dell'utente (campo **Descrizione** sulla pagina **Proprietà del sistema** in SO Windows) con la descrizione della postazione nel Pannello di controllo. Se la descrizione della postazione nel Pannello di controllo è assente, in questo campo verrà scritta la descrizione del computer sul lato utente. Se le descrizioni differiscono, i dati nel Pannello di controllo verranno sostituiti con quelli dell'utente.
- Spuntare il flag **Sincronizza la posizione geografica** per attivare la sincronizzazione della posizione geografica delle postazioni tra i Server Dr.Web in una rete antivirus con diversi server. Se il flag è spuntato, si può inoltre impostare il seguente parametro:
 - **Sincronizzazione iniziale** — numero di postazioni senza coordinate geografiche, le informazioni su cui vengono richieste quando viene stabilita una connessione tra i Server Dr.Web.
- Spuntare il flag **Usa criteri** per consentire di utilizzare criteri per configurare postazioni protette (vedi [Criteri](#)).
 - **Numero di versioni del criterio** — numero massimo di versioni che possono essere create per ciascun criterio.
- Nel campo **Numero di copie di backup per le versioni del Server Dr.Web** impostare il numero massimo di copie di backup conservate che sono state create a un passaggio a una nuova revisione del Server Dr.Web tramite il Pannello di controllo (vedi sezione [Aggiornamento di Server Dr.Web e ripristino da copia di backup](#)). Il valore 0 prescrive di conservare tutte le copie di backup.



- Spuntare il flag **Utilizza l'estensione del protocollo Agent per trasferire i dati di file** per consentire il trasferimento dei dati di file dall'Agent Dr.Web al Server Dr.Web attraverso il protocollo SFTP. Se il flag è tolto, il trasferimento dei dati non viene eseguito.
- Nel campo **Numero di macchine virtuali Lua** impostare il numero massimo di macchine virtuali Lua preliminarmente preparate per le esigenze del web server.
- Nel campo **Script per la creazione di una macchina virtuale Lua** inserire lo script da eseguire durante la creazione in background di una macchina virtuale Lua per le esigenze del web server.

10.3.2. Traffico

10.3.2.1. Aggiornamenti

Nella scheda **Aggiornamenti** vengono impostate limitazioni al quantità di traffico di rete durante la trasmissione degli aggiornamenti tra il Server Dr.Web e gli Agent Dr.Web.

Per maggiori informazioni consultare la sezione [Limitazione del traffico dati delle postazioni](#).

Per impostare limitazioni al traffico di aggiornamento di Agent Dr.Web

1. Nel campo **Numero di processi di aggiornamento simultaneo** viene impostato il numero massimo ammissibile di sessioni di distribuzione aggiornamenti avviate contemporaneamente da questo Server Dr.Web. Quando viene raggiunto il limite indicato, le richieste dagli Agent Dr.Web vengono messe in una coda di attesa. La dimensione della coda di attesa non è limitata. Impostare il valore **0** per togliere la limitazione al numero di processi simultanei.
2. Spuntare il flag **Limita la banda per gli aggiornamenti** per limitare la quantità di traffico di rete durante la trasmissione degli aggiornamenti tra il Server Dr.Web e gli Agent Dr.Web.
Se la spunta al flag è tolta, gli aggiornamenti vengono trasmessi agli Agent Dr.Web senza la limitazione della larghezza di banda.
3. 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 nei limiti della larghezza di banda impostata per il traffico dati cumulativo degli aggiornamenti di tutti gli Agent Dr.Web.
È possibile impostare fino a cinque limitazioni alla velocità di trasmissione di aggiornamenti. Per aggiungere un altro campo di limitazione di velocità, premere il pulsante **+**. Per rimuovere una limitazione, premere il pulsante **-** di fronte alla limitazione che si desidera rimuovere.
4. Nella tabella di calendario viene configurata una modalità di limitazione di trasmissione di aggiornamenti separatamente per ogni 30 minuti di ogni giorno della settimana.
Per modificare la modalità di limitazione di trasmissione di dati, fare clic sul relativo blocco della tabella. Inoltre, è supportata la selezione di più blocchi di tempo tramite trascinamento.



Il colore delle celle cambia ciclicamente secondo lo schema di colori riportato sotto la tabella, cominciando dalla variante con cui la trasmissione di aggiornamenti è consentita senza limitazioni di traffico fino alla variante con cui la trasmissione di aggiornamenti è proibita.

5. Dopo aver finito di modificare, premere il pulsante **Salva** per accettare le modifiche apportate.

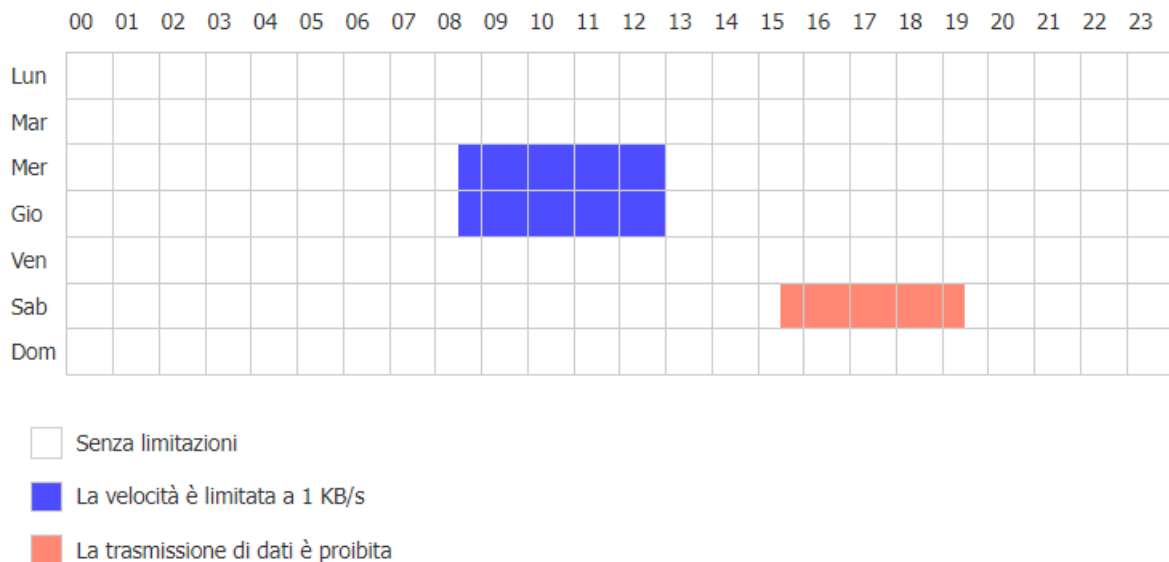
10.3.2.2. Installazioni

Nella scheda **Installazioni** vengono impostate limitazioni alla quantità di traffico di rete nella trasmissione dati nel corso di un'installazione di Agent Dr.Web su postazioni.

Per maggiori informazioni consultare la sezione [Limitazione del traffico dati delle postazioni](#).

Per impostare limitazioni al traffico durante l'installazione di Agent Dr.Web

1. Nel campo **Numero di processi di installazione simultanea** viene impostato il numero massimo ammissibile di sessioni di installazione di Agent Dr.Web avviate contemporaneamente da questo Server Dr.Web. Quando viene raggiunto il limite indicato, le richieste dagli Agent Dr.Web vengono messe in una coda di attesa. La dimensione della coda di attesa non è limitata. Impostare il valore **0** per togliere la limitazione al numero di processi simultanei.
2. Spuntare il flag **Limita il traffico durante l'installazione degli Agent** per limitare la quantità di traffico di rete durante la trasmissione dei dati dal Server Dr.Web sulle postazioni nel processo di installazione di Agent Dr.Web.
Se il flag è tolto, i dati vengono trasmessi durante l'installazione di Agent senza la limitazione della larghezza di banda.
3. Se il flag è spuntato, inserire nel campo **Velocità di trasmissione massima (KB/s)** un valore della velocità massima di trasmissione dati. I dati per l'installazione degli Agent Dr.Web verranno trasmessi nei limiti della larghezza di banda impostata per il traffico dati cumulativo di tutti gli Agent Dr.Web.
È possibile impostare fino a cinque limitazioni alla velocità di trasmissione di dati per l'installazione di Agent Dr.Web. Per aggiungere un altro campo di limitazione di velocità, premere il pulsante **+**. Per rimuovere una limitazione, premere il pulsante **-** di fronte alla limitazione che si desidera rimuovere.
4. Nella tabella di calendario viene configurata una modalità di limitazione di trasmissione di dati separatamente per ogni 30 minuti di ogni giorno della settimana.



Per modificare la modalità di limitazione di trasmissione di dati, fare clic sul relativo blocco della tabella. Inoltre, è supportata la selezione di più blocchi di tempo tramite trascinamento.

Il colore delle celle cambia ciclicamente secondo lo schema di colori riportato sotto la tabella, cominciando dalla variante con cui la trasmissione di dati è consentita senza limitazioni di traffico fino alla variante con cui la trasmissione di dati è proibita.

5. Dopo aver finito di modificare, premere il pulsante **Salva** per accettare le modifiche apportate.

10.3.2.3. Limitazione del traffico dati delle postazioni

Nella rete antivirus di Dr.Web Enterprise Security Suite esiste la possibilità di limitare la velocità di trasmissione di dati tra il Server Dr.Web e gli Agent Dr.Web. Le impostazioni sono suddivise in limitazioni di trasmissione di aggiornamenti e limitazioni di trasmissione di dati durante installazioni di Agent Dr.Web.

Sono possibili le seguenti varianti di limitazione del traffico:

1. Limitazione della velocità generale di trasmissione di dati su tutte le postazioni.
Viene impostata nella sezione di configurazione del Server Dr.Web: voce del menu principale **Amministrazione** → voce del menu di gestione **Configurazione del Server Dr.Web** → scheda **Traffico** → scheda interna **Aggiornamenti** o **Installazioni** → parametro rispettivamente **Limita la banda per gli aggiornamenti** o **Limita il traffico durante l'installazione degli Agent**.
2. Limitazione individuale della velocità di trasmissione degli dati di aggiornamento su concrete postazioni o gruppi di postazioni.
Viene impostata nella sezione di configurazione delle postazioni: la voce del menu principale **Rete antivirus** → selezionare una postazione o un gruppo dalla lista gerarchica



della rete → voce del menu di gestione **Limitazioni degli aggiornamenti** → parametro **Limita la banda per gli aggiornamenti**.

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 Dr.Web, la velocità totale di trasmissione di dati dal Server Dr.Web su tutte le postazioni non eccede il valore indicato. In particolare:
 - a) A prescindere da differenze nelle capacità di canale tra il Server Dr.Web e le postazioni, la velocità di trasmissione di dati viene divisa equamente tra tutte le postazioni.
 - b) Se la capacità di canale tra il Server Dr.Web e una postazione è inferiore al valore di velocità media per una postazione secondo il punto a), per tale postazione viene impostata una limitazione di trasmissione di dati pari alla larghezza di banda massima fino a questa postazione. Il valore residuo di limitazione, analogamente al punto a), viene diviso 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 Dr.Web 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 a cui viene sottratta la limitazione della postazione dal p. a) viene divisa equamente.
 - c) Se la capacità di canale tra il Server Dr.Web e una postazione senza limitazione individuale è inferiore al valore di velocità media per una postazione secondo il punto b), per tale postazione viene impostata una limitazione di trasmissione di dati pari alla larghezza di banda massima fino a questa postazione. Il valore residuo di limitazione, analogamente al punto b), viene diviso equamente tra le altre postazioni senza limitazione individuale.

10.3.3. Rete

10.3.3.1. DNS

Nella scheda **DNS** vengono impostati i parametri delle query inviate al server DNS:

- **Timeout per richieste DNS (s)** — il timeout in secondi per la risoluzione delle richieste DNS dirette/inverse. Impostare 0 per non limitare il tempo di attesa della fine della risoluzione di una richiesta DNS.



- **Numero di richieste DNS ripetute** — il numero massimo di richieste DNS ripetute in caso di una risoluzione di richiesta DNS non riuscita.
- Spuntare il flag **Imposta il tempo di conservazione delle risposte del server DNS** per impostare il tempo di conservazione nella cache (TTL) delle risposte del server DNS.
 - **Per le risposte positive (min)** — il tempo in minuti di conservazione nella cache (TTL) delle risposte positive del server DNS.
 - **Per le risposte negative (min)** — il tempo in minuti di conservazione nella cache (TTL) delle risposte negative del server DNS.
- **Indirizzo del server DNS-over-HTTPS** — l'indirizzo di un server compatibile DNS-over-HTTPS.



Per il corretto funzionamento, è necessario indicare il valore **Qualsiasi** nella sezione **Amministrazione** → **Configurazione generale del repository** → **SAM Dr.Web** → **Certificati validi**.

- **Server DNS** — lista dei server DNS che sostituisce la lista di sistema utilizzata di default.
- **Domini DNS** — lista dei suffissi DNS che sostituisce la lista di sistema utilizzata di default.

10.3.3.2. 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. Se necessario, è possibile impostare nella stringa di indirizzo la porta nel formato `<indirizzo>:<porta>`. Di default viene utilizzata la porta 3128.
- 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 server proxy** e **Password dell'utente del server 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 e Basic Utilizza l'autenticazione Basic. Non è consigliabile utilizzare questo metodo perché il trasferimento di credenziali di autenticazione non viene criptato.



Opzione	Descrizione
Autenticazione e Digest	Utilizza l'autenticazione Digest. Metodo di autenticazione crittografica.
Autenticazione e Digest con il supporto di IE	Utilizzare l'autenticazione Digest. Metodo di autenticazione crittografica. Supporta il browser Internet Explorer versione 6 e inferiori.
Autenticazione e NTLM	Utilizza l'autenticazione NTLM. Metodo di autenticazione crittografica. Per l'autenticazione viene utilizzato il protocollo NTLM di Microsoft.
Autenticazione e NTLM attraverso winbind	Utilizzare l'autenticazione NTLM attraverso l'applicazione esterna winbind. Metodo di autenticazione crittografica.
Autenticazione e GSS-Negotiate	Utilizza l'autenticazione GSS-Negotiate. Metodo di autenticazione crittografica.

10.3.3.3. Trasporto

Nella scheda **Trasporto** si impostano i parametri dei protocolli di trasporto utilizzati dal Server Dr.Web per la comunicazione con i client.

- Dalla lista a cascata **Crittografia** viene selezionato il criterio di cifratura del traffico trasmesso attraverso il canale di comunicazione tra il Server Dr.Web e i client connessi: Agent Dr.Web, Server Dr.Web adiacenti, Installer di rete.
- Dalla lista a cascata **Compressione** viene selezionato il criterio di compressione del traffico trasmesso attraverso il canale di comunicazione tra il Server Dr.Web e i client connessi: Agent Dr.Web, Server Dr.Web adiacenti, Installer di rete.

Per maggiori informazioni su questi parametri v. sezione [Cifratura e compressione del traffico dati](#).

- Se vengono selezionati i valori **Sì** e **Possibile** per la compressione del traffico dati, diventa disponibile una lista a cascata **Livello di compressione**. Da questa lista si può selezionare un livello di compressione dei dati da 1 a 9, dove 1 è il grado minimo e 9 è il grado massimo di compressione.



Per maggiori informazioni consultare la sezione [Cifratura e compressione del traffico dati](#).

- Nel campo **La chiave di crittografia per i ticket della sessione TLS** impostare il percorso del file della chiave di crittografia per i ticket delle sessioni TLS. Si utilizza per riprendere una sessione TLS in base ai ticket delle sessioni (session tickets) che vengono criptati tramite la chiave impostata.



Nella sottosezione **TCP/IP** vengono configurati i parametri delle connessioni con il Server Dr.Web attraverso i protocolli TCP/IP:

- **Indirizzo e Porta** — rispettivamente l'indirizzo IP e il numero di porta dell'interfaccia di rete a cui viene associato questo protocollo di trasporto. Sull'interfaccia con le impostazioni indicate il Server Dr.Web è in ascolto per la comunicazione con gli Agent Dr.Web installati su postazioni.
- Spuntare il flag **Rilevamento** per attivare il servizio di rilevamento di Server Dr.Web.
- Spuntare il flag **Multicasting** per utilizzare la modalità *Multicast over UDP* per il rilevamento del Server Dr.Web.
- **Gruppo Multicast** — indirizzo IP del gruppo multicast in cui è registrato il Server Dr.Web. Viene utilizzato per la comunicazione con gli Agent Dr.Web 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.
- **Nome** — nome di Server Dr.Web. Se non è indicato, viene utilizzato il nome impostato nella scheda **Generali** (v. sopra, in particolare, se nella scheda indicata nessun nome è impostato, 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 dalla descrizione del protocollo. Questo nome viene utilizzato dal servizio di rilevamento per la ricerca del Server da parte degli Agent Dr.Web ecc.
- Solo in SO della famiglia UNIX: nel campo **Percorso** viene impostato il percorso del socket di comunicazione, per esempio, con Agent Dr.Web.



Per maggiori informazioni consultare la sezione [Configurazione delle connessioni di rete](#).

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

10.3.3.4. E-mail

Nella scheda **E-mail** vengono configurati i parametri di invio delle email dal Pannello di controllo, per esempio, come [avvisi](#) dell'amministratore o messaggi per l'invio dei [pacchetti di installazione delle postazioni](#) o per il ripristino della password amministratore:

- **Indirizzo email del mittente** — l'indirizzo di casella email da cui verranno spediti i messaggi.
- **Indirizzo del server** — indirizzo del server SMTP che verrà utilizzato per l'invio delle email.
- **Porta** — porta per la connessione al server SMTP. Di default è la porta 465 se viene aperta una connessione TLS protetta separata, altrimenti è la porta 25.
- **Utente, Password** — se necessario, impostare il nome utente e la password dell'utente del server SMTP se il server SMTP richiede l'autenticazione.



- **Time-out della connessione con il server SMTP** — time-out in secondi per lo stabilimento della connessione con il server SMTP. Il valore è un numero intero positivo maggiore o uguale a 1.
- Dalla lista a cascata **Protezione della connessione** selezionare il tipo di scambio di dati crittografati:
 - **STARTTLS** — il passaggio alla connessione protetta viene effettuato attraverso il comando `STARTTLS`. Di default per la connessione è previsto l'utilizzo della porta 25.
 - **SSL/TLS** — aprì una connessione protetta crittografata separata. Di default per la connessione è previsto l'utilizzo della porta 465.
 - **No** — non usare la crittografia. Lo scambio di dati avverrà su una connessione non protetta.
- Spuntare il flag **Utilizza autenticazione CRAM-MD5** per utilizzare l'autenticazione *CRAM-MD5* sul mail server.
- Spuntare il flag **Utilizza autenticazione DIGEST-MD5** per utilizzare l'autenticazione *DIGEST-MD5* sul mail server.
- Spuntare il flag **Utilizza autenticazione LOGIN** per utilizzare l'autenticazione *LOGIN* sul mail server.
- Spuntare il flag **Utilizza autenticazione AUTH-NTLM** per utilizzare l'autenticazione *AUTH-NTLM* sul mail server.
- Spuntare il flag **Utilizza autenticazione Plain** per utilizzare l'autenticazione *plain text* sul mail server.
- Spuntare il flag **Controlla la correttezza del certificato** per controllare la correttezza del certificato TLS del mail server. Nel campo **Certificati TLS** indicare il percorso dei certificati TLS.
- Spuntare il flag **Modalità di debug** per ottenere un log dettagliato di sessione SMTP.
- Nel campo **Indirizzi e-mail dei destinatari** è possibile impostare indirizzi di caselle di posta elettronica per testare l'invio di email. Premere il pulsante **Invia un messaggio di test** per inviare un'email di test (similmente ad [avviso](#) di Server Dr.Web) secondo le impostazioni definite in questa sezione.

10.3.3.5. 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.

Per utilizzare il cluster, impostare i seguenti parametri:

- **Gruppo multicast** — l'indirizzo IP del gruppo multicast attraverso cui i Server Dr.Web si scambieranno informazioni.
- **Porta** — il numero di porta dell'interfaccia di rete a cui è associato il protocollo di trasporto per la trasmissione delle informazioni nel gruppo multicast.
- **Durata di vita** — la durata di vita di un datagramma nel trasferimento dati nel cluster di Server Dr.Web.



- **Interfaccia** — l'indirizzo IP dell'interfaccia di rete a cui è associato il protocollo di trasporto per la trasmissione delle informazioni nel gruppo multicast.



Le caratteristiche della creazione di un cluster dei Server Dr.Web sono riportate nella sezione [Cluster dei Server Dr.Web](#).

10.3.3.6. Download

Nella scheda **Download** vengono configurati i parametri di Server Dr.Web utilizzati nella generazione dei file di installazione di Agent Dr.Web per le postazioni della rete antivirus. In seguito, questi parametri vengono utilizzati durante la connessione dell'installer di Agent Dr.Web al Server Dr.Web:

- **Indirizzo di Server Dr.Web** — l'indirizzo IP o il nome a dominio di Server Dr.Web. Se l'indirizzo di Server Dr.Web non è impostato, viene utilizzato il nome di computer restituito dal sistema operativo.



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

- **Porta** — il numero di porta da utilizzare per la connessione dell'installer di Agent Dr.Web al Server Dr.Web.

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 Server Dr.Web** → scheda **Rete** → scheda **Trasporto**).

Le impostazioni della sezione **Download** vengono memorizzate nel file di configurazione `download.conf` (v. documento **Allegati**, [F3. File di configurazione download.conf](#)).

10.3.3.7. 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**.

Principi di base del funzionamento degli aggiornamenti per gruppi:

1. Se gli aggiornamenti per gruppi sono attivati, per tutte le postazioni connesse a questo Server Dr.Web l'aggiornamento si svolgerà in due fasi:
 - a) Le postazioni sono in ascolto dei gruppi multicast impostati di cui fa parte il Server Dr.Web. Se arrivano gli aggiornamenti per gruppi, le postazioni li scaricano attraverso *multicast over UDP*.



- b) Dopo la trasmissione degli aggiornamenti per gruppi il Server Dr.Web invia alle postazioni un avviso standard di disponibilità di aggiornamenti. Tutto quello che è stato impossibile scaricare tramite gli aggiornamenti per gruppi viene ulteriormente scaricato dalle postazioni come nel caso di aggiornamento standard attraverso il protocollo TCP.
2. Se gli aggiornamenti di gruppo sono disattivati, l'aggiornamento su tutte le postazioni viene eseguito solo nel modo regolare — 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 la frammentazione, si consiglia di impostare un valore inferiore all'MTU (Maximum Transmission Unit) della rete in uso.
- **Tempo di trasmissione del file (ms)** — durante l'intervallo specificato viene trasmesso un file di aggiornamento, dopodiché il Server Dr.Web 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 di gruppo (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 al gruppo multicast.
Un valore piccolo di intervallo potrebbe causare notevoli perdite durante la trasmissione dei pacchetti e sovraccaricare la rete. Si raccomanda di non modificare questa impostazione.
- **Intervallo tra le richieste di ritrasmissione (ms)** — con questo intervallo gli Agent Dr.Web inviano le richieste di ritrasmissione 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 richiesta di trasmissione ripetuta di pacchetti persi è arrivata dagli Agent Dr.Web, il Server Dr.Web ritiene che tutti gli Agent Dr.Web abbiano ottenuto con successo i file di aggiornamento e inizia a trasmettere il file successivo.
- **Intervallo per accumulare le richieste di ritrasmissione (ms)** — durante questo intervallo il Server Dr.Web accumula le richieste degli Agent Dr.Web per la ritrasmissione dei pacchetti persi.
Gli Agent Dr.Web chiedono l'invio ripetuto dei pacchetti persi. Il Server Dr.Web accumula queste richieste durante il tempo specificato, dopodiché 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** — l'indirizzo IP del gruppo multicast attraverso cui le postazioni riceveranno gli aggiornamenti di gruppo.



- **Porta** — il numero di porta dell'interfaccia di rete del Server Dr.Web a cui è associato 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 Dr.Web stesso.

- **Durata di vita** — la durata di vita di un datagramma nel trasferimento dati nel processo di aggiornamento multicast.
- **Interfaccia** — l'indirizzo IP dell'interfaccia di rete del Server Dr.Web a cui è associato 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.

Nella sezione **Lista di controllo degli accessi** vengono impostate limitazioni agli indirizzi di rete delle postazioni che riceveranno gli aggiornamenti per gruppi:

- Le postazioni cui è consentito ricevere aggiornamenti per gruppi saranno in ascolto dei gruppi multicast impostati e riceveranno gli aggiornamenti secondo lo schema standard (vedi [procedura 1](#)).
- Le postazioni cui è vietato ricevere aggiornamenti per gruppi non sono in ascolto dei gruppi multicast impostati per cercare aggiornamenti, ma scaricano tutti gli aggiornamenti attraverso TCP (vedi [procedura 2](#)).

Le liste vengono configurate similmente alla configurazione delle liste della sezione [Sicurezza](#).

10.3.4. Statistiche

Nella scheda **Statistiche** vengono impostate le informazioni statistiche che verranno registrate nel log, salvate nel database del Server Dr.Web e successivamente potranno essere visualizzate nella sezione [statistiche](#) del Pannello di controllo.

Per aggiungere al database il rispettivo tipo di 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, i monitor ecc.) installati sulla postazione e la registrazione delle informazioni nel database.
- **Sessioni degli utenti di postazioni** — abilita il monitoraggio delle sessioni degli utenti delle postazioni e la registrazione nel database dei nomi utente degli utenti loggati al sistema su un computer con l'Agent Dr.Web installato.
- **Avvio/arresto dei componenti** — abilita il monitoraggio delle informazioni sull'avvio e l'arresto dei componenti di Antivirus (Scanner, i monitor ecc.) su postazioni e la registrazione delle informazioni nel database.
- **Minacce alla sicurezza rilevate** — abilita il monitoraggio del rilevamento delle minacce alla sicurezza delle postazioni e la registrazione delle informazioni nel database.

Se il flag **Minacce alla sicurezza rilevate** è spuntato, è inoltre possibile configurare le impostazioni aggiuntive delle statistiche su minacce.

- Spuntare il flag **Tieni traccia delle epidemie** per attivare la modalità di avviso amministratore su casi di epidemie di virus. Se il flag è tolto, gli avvisi di infezioni di virus vengono inviati in modalità normale. Se il flag è spuntato, si possono inoltre impostare i seguenti parametri di monitoraggio delle epidemie di virus:
 - **Periodo di divieto di inviare avvisi** — intervallo di tempo in secondi dopo l'invio di un avviso di epidemia, durante il quale gli avvisi di infezioni singole delle postazioni non verranno inviati.
 - **Periodo di conteggio delle postazioni infette** — intervallo di tempo in secondi durante cui deve arrivare il numero impostato di messaggi di postazioni infette in modo che venga inviato un avviso di epidemia.
 - **Numero di avvisi** — numero di messaggi di infezioni che devono arrivare nel periodo di tempo impostato affinché il Server Dr.Web invii all'amministratore un singolo avviso di epidemia racchiudente tutti i casi di infezione (l'avviso **Un'epidemia nella rete**).
 - **Numero delle minacce più diffuse** — il numero delle minacce più comuni da includere nel report su epidemie.
- Spuntare il flag **Raggruppa i report di Protezione preventiva** per inviare un singolo report di riepilogo su più eventi di Protezione preventiva. Se il flag è tolto, gli eventi di Protezione preventiva arriveranno in avvisi separati a prescindere dal loro numero. Se il flag è spuntato, è inoltre possibile impostare i seguenti parametri di raggruppamento dei report:
 - **Periodo di divieto di inviare avvisi** — intervallo di tempo in secondi dopo l'invio di un report di riepilogo sugli eventi di Protezione preventiva, durante il quale gli avvisi di eventi singoli non verranno inviati.



- **Periodo di conteggio degli eventi** — intervallo di tempo in secondi durante cui deve verificarsi il numero impostato di eventi di Protezione preventiva in modo che venga inviato un report di riepilogo.
- **Numero di eventi** — numero di eventi di Protezione preventiva che devono arrivare nel periodo di tempo impostato affinché il Server Dr.Web invii all'amministratore un singolo report di riepilogo su questi eventi (l'avviso **Report di riepilogo di Protezione preventiva**).
- **Numero dei processi più attivi** — numero dei processi più comuni che hanno eseguito un'azione sospetta, da includere nel report di Protezione preventiva.
- Per abilitare l'invio delle statistiche sulle minacce alla sicurezza di postazioni 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 Dr.Web).

È obbligatorio soltanto il campo **Intervallo** di invio delle statistiche.

- **Terminazioni di connessioni anomale** — consente di tenere traccia delle connessioni client terminate in modo anomalo e avere la possibilità di inviare avvisi corrispondenti all'amministratore.

Configurare le seguenti impostazioni delle terminazioni di connessioni anomale:

- **Periodo di divieto di inviare avvisi** — intervallo di tempo in secondi dopo l'invio di un avviso di disconnessioni multiple, durante il quale gli avvisi di disconnessioni singole non verranno inviati.
- **Periodo di conteggio delle connessioni terminate** — intervallo di tempo in secondi durante cui deve verificarsi il numero impostato di disconnessioni client in modo che venga inviato un avviso corrispondente.
- **Numero di connessioni per un avviso di disconnessioni singole** — numero minimo di connessioni che devono essere interrotte con un indirizzo durante il periodo di conteggio in modo che venga inviato un avviso di una disconnessione anomala singola (l'avviso **Terminazione di connessione anomala**).
- **Numero di connessioni per un avviso di disconnessioni multiple** — numero minimo di connessioni che devono essere interrotte durante il periodo di conteggio in modo che venga inviato un avviso unico di disconnessioni anomale multiple (l'avviso **Registrato un gran numero di connessioni terminate in modo anomalo**).
- **Durata delle connessioni brevi** — se la durata di una connessione client terminata è inferiore a quella specificata, quando viene raggiunto il numero di connessioni impostato, verrà inviato un avviso di disconnessioni singole (l'avviso **Terminazione di connessione anomala**), indipendentemente dal periodo di conteggio. In tale caso la connessione non deve essere interrotta ulteriormente da connessioni più lunghe, e non deve essere inviato un avviso di disconnessioni anomale multiple (l'avviso **Registrato un gran numero di connessioni terminate in modo anomalo**).
- **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 di Agent** — abilita il monitoraggio delle informazioni sulle installazioni di Agent Dr.Web su postazioni e la registrazione delle informazioni nel database.
- **Dispositivi bloccati** — abilita il monitoraggio delle informazioni sui dispositivi bloccati dal componente Office control e la registrazione delle informazioni nel database.
- **Statistiche di Controllo applicazioni sull'attività dei processi** — abilita il monitoraggio delle informazioni sull'attività dei processi su postazioni, registrata da Controllo applicazioni, e la registrazione delle informazioni nel database.
- **Statistiche di Controllo applicazioni sul blocco dei processi** — abilita il monitoraggio delle informazioni sui blocchi dei processi su postazioni da parte di Controllo applicazioni e la registrazione delle informazioni nel database.
- **Blocchi multipli Controllo applicazioni** — consente di tenere traccia dei blocchi di processi multipli da parte di Controllo applicazioni e avere la possibilità di inviare avvisi corrispondenti all'amministratore.

Configurare le seguenti impostazioni degli eventi:

- **Periodo di divieto di inviare avvisi** — intervallo di tempo in secondi dopo l'invio di un report di riepilogo sui processi bloccati da Controllo applicazioni, durante il quale gli avvisi di blocchi singoli non verranno inviati.
- **Periodo di conteggio dei processi bloccati** — intervallo di tempo in secondi durante cui deve essere bloccato il numero impostato di processi in modo che venga inviato un report di riepilogo.
- **Numero di blocchi** — numero di eventi di processi bloccati da Controllo applicazioni che devono arrivare nel periodo di tempo impostato affinché il Server Dr.Web invii all'amministratore un singolo report di riepilogo su questi eventi (l'avviso **Registrato un gran numero di blocchi Controllo applicazioni**).
- **Numero dei profili più diffusi** — numero dei profili più diffusi in base a cui veniva effettuato il blocco, da includere nell'avviso di blocchi multipli.
- **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** — abilita il monitoraggio dello stato (lista dei componenti, modifiche) dei database dei virus su postazione e la registrazione delle informazioni nel database. Il flag è disponibile solo se è spuntato il flag **Stato delle postazioni**.
- **Dati sulla posizione geografica** — permette di ottenere dati sulla posizione geografica delle postazioni e di registrare le informazioni nel database.
- **Spazio su disco sulle postazioni** — permette di ottenere informazioni sullo spazio su disco sulle postazioni e registrare le informazioni nel database.
- **Raccogli informazioni sui dispositivi** — permette a Server Dr.Web di raccogliere informazioni sui dispositivi che vengono collegati alla postazione.



- **Raccogli informazioni sugli utenti** — permette a Server Dr.Web di raccogliere informazioni sugli utenti sulla postazione.



Le impostazioni di raccolta informazioni analoghe, che consentono ad Agent Dr.Web di inviare dati a Server Dr.Web, sono presenti in Agent Dr.Web. Le impostazioni di cui sopra determinano se Server Dr.Web conserverà ed elaborerà i dati ricevuti da Agent Dr.Web.

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).



Una descrizione dettagliata delle statistiche è riportata in sezione [Visualizzazione delle statistiche della postazione](#).

Nella tabella sottostante è riportata la corrispondenza dei flag dalla sezione **Statistiche** nelle impostazioni di Server Dr.Web 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 10-1. Corrispondenza delle impostazioni di Server Dr.Web e delle voci del menu di gestione

Impostazioni del Server Dr.Web	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 → Dispositivi rilevati
Lista dei moduli delle 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 → Minacce Statistiche → Statistiche delle minacce



Impostazioni del Server Dr.Web	Voci del menu
	Statistiche → Eventi di Protezione preventiva
Errori di scansione	Statistiche → Errori
Statistiche di scansione	Statistiche → Statistiche di scansione
Installazioni di Agent	Statistiche → Installazioni di Agent
Dispositivi bloccati	Statistiche → Dispositivi bloccati
Statistiche di Controllo applicazioni sull'attività dei processi	Statistiche → Eventi di Controllo delle applicazioni
Statistiche di Controllo applicazioni sul blocco dei processi	Amministrazione → Controllo delle applicazioni → Prontuario applicazioni .
Log di esecuzione dei task sulla postazione	Statistiche → Task
Stato delle postazioni	Statistiche → Stato Statistiche → Database dei virus
Stato dei database dei virus	Statistiche → Database dei virus

10.3.5. Sicurezza

Nella scheda **Sicurezza** vengono impostate limitazioni agli indirizzi di rete da cui gli Agent Dr.Web, gli installer di rete e gli altri Server Dr.Web (adiacenti) possono accedere a questo Server Dr.Web.

Il log di verifica di Server Dr.Web 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 agli indirizzi IP da cui gli Agent Dr.Web possono connettersi a questo Server Dr.Web.
- **Installer** — lista delle limitazioni agli indirizzi IP da cui gli installer di Agent Dr.Web possono connettersi a questo Server Dr.Web.
- **Relazioni** — lista delle limitazioni agli indirizzi IP da cui i Server Dr.Web adiacenti possono connettersi a questo Server Dr.Web.
- **Servizio di rilevamento** — lista delle limitazioni agli indirizzi IP da cui le richieste broadcast vengono accettate dal [servizio di rilevamento di Server Dr.Web](#).

Per configurare le limitazioni di accesso (vengono impostate separatamente per gli Agent, l'Installazione, i Server Dr.Web adiacenti o il Servizio di rilevamento):

1. Spuntare il flag **Usa questa lista di controllo di accesso** per impostare liste di indirizzi consentiti o proibiti. Se il flag è deselezionato, tutte le connessioni saranno consentite.
2. Per consentire l'accesso da un determinato indirizzo TCP, includerlo nella lista **TCP: consentito** o **TCPv6: consentito**.
3. Per proibire un indirizzo TCP, includerlo nella lista **TCP: negato** o **TCPv6: negato**.
4. 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**.

Per modificare una lista di indirizzi:

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**.



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 indica reti con una maschera: `255.255.255.0`
Contiene 254 indirizzi.
Gli indirizzi di host in queste reti sono di tipo: `195.136.12.*`




2. Il prefisso 8 indica reti con una maschera 255.0.0.0
Contiene fino a 16777214 indirizzi (256*256*256-2).
Gli indirizzi di host in queste reti sono di tipo: 125.*.*.*

10.3.6. Cache

Nella scheda **Cache** vengono configurati i parametri di pulizia della cache di server:

- **Periodicità di pulizia della cache** — periodicità di pulizia completa della cache.
- **File in quarantena** — periodicità di rimozione dei file in Quarantena sul lato Server Dr.Web.
- **File del repository** — periodicità di rimozione dei file nel repository.
- **Cache di file** — periodicità di pulizia della cache dei file.
- **Pacchetti di installazione** — periodicità di rimozione dei pacchetti di installazione individuali e di gruppo.

Premere il pulsante  **Rimuovi adesso tutti i pacchetti di installazione** per rimuovere tutti i pacchetti di installazione individuali e di gruppo precedentemente creati che si trovano nella directory `installers-cache` della directory `var`. Notare: quando si accede a questi pacchetti per scaricarli, verranno nuovamente creati, il che può richiedere un certo tempo.



Impostando valori numerici, prestare attenzione alle liste a cascata con le unità di misura della periodicità.

10.3.7. Database

Nella scheda **Database** viene selezionato il database necessario per il funzionamento di Server Dr.Web.



La struttura del database di Server Dr.Web è disponibile come manuale separato con lo stesso nome. Il documento può essere aperto dalla sezione **Supporto** nel Pannello di controllo della sicurezza Dr.Web.

Per configurare i parametri di utilizzo del database

1. Nel campo **Numero di connessioni** impostare il numero massimo ammissibile di connessioni di Server Dr.Web con il database.

In caso di utilizzo del database incorporato, non è consigliabile modificare il valore di default. In caso di utilizzo di un database esterno, potrebbe essere necessario un valore di parametro più grande. Per le raccomandazioni per la selezione del valore ottimale v. documento **Allegati**, sezione [Carico su Server Dr.Web e parametri di configurazione raccomandati](#).



Il database incorporato è progettato per la connessione al Server Dr.Web di circa 400–600 postazioni. Se lo permettono la configurazione dell'hardware del computer su cui è installato il Server Dr.Web e il carico di altri compiti eseguiti su questo computer, è possibile connettere circa 1000–1500 postazioni.

Altrimenti, è necessario utilizzare un database esterno. A seconda della configurazione e del carico sul computer che svolge le funzioni di Server Dr.Web, il database esterno può essere collocato sullo stesso computer o su un computer dedicato.

Se è utilizzato un database esterno e al Server Dr.Web sono connesse più di 10000 postazioni, sono consigliabili i seguenti requisiti minimi:

- processore con velocità 3GHz,
- da 6 core del processore,
- 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.

In caso di utilizzo di una rete con un numero elevato di connessioni client a Server Dr.Web, prima di modificare il valore, si consiglia di ottenere consulenza nel servizio di supporto tecnico dell'azienda Doctor Web.

2. Spuntare il flag **Pulisci il database automaticamente dopo le procedure di manutenzione** per eseguire la pulizia differita del database automaticamente dopo l'inizializzazione, l'aggiornamento e l'importazione. Se il flag è tolto, la pulizia automatica non verrà eseguita. In questo caso è consigliato configurare il task **Pulizia del database** nel calendario di Server Dr.Web o effettuare la pulizia manualmente attraverso la sezione [Gestione del database](#).

Per l'esecuzione della pulizia automatica viene creato un task nascosto nel calendario di Server Dr.Web. Il task viene eseguito la notte successiva alle procedure di manutenzione indicate, alle 01:17 secondo l'ora locale di Server Dr.Web. Il task viene eseguito solo se nel calendario di Server Dr.Web non è pianificato un altro task **Pulizia del database** entro le ventiquattro ore successive alle procedure di manutenzione indicate.

3. Dalla lista a cascata **Database** selezionare il tipo di database:

- **MySQL** — database esterno,
- **ODBC** — per utilizzare un database esterno tramite la connessione ODBC,



Se si verificano avvisi o errori nel funzionamento di Server Dr.Web con il DBMS Microsoft SQL Server attraverso ODBC, è necessario assicurarsi che sia utilizzata l'ultima versione disponibile del DBMS per questa edizione.

Per scoprire come determinare la disponibilità di service pack, consultare la seguente pagina Microsoft: <https://learn.microsoft.com/troubleshoot/sql/general/determine-version-edition-update-level>.

- **Oracle** — database esterno per le piattaforme ad eccezione di FreeBSD,



Se viene utilizzato il DBMS Oracle esterno 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).
4. Configurare le impostazioni necessarie di utilizzo del database:
- Per il database incorporato, se necessario, inserire nel campo **Nome del file** il percorso completo del file di database e impostare la dimensione della memoria cache e la modalità di registrazione dei dati.
 - I parametri per i database esterni sono descritti in documento **Allegati**, [Allegato A. Impostazioni per l'utilizzo dei DBMS. Parametri dei driver dei DBMS.](#)
5. Per applicare le impostazioni, premere il pulsante **Salva**.



Il pacchetto di Server Dr.Web contiene client incorporati dei DBMS supportati dunque:

- Se si intende utilizzare i client DBMS incorporati, forniti insieme a Server Dr.Web, nel corso dell'installazione (l'aggiornamento) di Server Dr.Web nelle impostazioni dell'installer assicurarsi che l'installazione del relativo client DBMS sia consentita nella sezione **Supporto dei database**.
- Se si intende utilizzare come database esterno il database Oracle attraverso la connessione ODBC, nel corso dell'installazione (l'aggiornamento) di Server Dr.Web nelle impostazioni dell'installer annullare l'installazione del client incorporato per il DBMS Oracle (nella sezione **Supporto dei database** → **Driver del database Oracle**). Altrimenti, l'utilizzo del database attraverso ODBC non sarà possibile a causa di conflitto di librerie.

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

Di default è previsto l'utilizzo del database incorporato. La scelta di questa modalità crea un significativo carico computazionale sul Server Dr.Web. Nel caso di una rete antivirus di dimensioni significative, si consiglia di utilizzare un database esterno. La procedura di cambio del tipo di database è descritta in documento **Allegati**, sezione [Cambio del tipo di database di Dr.Web Enterprise Security Suite](#).



È prevista la possibilità di eseguire le operazioni di pulizia del database utilizzato da Server Dr.Web, in particolare: rimuovere record degli eventi, nonché informazioni sulle postazioni che non visitavano il Server Dr.Web per un determinato periodo. Per ripulire il database, passare alla sezione del [calendario del Server Dr.Web](#) e creare un task corrispondente.



10.3.7.1. Ripristino dei database

In caso di un guasto al database incorporato **SQLite3** c'è la possibilità di ripristinare il database danneggiato attraverso i mezzi standard.

In caso di danneggiamento del database, viene eseguita la seguente sequenza di azioni:

1. Se il database è danneggiato, il Server Dr.Web non si avvia e non funziona:
 - a) Nel processo di funzionamento del Server Dr.Web: se un errore si è verificato durante un'interazione normale con il database incorporato, il Server Dr.Web viene arrestato in modo automatico.
 - b) Nel processo di avvio del Server Dr.Web: se nelle impostazioni del database **SQLite3** nella lista a cascata **Verifica dell'integrità dell'immagine** è selezionata l'opzione **Rapida** o **Completa**, viene controllata in modo automatico l'integrità dell'immagine del database. In caso di rilevamento di un errore, il Server Dr.Web non viene avviato.
2. Per poter avviare il Server Dr.Web, è necessario ripristinare il database danneggiato:
 - a) Se nelle impostazioni del database **SQLite3** è spuntato il flag **Ripristina immagine corrotta in automatico**, ad avvio di Server Dr.Web viene ripristinata automaticamente l'immagine danneggiata del database.
 - b) Se il ripristino automatico dell'immagine del database è disattivato, è possibile utilizzare l'opzione `repairdb` all'avvio di Server Dr.Web dalla riga di comando (v. inoltre documento **Allegati**, [H3.3. Comandi di gestione del database](#)).

10.3.8. 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 **Protocollo di Agent Dr.Web** per attivare il protocollo di interazione del Server Dr.Web con gli Agent Dr.Web.
- Spuntare il flag **Protocollo Microsoft NAP Health Validator** per attivare il protocollo di interazione del Server Dr.Web con il componente di controllo dell'operatività del sistema Microsoft NAP Validator.
- Spuntare il flag **Protocollo di installer di Agent Dr.Web** per attivare il protocollo di interazione del Server Dr.Web 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 Dr.Web in un sistema 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**.
- Spuntare il flag **Protocollo di Server proxy Dr.Web** per attivare il protocollo di interazione del Server Dr.Web con i Server proxy Dr.Web.



- Spuntare il flag **Estensione del Pannello di controllo della sicurezza Dr.Web** per gestire il Server Dr.Web e la rete antivirus attraverso 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 Dr.Web e la rete antivirus potranno essere gestiti solo 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 utilizzare l'estensione Dr.Web Server FrontDoor che consente la connessione dell'utility di diagnostica remota del Server Dr.Web (v. inoltre [Accesso remoto al Server Dr.Web](#)).
- Spuntare il flag **Estensione dell'agent SNMP Dr.Web** per consentire al Server Dr.Web lo scambio di informazioni con i sistemi di gestione della rete attraverso il protocollo SNMP (v. inoltre [Configurazione dell'agent SNMP Dr.Web](#)).
- Spuntare il flag **Estensione Yandex Locator** per consentire l'utilizzo dell'estensione Yandex Locator per determinare la posizione dei dispositivi mobili connessi al Server Dr.Web.
 - Nel campo **Chiave API** immettere la propria chiave API ottenuta tramite il servizio Yandex corrispondente.



Se viene abilitata l'estensione Yandex Locator, ma non viene impostata la chiave API, l'estensione non sarà attiva.



Informazioni dettagliate sull'utilizzo e sulla configurazione dell'estensione Yandex Locator sono ritrovabili nel documento **Allegati**, nella sezione [Rilevamento automatico della posizione di una postazione con SO Android](#).

10.3.9. 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 è possibile visualizzare la posizione del Server Dr.Web su una mappa geografica.

Per visualizzare la posizione del Server Dr.Web sulla mappa

1. Nei campi **Latitudine** e **Longitudine** inserire le coordinate geografiche del Server Dr.Web nel formato gradi decimali (Decimal Degrees).
2. Premere il pulsante **Salva** per memorizzare i dati inseriti nel file di configurazione del Server Dr.Web.

Non è necessario riavviare il Server Dr.Web per visualizzare la mappa. Tuttavia, per applicare le coordinate geografiche modificate, il Server Dr.Web dovrà essere riavviato.



3. Nella scheda **Posizione** viene visualizzata l'anteprima della mappa OpenStreetMap 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**.

10.3.10. Licenze

Nella scheda **Licenze** vengono configurate la distribuzione delle licenze tra i Server Dr.Web, nonché le impostazioni dei report sull'utilizzo delle licenze.

Impostazioni dell'avviso sulla limitazione sul numero di licenze nella chiave di licenza

- **Numero di licenze rimanenti** — numero massimo di licenze rimanenti, raggiunto il quale verrà inviato l'avviso **Limitazione sul numero di licenze nella chiave di licenza**.
- **Percentuale delle licenze rimanenti** — percentuale massima delle licenze rimanenti, raggiunta la quale verrà inviato l'avviso **Limitazione sul numero di licenze nella chiave di licenza**.

Impostazioni per il report sull'utilizzo delle licenze



Nel caso di invio dei report tra Server Dr.Web, queste impostazioni devono essere configurate sul Server Dr.Web principale, ma verranno utilizzate dai Server Dr.Web subordinati.

Se le relazioni con i Server Dr.Web adiacenti non sono configurate, queste opzioni vengono utilizzate solo dal Server Dr.Web corrente per i suoi report personali.

- **Periodo di creazione del report** — periodicità con cui sul Server Dr.Web verranno creati i report sulle chiavi di licenza da esso utilizzate.
Se un report sull'utilizzo delle licenze viene creato da un Server Dr.Web subordinato, subito dopo la creazione questo report viene inviato sul Server Dr.Web principale.
I report creati vengono inoltre inviati ad ogni connessione (incluso il riavvio) del Server Dr.Web, e inoltre, quando sul Server Dr.Web principale cambia il numero di licenze rilasciate.
- **Periodo di conteggio delle postazioni attive per il report sulle licenze** — periodo durante cui verrà conteggiato il numero di postazioni attive per la creazione del report sull'utilizzo delle licenze. Il valore 0 prescrive di prendere in considerazione nel report tutte le postazioni, indipendentemente dal loro stato di attività.



Impostazioni per il Server Dr.Web che rilascia licenze

- **Periodo di rinnovo automatico delle licenze rilasciate** — periodo di tempo per cui vengono rilasciate le licenze dalla chiave su questo Server Dr.Web. Dopo la fine di questo periodo viene eseguito il rinnovo automatico delle licenze rilasciate per lo stesso periodo. Il rinnovo automatico verrà eseguito fino a quando durerà il periodo di distribuzione delle licenze impostato in Gestione licenze al passaggio 5.
Questo meccanismo assicura il ritorno delle licenze sul Server Dr.Web principale nel caso in cui il Server Dr.Web subordinato verrà disconnesso e non potrà restituire le licenze rilasciate.
- **Periodo di sincronizzazione delle licenze** — periodicità di sincronizzazione delle informazioni sulle licenze rilasciate tra i Server Dr.Web. La sincronizzazione delle licenze consentirà di determinare che il numero di licenze rilasciate dal Server Dr.Web principale corrisponde al numero di licenze ricevute dal Server Dr.Web subordinato. Questo meccanismo consente di identificare errori e casi di falsificazione nel trasferimento delle licenze.

Impostazioni per il Server Dr.Web che riceve licenze

- **Intervallo per il rinnovo preliminare delle licenze ricevute** — intervallo di tempo prima della fine del periodo di rinnovo automatico delle licenze ricevute dal Server Dr.Web adiacente, a partire da cui questo Server Dr.Web richiede il rinnovo automatico preliminare di queste licenze.

L'uso di questa impostazione dipende dal tipo di connessione selezionato nell'impostazione **Parametri di connessione** durante la configurazione della relazione tra i Server Dr.Web (v. sezione [Configurazione delle relazioni tra i Server Dr.Web](#)):

- Per il tipo di connessione periodica: se il periodo di riconnessione definito nell'impostazione della relazione è superiore al **Periodo di rinnovo automatico delle licenze rilasciate** definito sul Server Dr.Web che ha rilasciato le licenze, il rinnovo automatico di queste licenze verrà inizializzato prima che finisca il **Periodo di rinnovo automatico delle licenze rilasciate**.
- Per la connessione permanente: questa impostazione non viene utilizzata.



Per informazioni dettagliate sulla distribuzione di licenze tra Server Dr.Web v. sezione [Distribuzione delle licenze attraverso le relazioni tra i server](#).

10.3.11. Log

Nella scheda **Log** viene configurata la registrazione del log di funzionamento di Server Dr.Web:

- Dalla lista a cascata **Livello di dettaglio del log di Server Dr.Web** selezionare il livello di dettaglio per la registrazione del log di funzionamento di Server Dr.Web.
- **Numero massimo di file** — il numero massimo di file di log da conservare (compresi quello corrente e quelli archiviati).



- **Modalità di rotazione del log di Server Dr.Web** — la modalità di rotazione del log di funzionamento di Server Dr.Web. Selezionare uno dei valori disponibili:
 - **rotazione per dimensione** determina una limitazione alla dimensione di ciascuno dei file di log.

Dimensione massima di ciascun file — la dimensione massima consentita di ciascun file di log. Quando il file corrente raggiunge la dimensione impostata, viene archiviato con il relativo cambio di nome, e viene creato un nuovo file di log.
 - **rotazione per tempo** determina la durata della registrazione di ciascuno dei file di log.

Tempo massimo di registrazione del file — la durata massima per la registrazione di ciascun file di log. Quando il tempo di registrazione del file raggiunge la durata impostata, esso viene archiviato con il relativo cambio di nome, e viene creato un nuovo file di log.
- Spuntare il flag **Archivia file di log** per archiviare i vecchi file di log nel processo di rotazione.



Per rendere effettive le modifiche apportate, è necessario riavviare Server Dr.Web.

Il riavvio può essere eseguito sia tramite il Pannello di controllo e sia tramite il comando console corrispondente.



Informazioni dettagliate sul log di Server Dr.Web sono ritrovabili nella sezione [Log del Server Dr.Web](#).

10.4. Accesso remoto al Server Dr.Web



Per connettere l'utility di diagnostica remota del Server Dr.Web, è necessario attivare l'estensione Dr.Web Server FrontDoor. 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 Dr.Web 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 Dr.Web attraverso l'utility di diagnostica remota.

Per configurare i parametri di connessione dell'utility di diagnostica remota di Server Dr.Web

1. Selezionare la voce **Amministrazione** nel 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 il protocollo di connessione:




- Spuntare il flag **Utilizza TLS** per consentire la connessione dell'utility di diagnostica remota a Server Dr.Web tramite il protocollo TLS. Se il flag è deselezionato, la connessione sarà possibile solo tramite il protocollo TCP.
Per una connessione tramite il protocollo TLS, configurare le seguenti impostazioni:
 - **Certificato** — file del certificato che verrà controllato al momento della connessione. Nella lista a cascata sono elencati i certificati disponibili dalla directory di Server Dr.Web.
 - **Chiave privata SSL** — file della chiave privata SSL che verrà controllata al momento della connessione. Nella lista a cascata sono elencate le chiavi private disponibili dalla directory di Server Dr.Web.
 - Nel campo **La chiave di crittografia per i ticket della sessione TLS** impostare il percorso del file della chiave di crittografia per i ticket delle sessioni TLS. Si utilizza per riprendere una sessione TLS in base ai ticket delle sessioni (session tickets) che vengono criptati tramite la chiave impostata.
 - **Lista delle cifre consentite** — stringa che definisce la lista delle cifre dal pacchetto OpenSSL, consentite per l'utilizzo nelle connessioni con i client. Se si lascia vuoto il campo, verrà utilizzato il valore `DEFAULT` che significa `ALL: !EXPORT: !LOW: !aNULL: !eNULL: !SSLv2`.

3. Configurare le impostazioni di interfaccia per la connessione:

- **Indirizzo** — indirizzo IP su cui il Server Dr.Web è in ascolto per la connessione dell'utility di diagnostica remota.
- **Porta** — porta su cui il Server Dr.Web è in ascolto per la connessione dell'utility di diagnostica remota. Di default viene utilizzata la porta 10101.

Per aggiungere un'altra interfaccia per la connessione, cliccare su  e configurare i valori dei campi aggiunti.

Per vietare la connessione su un'interfaccia precedentemente impostata, cancellarla dalla lista cliccando su  di fronte alla riga con questa interfaccia.

4. Premere il pulsante **Salva**.



L'utilizzo della versione console dell'utility di diagnostica remota del Server Dr.Web è descritto in documento **Allegati**, [H7.3. Utility di diagnostica remota del Server Dr.Web](#).

10.5. Configurazione dell'agent SNMP Dr.Web

L'agent SNMP Dr.Web è progettato per l'integrazione di Dr.Web Enterprise Security Suite con i sistemi di gestione della rete tramite il protocollo SNMP. Tale integrazione consente di monitorare lo stato del funzionamento dei componenti Dr.Web, nonché di raccogliere statistiche di rilevamento e neutralizzazione delle minacce.

I sistemi di monitoraggio o qualsiasi gestore SNMP possono contattare il Server Dr.Web il quale fornisce le informazioni richieste tramite l'estensione dell'agent SNMP Dr.Web.



Per scoprire le informazioni che possono essere fornite dall'agent SNMP Dr.Web, è possibile utilizzare il MIB fornito insieme al Server Dr.Web. Il file `DRWEB-ESUITE-STAT-MIB.txt` è situato nella sottodirectory `etc` della directory di installazione del Server Dr.Web.




Per consentire al Server Dr.Web lo scambio di informazioni con i sistemi di gestione della rete attraverso il protocollo SNMP, è necessario attivare l'estensione dell'agent SNMP Dr.Web. Per fare questo, nella sezione **Configurazione del Server Dr.Web**, nella scheda [Moduli](#) spuntare il flag **Estensione dell'agent SNMP Dr.Web**.

Per configurare i parametri di connessione all'agent SNMP Dr.Web

1. Selezionare la voce **Amministrazione** nel menu principale del Pannello di controllo, nella finestra che si è aperta selezionare la voce del menu di gestione **Configurazione dell'agent SNMP Dr.Web**.
2. Nel campo **Community** impostare il nome di community SNMPv2c. Di default è **public**.
3. Configurare le impostazioni di interfaccia per la connessione dei sistemi di gestione della rete:
 - **Interfaccia** — indirizzo IP su cui il Server Dr.Web è in ascolto per le connessioni in entrata dai sistemi di gestione della rete.
 - **Porta** — porta su cui il Server Dr.Web è in ascolto per le connessioni in entrata dai sistemi di gestione della rete.

Per aggiungere un'altra interfaccia per la connessione, cliccare su  e configurare i valori dei campi aggiunti.

Per vietare la connessione su un'interfaccia precedentemente impostata, cancellarla dalla lista cliccando su  di fronte alla riga con questa interfaccia.

4. Spuntare il flag **Consenti l'accesso solo da reti locali** per consentire la connessione all'agent SNMP Dr.Web solo da reti locali.

Compilare per questo scopo la **Lista degli indirizzi locali** da cui è consentita la connessione dei sistemi di gestione della rete all'agent SNMP Dr.Web.

5. Premere il pulsante **Salva**.


10.6. Configurazione del calendario di Server Dr.Web


Per configurare il calendario di esecuzione dei task per il Server Dr.Web

1. Selezionare la voce **Amministrazione** nel 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 Dr.Web.
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.

 **Aggiungi task dal calendario predefinito** — per aggiungere al calendario corrente tutti i task dal calendario predefinito. Nella lista verranno salvati tutti i task correnti e vengono aggiunti tutti i task dal calendario predefinito. I task dal calendario predefinito vengono aggiunti in qualsiasi caso, anche se il calendario corrente già li contiene (in forma originale o modificata), tra le altre cose, se completamente coincide con il calendario predefinito.


 **Imposta calendario predefinito** — per rimuovere tutti i task dal calendario corrente e impostare il calendario dei task predefinito.



Calendario predefinito — lista dei task che vengono creati all'installazione iniziale del Server Dr.Web. Questo calendario non è modificabile.

 **Crea task** — per aggiungere un nuovo task. Questa 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 di formato specifico.

 **Importa impostazioni in questa sezione da file** — per importare il calendario da un file di formato specifico.










Non è possibile importare una lista dei task del Server Dr.Web nello Scheduler dei task delle postazioni e viceversa.

- 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 dei task selezionati:

Impostazione		Azione
 Tipo di avvio	Sincrono	Imposta il tipo di avvio sincrono di tutti i task contrassegnati sotto. Un task con una periodicità impostata verrà collocato nella coda generale dei task di Scheduler eseguiti in sequenza.
	Asincrono	Imposta il tipo di avvio asincrono di tutti i task contrassegnati sotto. Un task con una periodicità impostata verrà eseguito in modo parallelo ad altri task, fuori coda.
 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.



Impostazione	Azione
 L'impostazione simile viene definita nell'editor del task nella scheda Generali tramite il flag Permetti l'esecuzione .	
 Gravità	Rendi critico Eeguire il task in modo straordinario se l'esecuzione di questo task è stata persa nell'ora programmata.
	Rendi non critico Eeguire il task solo nell'ora programmata, indipendentemente dall'omissione o dall'esecuzione del task.
 L'impostazione simile viene definita nell'editor del task nella scheda Generali tramite il 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 (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.
 Esegui task	Eeguire immediatamente i task selezionati nella lista. In tale caso il task verrà avviato anche se esso è vietato per l'esecuzione secondo il calendario.

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 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 contrassegnati con il carattere * sono da impostare.

Per modificare i parametri di un task

1. Nella scheda **Generali** impostare i seguenti parametri:

- Nel campo **Nome** impostare il nome del task sotto cui esso verrà visualizzato nel calendario.
- Spuntare il flag **Permetti l'esecuzione** per attivare l'esecuzione del task. Se il flag non è selezionato, il task sarà presente nella lista ma non verrà eseguito.



L'impostazione simile viene definita nella finestra principale di Scheduler tramite l'elemento della barra degli strumenti **Stato**.

- Spuntare il flag **Task critico** per eseguire il task in modo straordinario se l'esecuzione di questo task è stata persa nell'ora programmata per qualsiasi motivo. Scheduler controlla ogni minuto l'elenco dei task e se scopre un task critico perso, lo avvia. Se al momento dell'avvio il task è stato perso diverse volte, verrà eseguito solo 1 volta.





L'impostazione simile viene definita nella finestra principale di Scheduler tramite l'elemento della barra degli strumenti **Gravità**.

- Se il flag **Avvia il task in modo asincrono** è deselezionato, il task verrà messo nella coda generale dei task di Scheduler eseguiti in sequenza. Spuntare il flag per eseguire questo task in modo parallelo al di fuori della coda.

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

Tipo di task	Parametri e descrizione
Aggiornamento del repository	<p>Il task è studiato per avviare un aggiornamento dei prodotti da SAM.</p> <p>È necessario impostare i seguenti parametri:</p> <ul style="list-style-type: none">• Nella lista Prodotto spuntare i flag di fronte ai prodotti del repository che verranno aggiornati secondo questo task.• Spuntare il flag Aggiorna chiavi di licenza per attivare la procedura per l'aggiornamento automatico delle chiavi di licenza durante l'aggiornamento del repository. Informazioni dettagliate sono riportate nella sezione Aggiornamento automatico delle licenze.
Arresto del Server Dr.Web	





Tipo di task	Parametri e descrizione
	<p>Il task è studiato per l'arresto del Server Dr.Web.</p> <p>Viene avviato senza parametri aggiuntivi.</p>
Avvio del programma	<p>Il task è studiato per avviare un programma.</p> <div data-bbox="448 573 1439 692"> I programmi avviati tramite questo task vengono eseguiti in background.</div> <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 da avviare.• Nel campo Argomenti — parametri della riga di comando per il programma da avviare.• Spuntare il flag Attendi che il programma venga completato per l'attesa di completamento del programma avviato da questo task. In questo caso il Server Dr.Web registra nel log l'avvio del programma, il codice restituito e l'ora di completamento del programma. Se il flag Attendi che il programma venga completato è deselezionato, il task è considerato completato immediatamente dopo l'avvio del programma, e il Server Dr.Web registra nel log solo l'avvio del programma.
Backup dei dati critici del server	<p>Il task è studiato per il backup dei seguenti dati critici del Server Dr.Web:</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 directory in cui verranno salvati i dati (il percorso vuoto significa la directory 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 G3.5.</p> <div data-bbox="448 1800 1439 1919"> La directory per il backup deve essere vuota. Altrimenti, il contenuto della directory verrà rimosso nel corso dell'esecuzione di un backup.</div>




Tipo di task	Parametri e descrizione
	<p data-bbox="264 280 638 309">Creazione del report statistico</p> <p data-bbox="445 344 1362 409">Il task è studiato per creare un report con le informazioni statistiche della rete antivirus.</p> <p data-bbox="445 445 1425 577">Per poter creare un report, è necessario che in uno dei profili di avvisi attivi sia attivato l'avviso Report statistico (v. p. Configurazione degli avvisi). Il report creato viene salvato sul computer su cui è installato il Server Dr.Web. L'ottenimento del report dipende dal tipo di avviso:</p> <ul data-bbox="445 602 1425 779" 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 tutti gli altri metodi di invio: viene inviato un avviso corrispondente che contiene il link del percorso del report. <p data-bbox="445 804 1291 835">Per creare il task, nel calendario si devono definire i seguenti parametri:</p> <ul data-bbox="445 860 1444 1496" style="list-style-type: none">• Lingua del report — lingua in cui i dati saranno presentati nel report.• Formato della data — formato in cui verranno presentate le informazioni statistiche che contengono date. Sono disponibili i seguenti formati:<ul data-bbox="485 987 956 1064" style="list-style-type: none">▫ europeo: DD-MM-YYYY HH:MM:SS▫ americano: MM/DD/YYYY HH:MM:SS• Formato del report — formato di file 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 informazioni su cui verranno incluse nel report. Per selezionare più gruppi, utilizzare i tasti CTRL o MAIUSCOLO.• Tabelle del report — lista delle tabelle statistiche, i dati da cui verranno inclusi nel report. Per selezionare più tabelle, utilizzare i tasti CTRL o MAIUSCOLO.• Tempo di conservazione del report — periodo di tempo di conservazione del report sul computer con il Server Dr.Web installato a partire dal momento della creazione del report.
	<p data-bbox="264 1556 697 1585">Copiatura di backup del repository</p> <p data-bbox="445 1621 1414 1653">Il task è studiato per il salvataggio periodico delle copie di backup del repository.</p> <p data-bbox="445 1688 973 1720">È necessario impostare i seguenti parametri:</p> <ul data-bbox="445 1744 1414 2004" style="list-style-type: none">• Percorso — percorso completo della directory 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 directory 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



Tipo di task	Parametri e descrizione
	<p>antivirus verrà salvato:</p> <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 dei componenti selezionati nella lista sotto. <ul style="list-style-type: none">• Contrassegnare con i flag i componenti le cui aree selezionate verranno salvate. <div style="background-color: #fff9c4; padding: 10px; border: 1px solid #ccc;"><p> La directory per il backup deve essere vuota. Altrimenti, il contenuto della directory verrà rimosso nel corso dell'esecuzione di un backup.</p></div>
Esecuzione dello script	<p>Il task è studiato per l'esecuzione dello script Lua riportato nel campo Script.</p> <div style="background-color: #fff9c4; padding: 10px; border: 1px solid #ccc;"><p> L'esecuzione simultanea del tipo di task Esecuzione dello script su diversi Server Dr.Web che utilizzano un unico database può portare a errori di esecuzione di questo task.</p><hr/><p>Con l'esecuzione degli script Lua l'amministratore ottiene l'accesso a tutto il file system all'interno della directory di Server Dr.Web e ad alcuni comandi di sistema sul computer con il Server Dr.Web installato.</p><p>Per vietare l'accesso al calendario, disattivare il permesso Modifica del calendario del Server Dr.Web per il relativo amministratore (v. p. Amministratori e gruppi di amministratori).</p></div>
Il Server Dr.Web adiacente non si collega da molto tempo	<p>Il task è studiato per visualizzare l'avviso su quello che i Server Dr.Web adiacenti non si collegano da molto tempo a questo Server Dr.Web.</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 periodi di tempo, dopo i quali il Server Dr.Web adiacente verrà considerato server che non si collega da molto tempo.</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>






Tipo di task	Parametri e descrizione
	<p>Le impostazioni del messaggio sono riportate nella sezione Invio di messaggi alle postazioni.</p>
	<p>La postazione non si collega da molto tempo</p> <p>Il task è studiato per visualizzare l'avviso su quello che le postazioni non si collegano da molto tempo a questo Server Dr.Web.</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>
	<p>Le licenze disponibili stanno per esaurirsi</p> <p>Il task è studiato per inviare l'avviso Il numero di postazioni nel gruppo si avvicina al limite di licenza, se stanno per esaurirsi le licenze di tutte le chiavi assegnate ai gruppi di postazioni selezionati.</p> <div data-bbox="485 999 1439 1115" style="background-color: #e6f2e6; padding: 10px;"><p> Le chiavi di licenza assegnate ai gruppi selezionati possono anche essere assegnate ad altri oggetti di licenza.</p></div> <p>È necessario impostare i seguenti parametri:</p> <ul style="list-style-type: none">• Numero di licenze disponibili — numero massimo di licenze rimanenti nelle chiavi di licenza assegnate ai gruppi selezionati, raggiunto il quale verrà inviato un avviso all'amministratore.• Percentuale di licenze disponibili — percentuale massima di licenze rimanenti nelle chiavi di licenza assegnate ai gruppi selezionati, raggiunta la quale verrà inviato un avviso all'amministratore.• Gruppi — lista dei gruppi in cui verrà controllato il numero di licenze rimanenti. Per selezionare più gruppi, utilizzare i tasti CTRL e MAIUSCOLO. <p>Pulizia degli eventi non inviati</p> <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 Dr.Web subordinato al Server Dr.Web principale. Se la trasmissione di un evento non è riuscita, esso viene registrato nell'elenco degli eventi non inviati. Il Server Dr.Web subordinato con una periodicità impostata esegue tentativi di trasmissione. All'esecuzione del task Pulizia degli eventi non inviati vengono rimossi tutti gli eventi, di cui la durata di conservazione ha raggiunto o superato il periodo impostato.</p>




Tipo di task	Parametri e descrizione
	<p>Pulizia dei messaggi obsoleti</p> <p>Il task è studiato per cancellare dal database i seguenti messaggi:</p> <ul style="list-style-type: none">• avvisi degli agent,• 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>Il task viene avviato senza parametri supplementari.</p>
	<p>Pulizia dei record vecchi</p> <p>Il task è studiato per rimuovere informazioni obsolete dal database. I tipi di record da rimuovere sono indicati nei parametri del task.</p> <p>È necessario indicare il numero di giorni dopo i quali i record nel database vengono riconosciuti come vecchi e vengono rimossi dal Server Dr.Web.</p> <p>Il periodo di rimozione di dati viene impostato separatamente per ciascun tipo di record.</p>
	<p>Pulizia del database</p> <p>Il task è studiato per la raccolta e cancellazione di record inutilizzati nel database di Server Dr.Web tramite l'esecuzione del comando <code>vacuum</code>.</p> <p>Viene avviato senza parametri aggiuntivi.</p>
	<p>Pulizia delle postazioni scadute</p> <p>È necessario indicare il periodo dopo cui le postazioni con accesso scaduto verranno rimosse. Il termine (giorno, mese, anno) fino a cui una postazione è ammessa al Server Dr.Web è ritrovabile nelle proprietà della postazione (nella scheda Generali nel campo Data di scadenza dell'accesso viene indicata una data specifica o Mai — per la rimozione delle restrizioni).</p>
	<p>Pulizia delle postazioni vecchie</p> <p>Il task è studiato per la rimozione di postazioni obsolete.</p>



Tipo di task	Parametri e descrizione
	<p>È necessario indicare un periodo di tempo (di default è 90 giorni) dopo cui le postazioni che non hanno visitato il Server Dr.Web vengono riconosciute come vecchie e vengono spostate nel gruppo della rete antivirus Deleted. La rimozione definitiva di tali postazioni dal database di Server Dr.Web verrà eseguita al momento dell'esecuzione del task Pulizia dei record vecchi (il termine di rimozione delle postazioni dal gruppo Deleted viene impostato nei parametri del task Pulizia dei record vecchi per il tipo Postazioni rimosse e viene conteggiato dal momento dello spostamento nel gruppo Deleted).</p> <div data-bbox="264 577 1439 831" style="background-color: #e6f2e6; padding: 10px;"><p> Le informazioni vecchie vengono rimosse dal database automaticamente al fine di risparmiare spazio su disco. Di default per i task Pulizia dei record vecchi e Pulizia delle postazioni vecchie il periodo è di 90 giorni. Se questo parametro viene diminuito, le statistiche sui componenti della rete antivirus accumulate diventano meno rappresentative. L'aumento di questo parametro può aumentare notevolmente il fabbisogno di risorse del Server Dr.Web.</p></div>
Registrazione nel file di log	<p>Il task è studiato per registrare la stringa impostata nel file di log di Server Dr.Web.</p> <p>Stringa — testo del messaggio che viene registrato nel file di log.</p>
Riavvio del Server Dr.Web	<p>Il task è studiato per il riavvio del Server Dr.Web.</p> <p>Viene avviato senza parametri aggiuntivi.</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">• Risveglia tutte le postazioni — prescrive di accendere tutte le postazioni connesse a questo Server Dr.Web.• Risveglia le postazioni in base ai parametri impostati — prescrive di accendere solo le postazioni che corrispondono ai parametri indicati di seguito:<ul style="list-style-type: none">▫ Indirizzi IP — lista degli indirizzi IP delle postazioni da accendere. Viene impostata nel formato: 10.3.0.127, 10.4.0.1-10.4.0.5, 10.5.0.1/30. Compilando 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 — lista degli indirizzi MAC delle postazioni da accendere. Gli ottetti dell'indirizzo MAC vengono separati dal carattere ':'. Compilando la lista

Tipo di task	Parametri e descrizione
	<p>degli indirizzi, usare virgola o nuova riga come separatore.</p> <ul style="list-style-type: none">▫ Gruppi — lista dei gruppi le cui postazioni sono da accendere. Per modificare la lista dei gruppi, premere il pulsante Modifica (o gli identificatori dei gruppi, se i gruppi sono già impostati) e selezionare i gruppi richiesti nella finestra che si è aperta. Per selezionare diversi gruppi, utilizzare i tasti CTRL e MAIUSCOLO. <div data-bbox="448 472 1437 857" style="background-color: #fff9c4; padding: 10px;"><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 della scheda di rete o nelle proprietà della scheda di rete (Pannello di controllo → Rete ed Internet → Connessioni di rete → Configura connessione → Configura → Avanzate per la proprietà Risveglio con il Magic Packet impostare Valore → Attivato).</p></div>
Scadenza della chiave di 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>
Sincronizzazione con Active Directory	<p>Il task è studiato per sincronizzare la struttura della rete: i container di Active Directory che contengono computer diventano gruppi della rete antivirus in cui vengono messe le postazioni.</p> <p>È necessario impostare i seguenti parametri:</p> <ul style="list-style-type: none">• Controller di Active Directory — controller di Active Directory, ad esempio, <code>dc.example.com</code>.• Nome utente — nome utente dell'utente di Active Directory.• Password — password dell'utente di Active Directory. <div data-bbox="448 1659 1437 1944" style="background-color: #e8f5e9; padding: 10px;"><p> Per Server Dr.Web SO Windows le impostazioni sono opzionali. Come dati di registrazione di default vengono utilizzati i dati dell'account utente sotto cui il processo Server Dr.Web è stato avviato (di regola è LocalSystem).</p><p>Per Server Dr.Web SO della famiglia UNIX le impostazioni devono essere obbligatoriamente configurate.</p></div>



Tipo di task	Parametri e descrizione
	<ul style="list-style-type: none">• Dalla lista a cascata Protezione della connessione selezionare il tipo di scambio di dati crittografati:<ul style="list-style-type: none">▫ STARTTLS — il passaggio alla connessione protetta viene effettuato attraverso il comando <code>STARTTLS</code>. Di default per la connessione è previsto l'utilizzo della porta 25.▫ SSL/TLS — aprì una connessione protetta crittografata separata. Di default per la connessione è previsto l'utilizzo della porta 465.▫ No — non usare la crittografia. Lo scambio di dati avverrà su una connessione non protetta. <div data-bbox="448 636 1441 786" style="background-color: #e6f2e6; padding: 10px;"> 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.</div> <p>Dopo l'esecuzione del task diventa disponibile l'assegnazione delle impostazioni di Office control speciali a utenti e gruppi da Active Directory (Office control -> Impostazioni di gruppo -> Impostazioni di accesso -> Impostazioni specifiche).</p>
Sostituzione della chiave di cifratura	<p>Il task è studiato per la sostituzione periodica dei seguenti strumenti che assicurano la cifratura tra i componenti:</p> <ul style="list-style-type: none">• chiave privata <code>drwcsd.pri</code> sul Server Dr.Web,• chiave pubblica <code>*.pub</code> sulle postazioni,• certificato <code>drwcsd-certificate.pem</code> sulle postazioni. <p>Siccome alcune postazioni potrebbero essere spente al momento della 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, durante il quale le postazioni di sicuro si conatteranno al Server Dr.Web.</p> <p>Creando un task, selezionare la fase corrispondente dalla lista a cascata:</p> <ul style="list-style-type: none">• Aggiunzione della nuova chiave — è la prima fase della procedura in cui vengono creati una nuova coppia di chiavi di cifratura inattiva e un certificato. Le postazioni ricevono la nuova chiave pubblica e il certificato quando si conettono al Server Dr.Web.• Rimozione della chiave vecchia e passaggio alla chiave nuova — è la seconda fase in cui le postazioni vengono informate sul passaggio alle nuove chiavi di cifratura e al nuovo certificato, dopo di che gli strumenti correnti vengono sostituiti con quelli nuovi: le chiavi pubbliche e il certificato sulle postazioni e la chiave privata sul Server Dr.Web. <p>Le postazioni che per qualche ragione non hanno ricevuto la nuova chiave pubblica e il nuovo certificato non potranno connettersi al Server Dr.Web. Per risolvere</p>




Tipo di task	Parametri e descrizione
	questo problema, è necessario mettere manualmente la nuova chiave pubblica e il certificato sulle postazioni (la procedura per la sostituzione della chiave sulla postazione è consultabile nel documento Allegati , sezione Connessione di Agent Dr.Web ad un altro Server Dr.Web).

3. Nella sezione **Tempo** impostare i seguenti parametri:

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

Modalità di avvio	Parametri e descrizione
Finale	Il task verrà eseguito all'arresto di Server Dr.Web. Viene avviato senza parametri aggiuntivi.
Iniziale	Il task verrà eseguito all'avvio di Server Dr.Web. Viene avviato senza parametri aggiuntivi.
Tra N minuti dopo il task iniziale	Dalla lista a cascata Task iniziale è necessario selezionare il task relativamente al quale viene impostato il tempo di esecuzione del task che viene creato. 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.

Il risultato del completamento dei task viene registrato nella tabella nella sezione **Amministrazione** → **Log di esecuzione dei task**.

10.7. Configurazione del web server



Ad ogni salvataggio di modifiche della sezione **Configurazione del web server** viene automaticamente salvato un backup della versione precedente del file di configurazione del web server. Vengono conservati gli ultimi 10 backup.

I backup si trovano nella stessa directory del file di configurazione e vengono denominati nel seguente formato:

```
webmin.conf_<ora_di_creazione>
```




È possibile utilizzare i backup creati, in particolare, per ripristinare il file di configurazione se l'interfaccia del Pannello di controllo non è disponibile.

Per configurare i parametri di configurazione del web server

1. Selezionare la voce **Amministrazione** nel menu principale del Pannello di controllo.
2. Nella finestra che si è aperta, selezionare la voce del menu di gestione **Configurazione del web server**. Si apre la finestra di configurazione di web server.




I valori dei campi contrassegnati con il carattere * sono da impostare.

3. Nella barra degli strumenti sono disponibili i seguenti pulsanti per gestire le impostazioni della sezione:
 -  **Riavvia Server Dr.Web** — per riavviare il Server Dr.Web per accettare le modifiche apportate a questa sezione. Il pulsante diventa attivo dopo che si sono apportate modifiche alle 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 è possibile ritornare dopo che si sono apportate modifiche. Il pulsante diventa attivo dopo che si sono apportate modifiche alle 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 di default** — per ripristinare tutti i parametri di questa sezione ai valori di default.

4. Per accettare le modifiche apportate alle impostazioni della sezione, premere il pulsante **Salva**, dopodiché sarà necessario riavviare il Server Dr.Web. Per fare questo, premere il pulsante  **Riavvia Server Dr.Web** nella barra degli strumenti di questa sezione.

10.7.1. Generali

Nella scheda **Generali** vengono configurate le seguenti impostazioni di funzionamento del web server:

- **Indirizzo di Server Dr.Web** — l'indirizzo IP o il nome DNS del Server Dr.Web.

Viene impostato nel formato:

<Indirizzo IP o nome DNS del Server Dr.Web> [: <porta >]

Se l'indirizzo del Server Dr.Web non è impostato, viene utilizzato il nome di computer restituito dal sistema operativo o l'indirizzo di rete del Server Dr.Web: il nome a dominio, se disponibile, altrimenti, l'indirizzo IP.



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

Se il numero di porta non è impostato, viene utilizzata la porta impostata nella richiesta (per esempio, in caso di connessione al Server Dr.Web dal Pannello di controllo o attraverso **Web API**). In particolare, in caso di richiesta dal Pannello di controllo, è la porta specificata nella barra degli indirizzi per la connessione del Pannello di controllo al Server Dr.Web.

- **Numero di richieste parallele dai client** — numero di richieste parallele elaborate dal web server. Questo parametro influisce sulle prestazioni del server. Non è consigliabile modificarne il valore senza necessità.
- **Numero di flussi input/output** — numero di flussi che elaborano i dati trasmessi via rete. Questo parametro influisce sulle prestazioni del Server Dr.Web. Non è consigliabile modificarne il valore senza necessità.
- **Time-out di una sessione HTTP/1 (s)** — time-out di una sessione attraverso il protocollo HTTP versione 1. In caso di connessioni permanenti, il Server Dr.Web interrompe la connessione se nel periodo indicato non arrivano richieste dal client. Il time-out esiste fino all'inizio dello scambio di dati in una sessione.
- **Velocità minima di invio attraverso HTTP/1 (B/s)** — velocità minima dell'invio dati attraverso il protocollo HTTP versione 1. 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 minima di ricezione attraverso HTTP/1 (B/s)** — velocità minima della ricezione dati attraverso il protocollo HTTP versione 1. 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.



- **Time-out di invio attraverso HTTP/1 (s)** — time-out di invio dati in una sessione aperta attraverso il protocollo HTTP versione 1. Se non è possibile inviare dati nel periodo indicato, la sessione viene chiusa.
- **Time-out di ricezione attraverso HTTP/1 (s)** — time-out di ricezione dati in una sessione aperta attraverso il protocollo HTTP versione 1. Se nel periodo indicato non arrivano richieste dal client, la sessione viene chiusa. Il time-out esiste dopo l'inizio di scambio di dati in una sessione.
- **Dimensione del buffer di invio (KB)** — dimensione dei buffer utilizzati per l'invio dei dati. Questo parametro influisce sulle prestazioni del Server Dr.Web. 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 Dr.Web. Non è consigliabile modificarne il valore senza necessità.
- **Lunghezza massima di una richiesta (KB)** — lunghezza massima ammissibile di una richiesta HTTP.
- **Attiva la protezione dagli attacchi flood** — spuntare il flag per adottare le misure di protezione dagli attacchi flood. Impostare i seguenti parametri di rilevamento di un attacco:
 - **Periodo (s)** — intervallo di tempo in secondi entro cui deve arrivare un determinato numero di richieste in modo che venga confermato un attacco flood proveniente dal client.
 - **Numero di richieste** — numero minimo di richieste che devono arrivare entro un determinato periodo di tempo in modo che venga confermato un attacco flood proveniente dal client.
 - **Durata del blocco (s)** — le connessioni con il client saranno proibite entro il numero di secondi impostato.

Nella sezione **Compressione** vengono impostati i parametri di compressione traffico per i dati trasmessi attraverso il canale di comunicazione con il server web via HTTP/HTTPS:

- **Dimensione massima di risposta da comprimere (KB)** — dimensione massima delle risposte HTTP che verranno compresse. Impostare il valore 0 per togliere la limitazione alla dimensione massima delle risposte HTTP da comprimere.
- **Dimensione minima di risposta da comprimere (B)** — dimensione minima delle risposte HTTP che verranno compresse. Impostare il valore 0 per togliere la limitazione alla dimensione minima delle risposte HTTP da comprimere.
- **Ordine di utilizzo dei tipi di compressione:**
 - **Determinato dal client** — l'ordine di utilizzo dei tipi di compressione viene determinato dal client in base ai tipi di compressione consentiti.
 - **Determinato dal server** — l'ordine di utilizzo dei tipi di compressione viene determinato dal server in base ai tipi di compressione consentiti. In questo caso impostare l'ordine dei tipi di compressione nella lista sotto. Per modificare l'ordine, trascinare tenendo alla matrice il blocco corrispondente.



È possibile attivare o disattivare i seguenti tipi di compressione, e inoltre modificarne l'ordine (per il caso in cui l'ordine viene determinato dal Server Dr.Web):

- **Utilizza la compressione GZIP** — spuntare il flag per utilizzare questo tipo di compressione. Nel campo **Livello di compressione GZIP** impostare un valore nell'intervallo 0–9. Il valore 0 significa disattiva compressione.
- **Utilizza la compressione Deflate** — spuntare il flag per utilizzare questo tipo di compressione. Nel campo **Livello di compressione Deflate** impostare un valore nell'intervallo 0–9. Il valore 0 significa disattiva compressione.
- **Utilizza la compressione Brotli** — spuntare il flag per utilizzare questo tipo di compressione. Nel campo **Livello di compressione Brotli** impostare un valore nell'intervallo 0–11. Il valore 0 significa disattiva 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 Dr.Web.
- **Attiva il supporto di HTTP/2** — spuntare il flag affinché vengano supportate le connessioni al web server attraverso il protocollo HTTP versione 2.
 - **Time-out di una sessione HTTP/2 (s)** — time-out di una sessione attraverso il protocollo HTTP versione 2. In caso di connessioni permanenti, il server interrompe la connessione se nel periodo indicato non arrivano richieste dal client.
- **Mantieni attiva la sessione TLS** — per utilizzare una connessione permanente per TLS. Le versioni obsolete dei browser possono gestire in modo non corretto le connessioni permanenti TLS. Disattivare questo parametro nel caso di problemi con l'utilizzo del protocollo TLS.
- **Certificato** — percorso del file di certificato TLS. Nella lista a cascata sono elencati i certificati disponibili dalla directory di Server Dr.Web.
- **Chiave privata SSL** — percorso del file della chiave privata TLS. Nella lista a cascata sono elencate le chiavi private TLS disponibili dalla directory di Server Dr.Web.
- **La chiave di crittografia per i ticket della sessione TLS** — percorso del file della chiave di crittografia per i ticket delle sessioni TLS. Si utilizza per riprendere una sessione TLS in base ai ticket delle sessioni (session tickets) che vengono criptati tramite la chiave impostata.
- **Lista delle cifre consentite** — stringa che definisce la lista delle cifre dal pacchetto OpenSSL, consentite per l'utilizzo nelle connessioni con i client. Se si lascia vuoto il campo, verrà utilizzato il valore `DEFAULT` che significa `ALL: !EXPORT: !LOW: !aNULL: !eNULL: !SSLv2`.

10.7.2. Avanzate

Nella scheda **Avanzate** vengono configurate le seguenti impostazioni di funzionamento del web server:

- Spuntare il flag **Mostra errori degli script** per visualizzare gli errori degli script nel browser. Questo parametro viene utilizzato dal servizio di supporto tecnico e dagli sviluppatori dell'azienda Doctor Web. Non è consigliabile modificarne il valore senza necessità.
- Spuntare il flag **Rintraccia l'esecuzione degli script** per attivare il rintracciamento dell'esecuzione degli script. Questo parametro viene utilizzato dal servizio di supporto



tecnico e dagli sviluppatori dell'azienda Doctor Web. Non è consigliabile modificarne il valore senza necessità.

- Spuntare il flag **Consenti l'interruzione degli script** per consentire l'interruzione degli script. Questo parametro viene utilizzato dal servizio di supporto tecnico e dagli sviluppatori dell'azienda Doctor Web. Non è consigliabile modificarne il valore senza necessità.
- Tramite i campi nell'area **Intestazioni HTTP personalizzate** è possibile aggiungere le proprie intestazioni HTTP di risposta del web server con i valori richiesti. Di default il web server utilizza tre intestazioni di sicurezza personalizzate predefinite: `X-XSS-Protection`, `X-Content-Type-Options` e `X-Frame-Options`. È possibile visualizzarne e modificarne i valori tramite il file di configurazione `webmin.conf` situato nella sottodirectory `etc` della directory di installazione di Server Dr.Web.

10.7.3. Trasporto



Nella scheda **Trasporto** vengono configurati gli indirizzi di rete "in ascolto" da cui il web server accetta le connessioni in entrata, per esempio per la connessione del Pannello di controllo o per l'esecuzione di richieste attraverso Web API.

Nella sezione **Indirizzi in ascolto** viene configurata una lista delle interfacce su cui il web server sarà in ascolto per accettare connessioni attraverso il protocollo HTTP:

- **Indirizzo** — indirizzo IP di un'interfaccia di rete da cui la ricezione delle connessioni è consentita.
- **Porta HTTP** — numero di porta di un'interfaccia di rete da cui la ricezione delle connessioni attraverso il protocollo HTTP è consentita.
- **Porta HTTPS** — numero di porta di un'interfaccia di rete da cui la ricezione delle connessioni attraverso il protocollo HTTPS è consentita.

Di default, per "l'ascolto" da parte del web server vengono impostati:

- **Indirizzo:** `0.0.0.0` — utilizza "tutte le interfacce di rete" per questa macchina su cui è installato il web server.
- **Porta HTTP:** `9080` — utilizza la porta standard `9080` per il protocollo HTTP.
- **Porta HTTPS:** `9081` — utilizza la porta standard `9081` per il protocollo HTTPS.

Per aggiungere una nuova riga di indirizzo, premere il pulsante . Per eliminare la riga di un determinato indirizzo, premere il pulsante  accanto all'indirizzo da eliminare.

10.7.4. Sicurezza

Nella scheda **Sicurezza** vengono impostate le limitazioni riguardanti gli indirizzi di rete da cui il web server accetta le richieste HTTP e HTTPS.



Generali

- Spuntare il flag **Reindirizza via una connessione sicura** affinché tutte le connessioni HTTP vengano reindirizzate automaticamente via HTTPS.
- Spuntare il flag **Restituisci un'intestazione dettagliata** affinché il web server restituisca i dettagli dell'ambiente nell'intestazione "Server".
- Spuntare il flag **Converti gli URI in minuscolo** affinché tutti gli URI nelle richieste al web server vengano convertiti in minuscolo. Va convertito soltanto il frammento della parte gerarchica di un URI che contiene un percorso.
- Spuntare il flag **Attiva il controllo degli accessi per le applicazioni client** per vietare l'accesso all'interfaccia del Pannello di controllo per i programmi-bot e altre applicazioni client dalla lista sottostante.

Definire la lista delle applicazioni client vietate:

- Nel campo **Nome dell'applicazione client** impostare il nome dell'applicazione client per cui verrà negato l'accesso all'interfaccia del Pannello di controllo. È sensibile alle maiuscole. Se non è impostato, viene utilizzato l'URI dell'applicazione.
- Nel campo **Espressione regolare definente** impostare l'espressione regolare che definisce l'applicazione per cui verrà negato l'accesso all'interfaccia del Pannello di controllo.

Limitazione di accesso

Per impostare le limitazioni di accesso per un 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 la lista degli indirizzi

1. Inserire un 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 indica reti con una maschera: 255.255.255.0
Contiene 254 indirizzi.
Gli indirizzi di host in queste reti sono di tipo: 195.136.12.*
2. Il prefisso 8 indica reti con una maschera 255.0.0.0
Contiene fino a 16387064 indirizzi (256*256*256).
Gli indirizzi di host in queste reti sono di tipo: 125.*.*.*

10.7.5. Moduli



Si consiglia di non modificare le impostazioni di questa sezione senza istruzioni del servizio di supporto tecnico.

Nella sezione **Moduli** vengono configurati gli script Lua che vengono caricati man mano che vengono eseguiti altri script dell'interfaccia web.

- La lista a cascata **Directory dello script nei percorsi di ricerca** determina in quale posizione della lista dalla sezione **Percorsi** va aggiunta la directory corrente (directory in cui si trova lo script attualmente in esecuzione):
 - **primo** — all'inizio della lista,
 - **ultimo** — alla fine della lista,
 - **non utilizzare** — non aggiungere affatto.
- La sezione **Maschere** imposta l'insieme di maschere in base a cui vengono cercati i moduli Lua sui percorsi indicati nella sezione **Percorso**.
- La sezione **Percorsi** imposta i percorsi in base a cui vengono cercati i moduli Lua dalla sezione **Maschere**. I percorsi devono essere impostati relativamente alla directory radice del web server.

Per esempio:

Lo script situato nel percorso `var-root/webmin/esuite/include/head.ds` non verrà trovato senza indicazione di impostazioni aggiuntive nella sezione **Moduli**.

I moduli dalle directory `ds-modules` o `webmin/vfs` verranno trovati senza impostazioni nella sezione **Moduli** in quanto questi sono moduli globali, anziché moduli dell'interfaccia web.



10.7.6. Gestori



Si consiglia di non modificare senza istruzioni del servizio di supporto tecnico le impostazioni di questa sezione, ad eccezione delle sottosezioni **Accesso** e **Autenticazione**.

Nella sezione **Gestori** viene configurato in che modo e in quale ambiente verrà elaborata una richiesta ricevuta da un web client.

Generali

Le impostazioni disponibili variano in base al tipo di gestore.

Nel caso di web socket il gestore necessario viene selezionato in base all'attributo **Protocollo**.

Nel caso di altri tipi di gestori il gestore necessario viene selezionato in base all'attributo **Prefisso**.

I tipi di gestori utilizzati vengono selezionati nella lista a cascata **Tipo**:

• Gestori

Viene eseguito lo script indicato cui viene passato come parametro il percorso dall'URL. Se il percorso è assente, gli viene passato il percorso del campo **Directory**.

- **Prefisso** — prefisso del percorso nell'URL della richiesta HTTP.
- **Directory** — directory nella radice del web server relativamente a cui vengono calcolati i percorsi dei file forniti.
- **Script** — script gestore.

• Gestori misti

A seconda del tipo di file a cui viene effettuata la richiesta, si comporta come tipo **File statici** o come tipo **Script**.

- **Prefisso** — prefisso del percorso nell'URL della richiesta HTTP.
- Lista dei file indice. Determina quali file in quale ordine verranno caricati se il web client richiederà l'indice directory.
- **Script** — lista delle estensioni di file da ritenere script Lua.

• Script

Qualsiasi file a cui viene effettuata una richiesta viene eseguito come uno script Lua.

- **Prefisso** — prefisso del percorso nell'URL della richiesta HTTP.
- **Directory** — directory nella radice del web server relativamente a cui vengono calcolati i percorsi dei file forniti.



- **File statici**

Il contenuto dei file viene fornito così com'è.

- **Prefisso** — prefisso del percorso nell'URL della richiesta HTTP.
- **Directory** — directory nella radice del web server relativamente a cui vengono calcolati i percorsi dei file forniti.
- Lista dei file indice. Determina quali file in quale ordine verranno caricati se il web client richiederà l'indice directory.

- **File system virtuale**

È simile al tipo **File statici**, ma i file vengono caricati dall'archivio formato interno `dar` indicato nel campo **Directory**.

- **Prefisso** — prefisso del percorso nell'URL della richiesta HTTP.
- **Directory** — directory nella radice del web server relativamente a cui vengono calcolati i percorsi dei file forniti.

- **Websocket predefiniti**

Websocket-applicazione realizzata tramite una libreria condivisa fornita con il server (`dll` o `elf shared object`). Il nome file della libreria corrisponde al protocollo del web socket, i file sono locati in `lib-root/websockets`.

- **Script di autenticazione** — nome file dello script Lua che autentica l'utente.
- **Protocollo** — valore del campo `WebSocket-Protocol` trasmesso nella richiesta HTTP di connessione al web socket.

- **Websocket personalizzati**

Websocket-applicazione realizzata tramite uno script Lua. Il nome file dello script corrisponde al protocollo del web socket, i file sono locati in `home-root/websockets`.

- **Script di autenticazione** — nome file dello script Lua che autentica l'utente.
- **Protocollo** — valore del campo `WebSocket-Protocol` trasmesso nella richiesta HTTP di connessione al web socket.

Accesso

Le liste di controllo accessi (ACL) impostano limitazioni agli indirizzi di rete da cui i client potranno accedere al web server.

Le impostazioni sono simili alle [impostazioni di sicurezza di Server Dr.Web](#).

Se le impostazioni non sono definite, tutti gli indirizzi sono ritenuti consentiti.



Autenticazione

È disponibile per tutti i tipi di gestori tranne i web socket.



Le impostazioni della sezione definiscono la lista di risorse per le richieste a cui è necessario richiedere al web client l'autenticazione http basic.

- **Portata (realm)** — valore che il web server fornirà al client nel parametro `WWW-Authenticate: Basic realm="ADMIN"`. In sostanza, è una breve descrizione di quello chi deve autenticarsi. Non ha nulla a che fare con il nome utente.

Per impostare le limitazioni di accesso per un tipo di connessione

1. Al fine di consentire l'accesso libero per le connessioni client tramite HTTP o HTTPS a determinati percorsi, includere questi percorsi nelle rispettive liste **HTTP: accesso libero** o **HTTPS: accesso libero**.
2. Al fine di richiedere l'autenticazione alle connessioni client tramite HTTP o HTTPS a determinati percorsi, includere questi percorsi nelle liste **HTTP: richiesta di autenticazione** o **HTTPS: richiesta di autenticazione**.
3. Per l'accesso ai percorsi non inclusi in nessuna delle liste, l'autenticazione è richiesta o meno a seconda che sia impostato il flag **Priorità della richiesta di autenticazione**: se il flag è impostato, per la connessione ai percorsi non inclusi in nessuna delle liste (o inclusi in entrambe) è richiesta l'autenticazione. In caso contrario, su tali percorsi è consentito l'accesso libero.

Per modificare la lista degli indirizzi

1. Inserire nel campo un'espressione regolare che definisce il percorso relativamente alla directory specificata nel campo **Directory**.
2. Per aggiungere un nuovo campo di indirizzo, premere il pulsante  della sezione corrispondente.
3. Per eliminare un campo, premere il pulsante .

10.8. Procedure personalizzate



Con l'esecuzione degli script Lua l'amministratore ottiene l'accesso a tutto il file system all'interno della directory di Server Dr.Web e ad alcuni comandi di sistema sul computer con il Server Dr.Web installato.

Per vietare l'accesso alle procedure personalizzate, disattivare il permesso **Modifica della configurazione del Server Dr.Web e di quella del repository** per il relativo amministratore (v. p. [Amministratori e gruppi di amministratori](#)).



Per semplificare e automatizzare l'esecuzione di determinati task di Server Dr.Web, è possibile utilizzare procedure personalizzate implementate sotto forma di script Lua.



Le procedure personalizzate si trovano nella seguente sottodirectory della directory di installazione di Server Dr.Web:

- in caso di SO Windows: `var\extensions`
- in caso di SO FreeBSD: `/var/drwcs/extensions`
- in caso di SO Linux: `/var/opt/drwcs/extensions`

Dopo l'installazione di Server Dr.Web, in questa sottodirectory si trovano le procedure personalizzate predefinite.

Si consiglia di modificare procedure personalizzate attraverso il Pannello di controllo.



Prima dell'aggiornamento di Server Dr.Web, è necessario salvare le procedure personalizzate e gli script. Notare che in caso di passaggio a una versione più nuova di Server Dr.Web, le procedure personalizzate e gli script che funzionavano nella versione precedente potrebbero non funzionare. Se viene riscontrato un problema, contattare il [supporto tecnico](#).

Per configurare l'esecuzione delle procedure personalizzate

1. Selezionare la voce **Amministrazione** nel menu principale del Pannello di controllo.
2. Nella finestra che si è aperta, selezionare la voce del menu di gestione **Procedure personalizzate**. Si apre la finestra di configurazione delle procedure personalizzate.



Una descrizione dettagliata delle procedure personalizzate e dei loro parametri è riportata in documento **Allegati**, [Allegato M. 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 nell'albero delle procedure sono presenti i seguenti gruppi predefiniti:

- **Examples of the hooks** — contiene i modelli di tutte le procedure personalizzate disponibili. Sulla base di questi modelli è possibile creare le proprie procedure personalizzate. Non è fornita la possibilità di modifica ed esecuzione delle procedure modello.
- **IBM Syslog** — contiene i modelli di procedure personalizzate utilizzate per l'integrazione con il sistema IBM Tivoli. Gli eventi che corrispondono alle procedure attivate vengono registrati nel formato *Syslog*.

Tutti gli eventi vengono scritti in un file nel seguente percorso:







- in caso di SO Windows:
var\export\tivoli\syslog\drwcs_syslog.log
- in caso di SO FreeBSD:
/var/drwcs/export/tivoli/syslog/drwcs_syslog.log
- in caso di SO Linux:
/var/opt/drwcs/export/tivoli/syslog/drwcs_syslog.log
- **IBM W7Log** — contiene i modelli di procedure personalizzate utilizzate per l'integrazione con il sistema IBM Tivoli. Gli eventi che corrispondono alle procedure attivate vengono registrati nel formato *IBM W7Log XML*.

Per ciascun evento viene creato un file separato nel seguente percorso:

- in caso di SO Windows:
var\export\tivoli\w7log*<nome_evento>*_*<unix_timestamp>*
- in caso di SO FreeBSD:
/var/drwcs/export/tivoli/w7log/*<nome_evento>*_*<unix_timestamp>*
- in caso di SO Linux:
/var/opt/drwcs/export/tivoli/w7log/*<nome_evento>*_*<unix_timestamp>*



L'icona di un elemento dell'albero dipende dal tipo o dallo stato di questo elemento (v. [tabella 10-7](#)).

Tabella 10-7. Le icone degli elementi dell'albero delle procedure

Icona	Descrizione
Gruppi di procedure	
	Gruppo di procedure per cui è consentita l'esecuzione delle procedure.
	Gruppo di procedure per cui è proibita l'esecuzione delle procedure.
Procedure	
	Procedura per cui è consentita l'esecuzione.
	Procedura per cui è proibita l'esecuzione.

Gestione dell'albero delle procedure

Per gestire oggetti nell'albero delle procedure, si usano i seguenti elementi della barra degli strumenti:

- + — lista a cascata per aggiungere un elemento all'albero delle procedure:
 -  **Aggiungi procedura personalizzata** — per aggiungere una nuova procedura personalizzata.
 -  **Aggiungi gruppo di procedure personalizzate** — per creare un nuovo gruppo custom in cui verranno messe le procedure.





✗ Rimuovi gli oggetti selezionati — per rimuovere una procedura personalizzata o un gruppo selezionato nell'albero delle procedure.

🟢 Consenti l'esecuzione della procedura personalizzata — l'azione simile si esegue tramite l'editor delle procedure selezionando il flag **Consenti l'esecuzione della procedura personalizzata**. Vedi inoltre [Attivazione delle procedure](#).

🔴 Proibisci l'esecuzione della procedura personalizzata — l'azione simile si esegue tramite l'editor delle procedure togliendo la spunta alla voce **Consenti l'esecuzione della procedura personalizzata**. Vedi inoltre [Attivazione delle procedure](#).

Gestione dei gruppi di procedure

Per creare un nuovo gruppo

1. Nella barra degli strumenti selezionare  →  **Aggiungi gruppo di procedure personalizzate**.
2. Nella finestra che si è aperta, impostare i seguenti parametri:
 - Spuntare il flag **Consenti l'esecuzione della procedura personalizzata** per attivare le procedure che faranno parte di questo gruppo. V. inoltre [Attivazione delle procedure](#).
 - Nel campo **Nome del gruppo** specificare un nome per il gruppo che viene creato.
3. Premere il pulsante **Salva**.

Per modificare l'ordine di utilizzo dei gruppi



1. Nell'albero delle procedure trascinare un gruppo di procedure e collocarlo nell'ordine richiesto rispetto agli altri gruppi.
2. L'ordine di utilizzo delle procedure cambierà automaticamente quando viene modificato l'ordine dei gruppi: per prime verranno eseguite le procedure dai gruppi che si trovano più in alto nell'albero delle procedure.

Per spostare una procedura in un altro gruppo

1. Nell'albero delle procedure selezionare la procedura che si desidera spostare.
2. Nella barra delle proprietà aperta dalla lista a cascata **Gruppo padre** selezionare il gruppo in cui si vuole spostare la procedura.
3. Premere il pulsante **Salva**.

Gestione delle procedure

Per aggiungere una nuova procedura

1. Nella barra degli strumenti selezionare  →  **Aggiungi procedura personalizzata**.
2. Nella finestra che si è aperta, impostare i seguenti parametri:



- Spuntare il flag **Consenti l'esecuzione della procedura personalizzata** per attivare la procedura che viene creata. V. inoltre [Attivazione delle procedure](#).
 - Dalla lista a cascata **Gruppo padre** selezionare il gruppo in cui sarà situata la procedura che viene creata. In seguito sarà possibile spostare la procedura in un altro gruppo — vedi [sopra](#).
 - Dalla lista a cascata **Procedura personalizzata** selezionare il tipo di procedura. Il tipo di procedura definisce l'azione per cui verrà invocata questa procedura.
 - Nel campo **Testo della procedura personalizzata** immettere lo script lua che verrà eseguito quando verrà invocata questa procedura.
Nella sottosezione **Informazioni sulla procedura** viene riportato l'evento per cui verrà invocata questa procedura; viene indicato se per questa procedura è disponibile il database di Server Dr.Web; nonché vengono riportate liste dei parametri di input e dei valori restituiti per questo tipo di procedura.
3. Premere il pulsante **Salva**.


Per modificare una procedura

1. Nell'albero delle procedure selezionare la procedura che si desidera modificare.
 2. Nella parte destra della finestra si apre automaticamente la barra delle proprietà di questa procedura. Possono essere modificati tutti i parametri che venivano impostati durante la creazione della procedura, ad eccezione del parametro **Procedura personalizzata**. Questo parametro definisce l'evento per cui viene invocata questa procedura e non può essere modificato dopo la creazione della procedura.
3. Premere il pulsante **Salva**.

Attivazione delle procedure

L'attivazione delle procedure e dei gruppi di procedure definisce se le procedure verranno eseguite o meno al verificarsi degli eventi corrispondenti.

Per attivare una procedura o un gruppo di procedure

1. Nell'albero delle procedure selezionare la procedura o il gruppo che si desidera attivare.
2. Eseguire una delle seguenti azioni:
 - Nella barra degli strumenti premere il pulsante  **Consenti l'esecuzione della procedura personalizzata**.
 - Nella parte destra della finestra nella barra delle proprietà dell'oggetto selezionato spuntare il flag **Consenti l'esecuzione della procedura personalizzata** se la spunta è tolta. Premere il pulsante **Salva**.



Caratteristiche dell'attivazione delle procedure:

Affinché una procedura venga eseguita al verificarsi dell'evento corrispondente, è necessario quanto segue:

- a) la procedura deve essere attivata;
- b) deve essere attivato il gruppo in cui rientra questa procedura.



Se un gruppo di procedure è disattivato, le procedure che ne fanno parte non verranno eseguite anche se loro stesse sono attivate.

Quando viene attivato un gruppo, verranno eseguite soltanto quelle procedure contenute che sono attivate.

10.9. Modelli di messaggio

Nella sezione **Modelli di messaggio** è riportata una lista di modelli di messaggio di testo arbitrari che vengono inviati dall'amministratore sulle postazioni della rete antivirus (v. [Invio di messaggi alle postazioni](#)).

Messaggi possono essere inclusi nella lista dei modelli in uno dei seguenti modi:

1. Un modello può essere creato sulla base di un messaggio che è già stato inviato dall'amministratore. Tale modello viene creato nella sezione [Log dei messaggi](#).
2. Può essere creato un modello completamente nuovo. Per farlo, premere il pulsante **+ Crea modello** nella barra degli strumenti nella sezione **Modelli di messaggio**. Le impostazioni del messaggio sono simili alle impostazioni dalla sezione [Invio di messaggi alle postazioni](#).

Per gestire modelli di messaggio, utilizzare le seguenti opzioni nella barra degli strumenti:

Rimuovi — per rimuovere i modelli di messaggio selezionati.

Crea modello — per creare un nuovo modello di messaggio (vedi [sopra](#)).

Modifica — per modificare le impostazioni di un modello già esistente. L'opzione è disponibile solo se viene selezionato un modello nella lista.

Invia messaggio su postazioni — per inviare su postazioni uno o più messaggi in base ai modelli selezionati nella lista (vedi sotto).


Per inviare un messaggio

1. Spuntare il flag di fronte al modello di messaggio che si vuole inviare.
2. Premere il pulsante **Invia messaggio su postazioni**.
3. Si apre la finestra **Invio del messaggio**. Configurare le seguenti impostazioni:



- a) Nell'albero **Rete antivirus** selezionare destinatari del messaggio dall'elenco proposto: questi possono essere sia singole postazioni che gruppi di postazioni.
 - b) Le impostazioni del messaggio sono simili alle impostazioni dalla sezione [Invio di messaggi alle postazioni](#).
4. Premere il pulsante **Invia**.

Per inviare diversi messaggi


1. Spuntare i flag di fronte ai modelli di messaggio che si vuole inviare.
2. Premere il pulsante  **Invia messaggio su postazioni**.
3. Si apre la finestra **Invio di più messaggi**. Nella sezione **Elenco dei messaggi** sono riportati tutti i messaggi che sono stati selezionati per l'invio. I nomi dei messaggi corrispondono ai nomi dei relativi modelli.
4. Premere il pulsante **Invia tutto** per inviare tutti i messaggi dalla lista.
5. Per modificare uno dei messaggi, selezionarlo nella sezione **Elenco dei messaggi**. Nella sezione **Impostazioni del messaggio** configurare i seguenti parametri:
 - a) Nell'albero **Rete antivirus** selezionare destinatari del messaggio dall'elenco proposto: questi possono essere sia singole postazioni che gruppi di postazioni.
 - b) Le impostazioni del messaggio sono simili alle impostazioni dalla sezione [Invio di messaggi alle postazioni](#).
 - c) Per eliminare il messaggio selezionato dalla lista dei messaggi da inviare, premere il pulsante **Rimuovi**.

10.10. 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.

10.10.1. Configurazione degli avvisi

Per configurare gli avvisi sugli eventi della rete antivirus

1. Selezionare la voce **Amministrazione** nel menu principale del Pannello di controllo, nella finestra che si è aperta selezionare la voce del menu di gestione **Configurazione degli avvisi**.
2. Gli avvisi vengono configurati separatamente per ciascun amministratore del Pannello di controllo. Il nome dell'amministratore per cui sono configurate le impostazioni visualizzate è riportato nel campo **Amministratore che riceve gli avvisi**. Per configurare gli avvisi per un altro amministratore, premere il pulsante  e selezionare l'amministratore nella finestra che si è aperta.



3. Alla configurazione iniziale è aggiunto un blocco (profilo) di avvisi predefinito per l'amministratore principale **admin**. Se la lista degli avvisi amministratore è vuota, premere **Aggiungi avviso** nella sezione **Lista degli avvisi**.

4. Per abilitare l'invio di avvisi, impostare l'interruttore a sinistra dell'intestazione di un blocco sulla posizione corrispondente:



— l'invio di avvisi per questo blocco è abilitato.



— gli avvisi di questo blocco non verranno inviati.

5. È possibile creare più blocchi (profili) di avvisi, per esempio, per diversi 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. I blocchi di avvisi diversi vengono configurati in modo indipendente.

6. Nel campo **Intestazione** impostare il nome del blocco di avvisi aggiunto. Questo nome verrà utilizzato, per esempio, nella configurazione del task **Creazione del report statistico** nel calendario del Server Dr.Web. In seguito, per la modifica dell'intestazione fare clic sull'intestazione con il tasto sinistro del mouse e inserire il nome richiesto. Se c'è più di un blocco di avvisi, quando si fa clic sul testo dell'intestazione, verrà offerta una lista a cascata con le intestazioni dei blocchi di avvisi esistenti.

7. Per configurare l'invio di avvisi, selezionare il modo di invio richiesto dalla lista a cascata **Metodo di invio degli avvisi**:

- [Agent Dr.Web](#) — per inviare gli avvisi attraverso il protocollo di Agent Dr.Web.
- [Console web](#) — per inviare gli avvisi da visualizzare nella [console web](#).
- [E-mail](#) — per inviare gli avvisi via posta elettronica.
- [Notifiche push](#) — per inviare notifiche push sul Pannello di controllo della sicurezza mobile Dr.Web. Questa voce diventa disponibile nella lista a cascata **Metodo di invio degli avvisi** solo dopo che un Pannello di controllo della sicurezza mobile Dr.Web viene connesso a questo Server Dr.Web.
- [SNMP](#) — per inviare gli avvisi attraverso il protocollo SNMP.
- [Syslog](#) — per inviare gli avvisi attraverso il protocollo Syslog.

Le impostazioni di ciascuno dei tipi di invio degli avvisi sono descritte di seguito in questa sezione.

8. 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.

9. Negli avvisi vengono utilizzati i testi da modelli predefiniti.





Gli avvisi predefiniti e i relativi parametri sono descritti in documento **Allegati**, [C2. Parametri dei modelli di avviso](#).

Per modificare il modello di un avviso specifico:


- a) Premere **Passa alla modalità di modifica degli avvisi** nell'intestazione della sezione.
- b) Premere sull'avviso che si vuole modificare. Si aprirà il modello di avviso.



- c) Se necessario, modificare il testo del messaggio da inviare. Nel testo di un avviso è possibile utilizzare le variabili di modello (tra parentesi graffe). Le variabili possono essere aggiunte tramite le liste a cascata nella parte superiore della finestra. Durante la preparazione del messaggio, il sistema di avviso sostituisce le variabili di modello con un testo specifico che dipende dalle sue impostazioni correnti. La lista delle variabili disponibili è riportata in documento **Allegati**, [C2. Parametri dei modelli di avviso](#).
- Per ripristinare i valori di default del modello di avviso, premere  **Modello predefinito**.
- d) Dopo aver apportato tutte le modifiche necessarie, premere  **Esci dalla modalità di modifica degli avvisi** nell'intestazione della sezione.




In caso del metodo di invio **SNMP** i modelli di avviso vengono impostati sul lato destinatario (*postazione di comando* secondo RFC 1067), pertanto, la modifica di essi tramite il Pannello di controllo non è disponibile.

10. Per gli avvisi della sottosezione **Postazioni** è possibile impostare i gruppi di postazioni sugli eventi sulle quali verranno inviati gli avvisi:
- Premere  a sinistra dell'avviso.
 - Nell'albero **Gruppi di postazioni monitorate** selezionare i gruppi di postazioni per cui verranno monitorati gli eventi e verrà inviato l'avviso corrispondente. Per selezionare più gruppi, utilizzare i tasti CTRL o MAIUSCOLO.
 - Dopo aver selezionato tutti i gruppi richiesti, premere **Salva**.
11. Premere il pulsante **Salva** per applicare tutte le modifiche apportate.

Avvisi attraverso il protocollo di Agent Dr.Web

Per gli avvisi attraverso il protocollo di Agent Dr.Web impostare i seguenti parametri:

- Nella sezione **Invio ripetuto dal Server Dr.Web** configurare le impostazioni di invii ripetuti dell'avviso che verranno effettuati dal Server Dr.Web in caso di errore:
 - **Numero** — numero di tentativi ripetuti effettuati dal Server Dr.Web se l'invio del messaggio non è riuscito. Di default è 10.
 - **Time-out** — periodo in secondi dopo cui il Server Dr.Web effettua un nuovo tentativo di invio del messaggio. Di default è di 300 secondi.
- Postazioni** — lista delle postazioni e dei gruppi di postazioni su cui verranno inviati gli avvisi. Per modificare la lista, premere **Modifica** , selezionare le postazioni e i gruppi di postazioni richiesti nell'albero e premere **Applica**.
- Invia un messaggio di test** — per inviare un avviso di test in conformità alle impostazioni del sistema di avviso.



Avvisi che vengono visualizzati nella console web

Per gli avvisi che vengono visualizzati nella Web console, impostare i seguenti parametri:

- Nella sezione **Invio ripetuto dal Server Dr.Web** configurare le impostazioni di invii ripetuti dell'avviso che verranno effettuati dal Server Dr.Web in caso di errore:
 - **Numero** — numero di tentativi ripetuti effettuati dal Server Dr.Web se l'invio del messaggio non è riuscito. Di default è 10.
 - **Time-out** — periodo in secondi dopo cui il Server Dr.Web effettua un nuovo tentativo di invio del messaggio. Di default è di 300 secondi.
- **Tempo di conservazione di un avviso** — tempo per cui 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 Dr.Web.

Per gli avvisi ricevuti tramite questo metodo di invio è possibile impostare un tempo di conservazione illimitato nella sezione [Avvisi nella console web](#).
- **Invia un messaggio di test** — per inviare un avviso di test in conformità alle impostazioni del sistema di avviso.

Avvisi via email

Per gli avvisi via email, impostare i seguenti parametri:

- Nella sezione **Invio ripetuto dal Server Dr.Web** configurare le impostazioni di invii ripetuti dell'avviso che verranno effettuati dal Server Dr.Web in caso di errore:
 - **Numero** — numero di tentativi ripetuti effettuati dal Server Dr.Web se l'invio del messaggio non è riuscito. Di default è 10.
 - **Time-out** — periodo in secondi dopo cui il Server Dr.Web effettua un nuovo tentativo di invio del messaggio. Di default è di 300 secondi.
- **Indirizzi e-mail dei destinatari** — indirizzi di posta elettronica dei destinatari dei messaggi. In ciascun campo è possibile inserire solo un indirizzo di posta elettronica di destinatario. Per aggiungere un altro campo di destinatario, premere il pulsante **+**. Per rimuovere un campo, premere il pulsante **-**.



I parametri di invio di email vengono configurati nel menu **Amministrazione**, nella sezione **Configurazione del Server Dr.Web**, nella scheda **Rete**, nella scheda interna [E-mail](#).




- **Invia un messaggio di test** — per inviare un avviso di test in conformità alle impostazioni del sistema di avviso.

È inoltre possibile aggiungere intestazioni personalizzate arbitrarie nella sezione aggiuntiva **Intestazioni** nell'editor del modello (v. [p. 9a sopra](#)) per ciascun avviso via email. In particolare, le intestazioni di messaggi di posta possono essere utilizzate per configurare i filtri di posta. Le



intestazioni devono essere formate in conformità agli standard RFC 822, RFC 2822 e non devono intersecarsi con i campi definiti negli standard per messaggi di posta elettronica. Così, lo standard RFC 822 garantisce l'assenza nella specifica di intestazioni che inizino con X-, perciò è consigliabile impostare nomi in formato X-*<nome-intestazione>*. Per esempio: X-Template-Language: Italian.

Per aggiungere o modificare un'intestazione per un avviso specifico


1. Premere  **Passa alla modalità di modifica degli avvisi** nell'intestazione della sezione.
2. Dalla lista a cascata **Metodo di invio degli avvisi** selezionare **Email**.
3. Premere sull'avviso che si vuole modificare. Si aprirà il modello di avviso.
4. Nel campo **Intestazioni** inserire una o più intestazioni in formato X-*<nome>*: *<valore>*. Come valore si possono utilizzare le variabili di modello (tra parentesi graffe), disponibili nelle liste a cascata nella parte superiore della finestra. Le intestazioni devono essere separate da una riga vuota.
5. Premere il pulsante **Salva**.
6. Premere  per chiudere la finestra dell'editor dei modelli.
7. Dopo aver apportato tutte le modifiche necessarie, premere  **Esci dalla modalità di modifica degli avvisi** nell'intestazione della sezione.
8. Premere il pulsante **Salva** per applicare tutte le modifiche apportate.

È inoltre possibile impostare intestazioni comuni per gli avvisi via email.



Le intestazioni comuni vengono aggiunte a tutti i modelli di avviso via email. Una volta aggiunte, le intestazioni comuni non differiscono dalle altre intestazioni di avviso personalizzate, pertanto, in seguito le intestazioni comuni non potranno essere modificate in massa separatamente dalle altre. È possibile modificare o rimuovere le intestazioni comuni solo come le altre intestazioni personalizzate modificando il modello per ciascun avviso individuale.

Per aggiungere un'intestazione comune

1. In qualsiasi blocco di avvisi via email premere il pulsante **Modifica intestazioni comuni**.
2. Nella finestra che si è aperta **Intestazioni comuni per tutti i modelli** inserire una o più intestazioni in formato X-*<nome>*: *<valore>*. Come valore si possono utilizzare le variabili di modello (tra parentesi graffe), disponibili nelle liste a cascata nell'intestazione del messaggio. Le intestazioni devono essere separate da una riga vuota.
3. Premere il pulsante **Aggiungi**. In caso di aggiunta riuscita, il testo inserito scomparirà dal campo di input.
4. Premere  per chiudere la finestra dell'editor dei modelli.
5. Premere il pulsante **Salva** per applicare tutte le modifiche apportate.

**Esempio:**

- Per un avviso A è impostata un'intestazione personalizzata `X-Header-A: A`.
- Per un avviso B è impostata un'intestazione personalizzata `X-Header-B: B`.

Dopo l'aggiunta di un'intestazione comune `X-Header-C: C`:

- Per l'avviso A verranno impostate le intestazioni `X-Header-A: A, X-Header-C: C`.
- Per l'avviso B verranno impostate le intestazioni `X-Header-B: B, X-Header-C: C`.

Per rimuovere l'intestazione `X-Header-C: C` da tutti i modelli di avviso, è necessario modificare i modelli di avviso A e B separatamente (v. [p. 9a sopra](#)).

Per rimuovere o sostituire tutte le intestazioni di tutti gli avvisi

1. In qualsiasi blocco di avvisi via email premere il pulsante **Modifica intestazioni comuni**.
2. Nella finestra che si è aperta **Intestazioni comuni per tutti i modelli** inserire una o più intestazioni in formato `X-<nome>: <valore>`. Le nuove intestazioni sostituiranno tutte le intestazioni precedentemente impostate di tutti gli avvisi via email. Come valore si possono utilizzare le variabili di modello (tra parentesi graffe), disponibili nelle liste a cascata nell'intestazione del messaggio. Le intestazioni devono essere separate da una riga vuota.
Per rimuovere tutte le intestazioni precedentemente impostate, lasciare il campo di input vuoto.
3. Premere il pulsante **Sostituisci**. In caso di sostituzione riuscita, il testo inserito scomparirà dal campo di input.
4. Premere **✕** per chiudere la finestra dell'editor dei modelli.
5. Premere il pulsante **Salva** per applicare tutte le modifiche apportate.

Esempio:

- Per l'avviso A sono impostate le intestazioni `X-Header-A: A, X-Header-C: C`.
- Per l'avviso B sono impostate le intestazioni `X-Header-B: B, X-Header-C: C`.

Se si inserisce `X-Header-D: D` nel campo di input e si preme **Sostituisci**:

- Per l'avviso A verrà impostata l'intestazione `X-Header-D: D`. Le vecchie intestazioni verranno rimosse.
- Per l'avviso B verrà impostata l'intestazione `X-Header-D: D`. Le vecchie intestazioni verranno rimosse.

Se si lascia il campo di input vuoto e si preme **Sostituisci**:

- Per l'avviso A verranno rimosse tutte le intestazioni.
- Per l'avviso B verranno rimosse tutte le intestazioni.





Notifiche push

Per le notifiche push che vengono inviate al Pannello di controllo mobile impostare i seguenti parametri:

- Nella sezione **Invio ripetuto dal Server Dr.Web** configurare le impostazioni di invii ripetuti dell'avviso che verranno effettuati dal Server Dr.Web in caso di errore:
 - **Numero** — numero di tentativi ripetuti effettuati dal Server Dr.Web se l'invio del messaggio non è riuscito. Di default è 10.
 - **Time-out** — periodo in secondi dopo cui il Server Dr.Web effettua un nuovo tentativo di invio del messaggio. Di default è di 300 secondi.
- **Invia un messaggio di test** — per inviare un avviso di test in conformità alle impostazioni del sistema di avviso.

Avvisi attraverso il protocollo SNMP

Per gli avvisi attraverso il protocollo SNMP, impostare i seguenti parametri:

- Nella sezione **Invio ripetuto dal Server Dr.Web** è possibile configurare i parametri di tentativi ripetuti del Server Dr.Web di inviare l'avviso in caso di errore:
 - **Numero** — numero di tentativi ripetuti effettuati dal Server Dr.Web se l'invio dell'avviso non è riuscito. Di default è 10.
 - **Time-out** — periodo in secondi dopo cui il Server Dr.Web effettua un nuovo tentativo di invio dell'avviso. Di default è di 300 secondi.
- Nella sezione **Invio ripetuto dal sottosistema SNMP** è possibile configurare i parametri di tentativi ripetuti del sottosistema SNMP di inviare l'avviso in caso di errore:
 - **Numero** — numero di tentativi ripetuti effettuati dal sottosistema SNMP se l'invio dell'avviso non è riuscito. Di default è 5.
 - **Time-out** — periodo in secondi dopo cui il sottosistema SNMP effettua un nuovo tentativo di invio dell'avviso. Di default è di 5 secondi.
- **Destinatario** — entità che riceve la query SNMP. Per esempio, l'indirizzo IP o il nome DNS del computer. In ciascun campo viene inserito solo un destinatario. Per aggiungere un altro campo di destinatario, premere il pulsante . Per rimuovere un campo, premere il pulsante .
- **Mittente** — entità che invia la richiesta SNMP. Per esempio, l'indirizzo IP o il nome DNS del computer (deve essere riconosciuto dal server DNS). Di default viene utilizzato un valore vuoto.
- **Community** — community SNMP o contesto. Di default è `public`.
- **Invia messaggio di test** — per inviare un avviso di test in conformità alle impostazioni specificate.



Per ottenere le descrizioni OID all'analisi di trap SNMP, è possibile utilizzare il MIB fornito insieme al Server Dr.Web. I file `DRWEB-ESUITE-NOTIFICATIONS-MIB.txt` e `DRWEB-MIB.txt` si trovano nella sottodirectory `etc` della directory di installazione di Server Dr.Web.

Avvisi attraverso il protocollo Syslog

Per gli avvisi attraverso il protocollo Syslog impostare i seguenti parametri:

- Nella sezione **Invio ripetuto dal Server Dr.Web** è possibile configurare i parametri di tentativi ripetuti del Server Dr.Web di inviare l'avviso in caso di errore:
 - **Numero** — numero di tentativi ripetuti effettuati dal Server Dr.Web se l'invio dell'avviso non è riuscito. Di default è 10.
 - **Time-out** — periodo in secondi dopo cui il Server Dr.Web effettua un nuovo tentativo di invio dell'avviso. Di default è di 300 secondi.
- **Destinatario** — indirizzo del destinatario dell'avviso tramite protocollo Syslog. Il protocollo di trasmissione è TCP o UDP. Di default è il protocollo UDP, la porta 514.
- **Formato** — formato dell'avviso: RFC 5424 o CEF (Common Event Format). Di default è RFC 5424.
- **Timeout della connessione al destinatario (s)** — periodo in secondi durante cui Server Dr.Web tenta di connettersi al destinatario dell'avviso tramite protocollo TCP. Di default è di 5 secondi.
- **Facility** — rappresenta la categoria del processo che ha generato l'avviso (per esempio, kernel, sistema di posta). Assume i valori compresi tra 0 e 23. Di default è 14.
- **Mittente** — identificatore di Server Dr.Web (nome di dominio completo, nome host, indirizzo IP). Di default viene utilizzato un valore vuoto.
- **Invia messaggio di test** — per inviare un avviso di test in conformità alle impostazioni specificate.







10.10.2. 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 della web console

1. Selezionare la voce **Amministrazione** nel menu principale del Pannello di controllo. Nella finestra che si è aperta selezionare la voce del menu di gestione **Avvisi della web console**. Si apre l'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 tramite le opzioni nella barra degli strumenti:
- 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 secondo le impostazioni definite.
 - 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 i seguenti elementi della barra degli strumenti:
 -  **Elimina avvisi** — per eliminare definitivamente tutti gli avvisi selezionati senza possibilità di recupero.
 -  **Contrassegna avvisi come letti** — per contrassegnare come letti tutti gli avvisi selezionati.
 - Per gestire determinati tipi di avvisi, spuntare i flag di fronte agli avvisi dei tipi richiesti. Con questo diventano disponibili i seguenti elementi della barra degli strumenti:
 -  **Postazioni non confermate** — l'opzione è disponibile solo se vengono selezionati gli avvisi di tipo **La postazione è in attesa di conferma**. Nella lista a cascata è possibile confermare la registrazione o negare l'accesso al Server Dr.Web per le postazioni dagli avvisi selezionati.
 -  **Scansiona** — l'opzione è disponibile solo se vengono selezionati gli avvisi dei tipi **Un'epidemia nella rete, Errore di scansione, È stata rilevata una minaccia alla sicurezza**. Nella lista a cascata è possibile configurare i parametri di avvio di Scanner Dr.Web sulle postazioni dagli avvisi selezionati.
 -  **Gestione dei componenti** — l'opzione è disponibile solo se vengono selezionati gli avvisi del tipo **Errore critico di aggiornamento della postazione**. Nella lista a cascata è possibile configurare la variante di avvio dell'aggiornamento del software antivirus sulle postazioni dagli avvisi selezionati.
 -  **Riavvia la postazione** — l'opzione è disponibile solo se vengono selezionati gli avvisi del tipo **È necessario riavviare la postazione per applicare gli aggiornamenti**. L'opzione lancia il riavvio delle postazioni dagli avvisi selezionati.
 - Se necessario, è possibile esportare gli avvisi in un file. È possibile esportare gli avvisi visualizzati al momento nella tabella secondo le impostazioni dell'intervallo di tempo e dei filtri nelle colonne della tabella (v. p. 4.b).

Per esportare avvisi, fare clic su uno dei seguenti pulsanti 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.**



4. Per gestire gli avvisi tramite le opzioni disponibili nella tabella degli avvisi:
- Impostare l'icona  **Conserva il messaggio senza la rimozione automatica** 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 degli avvisi nella sezione [Configurazione degli avvisi](#) nelle impostazioni del metodo di invio **Console web**). Tali avvisi verranno conservati fino a quando non verranno rimossi manualmente nella sezione **Avvisi della web console** o non verrà deselezionata l'icona  di fronte a questi avvisi.
 - Per visualizzare soltanto determinati avvisi, fare clic nella tabella sull'intestazione della colonna che si vuole filtrare. Nel menu che si è aperto spuntare i flag per i parametri degli avvisi che verranno visualizzati nella tabella.

Possono essere filtrate le seguenti sezioni:

Colonna	Parametro	Azione
Gravità	Critica	Per visualizzare gli avvisi soltanto con il livello di gravità selezionato. Per visualizzare tutti gli avvisi, spuntare tutti i flag.
	Alta	
	Media	
	Bassa	
	Minima	
Fonte	Agent	Per visualizzare gli avvisi relativi agli eventi sulle postazioni.
	Server Dr.Web	Per visualizzare gli avvisi relativi agli eventi sul Server Dr.Web.

- Per configurare l'aspetto della tabella, fare clic sull'icona  nell'angolo destro dell'intestazione della tabella. Nella lista a cascata è possibile configurare le seguenti opzioni:
 - Attivare o disattivare la continuazione in nuove righe per messaggi lunghi.
 - Selezionare colonne che verranno visualizzate nella tabella (sono contrassegnate da un flag accanto al nome). Per attivare/disattivare una colonna, fare clic sulla riga con il suo nome.
 - Selezionare l'ordine delle colonne nella tabella. Per modificare l'ordine, trascinare nella lista la colonna desiderata sul posto richiesto.

10.10.3. 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 degli avvisi](#).



Per visualizzare e gestire gli avvisi non inviati

1. Selezionare la voce **Amministrazione** nel menu principale del Pannello di controllo. Nella finestra che si è aperta selezionare la voce del menu di gestione **Avvisi non inviati**. Si apre l'elenco degli avvisi non inviati di questo Server Dr.Web.
2. Nell'elenco degli avvisi non inviati vengono elencati gli avvisi di cui l'invio non è riuscito, ma il numero di tentativi di invio, determinato nelle impostazioni di questo avviso, non si è ancora esaurito.
3. La tabella di avvisi non inviati contiene le seguenti informazioni:
 - **Avviso** — nome dell'avviso dall'elenco degli avvisi predefiniti.
 - **Intestazione** — nome del blocco di avvisi, secondo le cui impostazioni viene inviato questo avviso.
 - **Tentativi di invio rimanenti** — numero di tentativi rimanenti di invio dell'avviso se un invio non è riuscito. Il numero iniziale di tentativi di invio ripetuto viene impostato quando si configurano gli avvisi nella sezione [Configurazione degli avvisi](#). Dopo che un avviso è stato inviato, non è possibile modificare il numero di tentativi di invio ripetuto di questo avviso.
 - **Ora 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 quando si configurano gli avvisi nella sezione [Configurazione degli avvisi](#). Dopo che un avviso è stato inviato, non è possibile modificare la periodicità di tentativi ripetuti di invio di questo avviso.
 - **Destinatario** — indirizzi dei destinatari dell'avviso.
 - **Errore** — errore per cui non è stato possibile inviare l'avviso.
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. Verrà effettuato un tentativo straordinario di invio dell'avviso. Se l'invio non sarà riuscito, il numero di tentativi rimanenti diminuirà di uno, e il tempo del successivo tentativo verrà conteggiato dal momento dell'invio corrente con la periodicità impostata nella sezione [Configurazione degli avvisi](#).
 - ✖ **Rimuovi** — per rimuovere definitivamente tutti gli avvisi non inviati selezionati senza possibilità di recupero.
5. Gli avvisi non inviati vengono cancellati dalla lista nei seguenti casi:
 - a) L'avviso è stato inviato 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 degli avvisi](#) è stato eliminato il blocco di avvisi, secondo le cui impostazioni venivano inviati questi avvisi.

10.11. 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 scopo, il repository opera con set di file chiamati *prodotti*. Ciascun prodotto è situato in una sottodirectory separata della directory di Server Dr.Web `var/repository`. Le funzioni di repository e la loro gestione vengono effettuate indipendentemente per ciascun prodotto.

Per la gestione del repository si utilizza il concetto *revisione* del prodotto. Una revisione è uno stato dei file di un prodotto che è corretto a un determinato momento (comprende i nomi dei file e i checksum), è caratterizzata da un numero univoco.

Aggiornamento dei prodotti del repository

L'aggiornamento delle revisioni di prodotti può essere effettuato nelle seguenti direzioni:

a) Download degli aggiornamenti sul Server Dr.Web da SAM Dr.Web.

L'aggiornamento del repository di Server Dr.Web da SAM viene effettuato automaticamente secondo i task nel calendario di Server Dr.Web.

- Per vedere i task per l'aggiornamento del repository, andare alla sezione [Configurazione generale del repository](#) scheda **Scheduler**.
- Per modificare il calendario dell'aggiornamento da SAM, andare alla sezione [Configurazione del calendario di Server Dr.Web](#).
- Per verificare la disponibilità degli aggiornamenti e scaricarli manualmente, andare alla sezione [Stato del repository](#) e premere il pulsante **Verifica aggiornamenti**.



Vedi inoltre [Aggiornamento del repository di un Server Dr.Web non connesso a internet](#).

b) Distribuzione degli aggiornamenti tra vari Server Dr.Web in una configurazione con diversi server.

Se più Server Dr.Web sono installati nella rete antivirus, è possibile configurare le relazioni tra i server per la trasmissione degli aggiornamenti del repository:

- Nel caso di relazione principale-subordinato, i Server Dr.Web che ricevono aggiornamenti da SAM saranno quelli principali, i Server Dr.Web subordinati riceveranno tutti gli aggiornamenti dai Server Dr.Web principali in maniera automatica.



- Nel caso di relazione tra Server Dr.Web paritari, qualsiasi di essi può essere nominato server che riceve aggiornamenti da SAM. In questo caso, tutti gli altri Server Dr.Web riceveranno tutti gli aggiornamenti da esso in maniera automatica.

La configurazione delle reazioni tra i server è descritta nella sezione [Caratteristiche di una rete con diversi Server Dr.Web](#).



Se nella rete sono configurate relazioni tra i server, e i Server Dr.Web adiacenti ricevono aggiornamenti dal Server Dr.Web corrente, è necessario attivare sul Server Dr.Web corrente anche l'aggiornamento dei sistemi e delle lingue di interfaccia dei Server Dr.Web adiacenti.

c) Distribuzione degli aggiornamenti dal Server Dr.Web sulle postazioni.

La verifica, il download dal Server Dr.Web e l'installazione degli aggiornamenti sulle postazioni vengono effettuati in maniera automatica ogni volta che gli Agent Dr.Web si connettono al Server Dr.Web, nonché con una determinata periodicità nel processo di funzionamento degli Agent Dr.Web (un'attività non configurabile, viene effettuata in modo trasparente per l'amministratore).

Se necessario, è possibile configurare limitazioni di tempo e quantità di traffico per gli aggiornamenti degli Agent Dr.Web nella sezione [Limitazione degli aggiornamenti delle postazioni](#).

Configurazione dei parametri del repository

Il repository permette all'Amministratore della rete antivirus di impostare i seguenti parametri:

- **Lista dei siti di aggiornamento per il tipo di operazioni a).**

I parametri di connessione a SAM vengono configurati nella sezione [Configurazione generale del repository](#).

- **Limitazione della lista dei prodotti che richiedono il tipo di sincronizzazione a).**

La lista dei prodotti da scaricare da SAM viene configurata nelle sezioni [Configurazione generale del repository](#) e [Configurazione dettagliata del repository](#).

In questo modo, l'amministratore ha la possibilità di tracciare le sole modifiche necessarie di singole categorie di prodotti.

- **Limitazione della lista delle parti di un prodotto che richiedono il tipo di sincronizzazione c).**

L'amministratore del Server Dr.Web può scegliere quello che deve essere installato sulle postazioni. I componenti antivirus possono essere selezionati nella sezione [Componenti da installare del pacchetto antivirus](#).



- **Controllo del passaggio a nuove revisioni.**

La configurazione delle revisioni per ciascun prodotto del repository separatamente viene impostata nella sezione [Configurazione dettagliata del repository](#).

È possibile testare in autonomo i prodotti prima di distribuirli.

- **Gestione del contenuto del repository a livello di directory e file.**

La sezione [Contenuti del repository](#) consente di visualizzare e gestire il contenuto corrente del repository a livello di directory e file del repository: esportare ed importare sia i singoli prodotti che l'intero contenuto del repository e le sue impostazioni.

Lista dei prodotti del repository

Attualmente sono forniti i seguenti prodotti:

- **Utility di amministrazione Dr.Web**

Utility per tutti i sistemi operativi supportati:

- Loader di repository Dr.Web (versioni grafica e console),
- Pannello di controllo mobile Dr.Web (link su App Store e Google Play),
- Utility Dr.Web per la raccolta di informazioni sul sistema,
- Utility di generazione delle chiavi e dei certificati digitali,
- Utility di diagnostica remota del Server Dr.Web,
- Utility di diagnostica remota di Server Dr.Web per l'uso degli script,
- Utility di rimozione di Dr.Web per Windows,
- Utility per l'installazione remota di Agent Dr.Web per UNIX,
- Utility per l'installazione remota di Agent Dr.Web per Windows.



Tutte le utility sono disponibili per il download attraverso la sezione del Pannello di controllo **Amministrazione** → **Utility**.

- **Agent Dr.Web per UNIX**

Database dei filtri incorporati e di Antispam, nonché il motore di Antispam di Dr.Web per UNIX.

- **Agent Dr.Web per Windows**

Software dei componenti antivirus per le postazioni SO Windows.

- **Database di Dr.Web per Android**

Database dei virus per le postazioni SO Android.



- **Database di SplDer Gate**

Database dei filtri incorporati dei componenti antivirus per Windows.

- **Database di Antispam Dr.Web**

Database di Antispam di Dr.Web per Windows.

- **Database dei virus Dr.Web**

Database dei virus, motori antivirus per le postazioni SO Windows e SO della famiglia UNIX.

- **Dati di sicurezza di Server Dr.Web**

Set di chiavi, script e certificati che forniscono sicurezza durante l'aggiornamento dei componenti della rete antivirus e lo scambio di dati tra il Server Dr.Web e gli Agent Dr.Web.

- **Applicazioni affidabili**

Gruppi di applicazioni affidabili per il componente Controllo delle applicazioni per le postazioni con SO Windows.



Il prodotto **Applicazioni affidabili** non viene aggiornato da SAM. Questo prodotto può solo essere distribuito tra i Server Dr.Web adiacenti attraverso la comunicazione tra i server.

Per maggiori informazioni su come configurare il repository per il prodotto **Applicazioni affidabili** vedi sezione [Applicazioni affidabili](#).

- **Documentazione**

Un set di manuali e materiali di consultazione disponibili attraverso la sezione **Supporto** del Pannello di controllo.

- **Hash di minacce conosciuti**

Liste degli hash di minacce conosciuti.

- **Prodotti aziendali Dr.Web**

Pacchetti di installazione per i seguenti prodotti:

- Prodotti per l'installazione sulle postazioni protette sotto SO UNIX (inclusi i server LAN), Android, macOS,
- Dr.Web per IBM Lotus Domino,
- Dr.Web per Microsoft Exchange Server,
- Server proxy Dr.Web — pacchetto per l'installazione autonoma di un Server proxy non legato ad Agent Dr.Web per Windows,
- Installer completo di Agent Dr.Web per Windows,
- Agent Dr.Web per Active Directory,
- Utility per modificare lo schema Active Directory,



- Utility per modificare gli attributi degli oggetti Active Directory,
- NAP Validator.



Tutti i pacchetti di installazione per i prodotti aziendali sono disponibili per il download sulla pagina di installazione sull'indirizzo:

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

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

- **Modulo di aggiornamento Dr.Web**

Modulo per l'aggiornamento di Agent Dr.Web per Windows versione 6 alla versione attuale.

- **Notizie di Doctor Web**

Notizie dal sito Doctor Web.

- **Server proxy Dr.Web**

Software per installare un Server proxy Dr.Web legato a un Agent Dr.Web per Windows.

- **Server Dr.Web**

- software di Server Dr.Web,
- software di Pannello di controllo della sicurezza Dr.Web.

10.11.1. Stato del repository

Per controllare lo stato attuale del repository o aggiornare i componenti della rete antivirus

1. Selezionare la voce **Amministrazione** nel 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 dei prodotti.



Nella colonna **Stato** è indicato lo stato dei prodotti nel repository di Server Dr.Web al momento dell'ultimo aggiornamento.

3. Per gestire i contenuti del repository, utilizzare i seguenti pulsanti nella barra degli strumenti:
 - Premere il pulsante **Verifica aggiornamenti** per verificare la disponibilità degli aggiornamenti di tutti i prodotti su SAM. Se un componente che viene verificato è obsoleto, esso verrà aggiornato in automatico.



- Premere uno dei seguenti pulsanti nella barra degli strumenti per scaricare il log di aggiornamento del repository:

 **Registra le informazioni in file CSV,**

 **Registra le informazioni in file HTML,**

 **Registra le informazioni in file XML,**

 **Registra le informazioni in file PDF.**

- Premere il pulsante  **Ricarica il repository da disco** per ricaricare la versione corrente del repository da disco.

Quando viene avviato, il Server Dr.Web carica i contenuti del repository nella memoria, e se nel processo di funzionamento del Server Dr.Web i contenuti del repository sono stati modificati dall'amministratore in un modo diverso da quello fornito dal Pannello di controllo, per esempio, aggiornati tramite un'utility esterna o manualmente, per utilizzare la versione del repository caricata sul disco, è necessario ricaricare il repository.

10.11.2. Aggiornamenti differiti

La sezione **Aggiornamenti differiti** contiene una lista di prodotti per cui gli aggiornamenti di prodotti sono stati temporaneamente vietati nella sezione **Configurazione dettagliata del repository** → <Prodotto> → [Aggiornamenti differiti](#). Una revisione differita è considerata *congelata*.

La tabella dei prodotti congelati contiene le seguenti informazioni:

- **Directory nel repository** — nome della directory del prodotto congelato nel repository:
 - 05-drwmeta — dati di sicurezza di Server Dr.Web,
 - 10-drwbases — database dei virus,
 - 10-drwgatedb — database di SpIDer Gate,
 - 10-drwspamdb — database di Antispam,
 - 10-drwupgrade — Modulo di aggiornamento Dr.Web,
 - 15-drwhashdb — hash di minacce conosciuti,
 - 20-drwagent — Agent Dr.Web per Windows,
 - 20-drwandroid11 — database di Dr.Web per Android,
 - 20-drwcs — Server Dr.Web,
 - 20-drwunix — Agent Dr.Web per UNIX,
 - 25-drwcsdoc — documentazione,
 - 40-drwproxy — Server proxy Dr.Web,
 - 70-drwextra — prodotti aziendali Dr.Web,
 - 70-drwutils — utility di amministrazione Dr.Web,
 - 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 il congelamento del prodotto e includere questa revisione nell'elenco delle revisioni con la distribuzione sulle postazioni secondo la [procedura](#) generale.
 - ✘ **Annulla l'aggiornamento** — per annullare il congelamento del prodotto e vietare questa revisione. Riprende il processo dell'ottenimento degli aggiornamenti da SAM. La revisione scongelata verrà rimossa dall'elenco delle revisioni del prodotto. Quando arriverà 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 congelamento viene conteggiato dal momento della ricezione della revisione da 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.

10.11.3. Configurazione generale del repository

La sezione **Configurazione generale del repository** consente di impostare i parametri di connessione a SAM e di aggiornamento del repository per tutti i prodotti.

Per modificare la configurazione del repository

1. Selezionare la voce **Amministrazione** nel menu principale del Pannello di controllo.
2. Nella finestra che si è aperta selezionare la voce del menu di gestione **Configurazione generale del repository**.



3. Configurare tutti i parametri necessari dell'aggiornamento da SAM descritti [di seguito](#).
4. Se nel processo di modifica dei parametri è necessario annullare le modifiche apportate, utilizzare i seguenti pulsanti di fronte a ciascun parametro:
 - ➡ **Imposta il valore iniziale** — resetta il valore del parametro al valore che aveva prima della modifica corrente.
 - ➡ **Resetta al valore di default** — resetta il valore del parametro al valore salvato nel file di configurazione di Server Dr.Web.
5. Premere il pulsante **Salva** per salvare tutte le modifiche apportate nei file di configurazione del repository. La versione corrente del repository viene ricaricata da disco.



Ci vuole del tempo per applicare le nuove impostazioni della configurazione del repository. Se il repository viene aggiornato da SAM subito dopo la modifica della configurazione, possono essere utilizzate le impostazioni precedenti.

10.11.3.1. SAM Dr.Web

Nella scheda **SAM Dr.Web** vengono configurati i parametri di connessione al Sistema di aggiornamento mondiale Dr.Web. Gli aggiornamenti vengono scaricati tramite i protocolli la cui lista è presentata nella lista a cascata **Protocollo di ricezione degli aggiornamenti**:

Tipo di protocollo	Descrizione
HTTP/HTTPS	Protocolli per la ricezione degli aggiornamenti da un server web
FTP/FTPS	Protocolli per la ricezione degli aggiornamenti da un FTP server
FILE	Protocollo per la ricezione degli aggiornamenti da una directory locale su un computer con Server Dr.Web installato.
SMB/SMBS	Protocolli per la ricezione degli aggiornamenti da un file system unico (sono disponibili solo per SO della famiglia UNIX)
SCP/SFTP	Protocolli per la ricezione degli aggiornamenti tramite una connessione sicura

Per modificare la connessione a SAM



- Dalla lista a cascata **Protocollo di ricezione degli aggiornamenti** selezionare il tipo di protocollo per la ricezione degli aggiornamenti dai server di aggiornamento. Per tutti i protocolli il download degli aggiornamenti viene eseguito secondo le impostazioni nella sezione **Lista dei server del Sistema di aggiornamento mondiale Dr.Web**.
- **URI di base** — la directory sui server di aggiornamento che contiene gli aggiornamenti dei prodotti Dr.Web. Se l'aggiornamento viene effettuato dai server SAM Dr.Web, si consiglia di non modificare questa impostazione senza necessità.
- Se nella lista **Protocollo di ricezione degli aggiornamenti** è selezionato uno dei protocolli protetti che supporta la crittografia, dalla lista a cascata **Certificati validi** selezionare il tipo



di certificati TLS da accettare automaticamente quando viene stabilita una connessione attraverso il protocollo selezionato.

- Se nella lista **Certificati validi** è selezionata l'opzione **Personalizzato**, è necessario impostare il percorso del file con il proprio certificato TLS nel campo **Certificato**.
- **Nome utente** — il nome utente per l'autenticazione sul server di aggiornamento, se il server richiede l'autenticazione.
- **Password** — la password dell'utente per l'autenticazione sul server di aggiornamento, se il server richiede l'autenticazione.
- Dalla lista a cascata **Metodo di autenticazione** selezionare il metodo di autenticazione sul server di aggiornamento.
- Nel campo **Numero di revisioni temporaneamente conservate** viene impostato il numero di revisioni di ciascun prodotto temporaneamente conservate su disco, senza contare le revisioni contrassegnate nella scheda **Lista delle revisioni** sezione **Configurazione dettagliata del repository**.

Se necessario, è possibile configurare questa impostazione separatamente per ciascun prodotto nella sezione [Sincronizzazione](#), ma dopo un salvataggio di modifiche nella configurazione generale l'impostazione sarà sostituita dal valore generale.

- Spuntare il flag **Utilizza CDN** per consentire l'utilizzo di Content Delivery Network per il caricamento del repository.
- 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 aggiornamento della società Doctor Web. Se necessario, è possibile configurare le proprie zone di aggiornamento ed inserirle nella lista dei server per la ricezione degli aggiornamenti.

10.11.3.2. Scheduler

Nella scheda **Scheduler** sono riportati tutti i task di aggiornamento repository presenti nel calendario di Server Dr.Web.



I task di aggiornamento repository vengono creati, eliminati e modificati nella sezione [Configurazione del calendario di Server Dr.Web](#).



10.11.3.3. Agent Dr.Web

- Nella scheda **Agent Dr.Web per UNIX** selezionare per quali sistemi operativi della famiglia UNIX è necessario aggiornare i componenti che vengono 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**.

- Nella scheda **Agent Dr.Web per Windows** indicare se è necessario aggiornare tutti i componenti che vengono installati su postazioni SO Windows o solo i database dei virus.
- Nella scheda **Lingue di Agent Dr.Web per Windows** impostare una lista delle lingue dell'interfaccia di Agent Dr.Web e di pacchetto antivirus per SO Windows che verranno scaricate da SAM.

10.11.3.4. Server Dr.Web

- Nella scheda **Server Dr.Web** indicare per quali sistemi operativi verrà eseguito l'aggiornamento dei file di Server Dr.Web:
 - Per ricevere gli aggiornamenti per i Server Dr.Web sotto tutti i sistemi operativi supportati, spuntare il flag **Aggiorna tutte le piattaforme disponibili su SAM**.
 - Per ricevere gli aggiornamenti per il Server Dr.Web solo sotto alcuni dei sistemi operativi supportati, spuntare i flag solo accanto a questi sistemi operativi.



Per disattivare completamente la ricezione degli aggiornamenti da SAM per il Server Dr.Web, passare alla sezione **Configurazione dettagliata del repository**, voce **Server Dr.Web**, e nella scheda **Sincronizzazione** spuntare il flag **Disattiva l'aggiornamento del prodotto**.

- Nella scheda **Lingue di Pannello di controllo della sicurezza Dr.Web** impostare una lista delle lingue dell'interfaccia di Pannello di controllo che verranno scaricate da SAM.
 - Nella sottosezione **Lingue utilizzate** viene fornita una lista di lingue assegnate ad almeno un amministratore nelle impostazioni.
 - Nella sezione **Lingue non utilizzate** viene fornita una lista di lingue che non sono assegnate a nessun amministratore nelle impostazioni.
- Nella scheda **Documentazione** selezionare le lingue in cui saranno disponibili i manuali nella sezione [Aiuto](#) → **Documentazione**.
 - La suddivisione della documentazione in **Lingue utilizzate/Non utilizzate** è implementata secondo lo stesso principio della scheda **Lingue del Pannello di controllo della sicurezza Dr.Web**.
 - Per avere accesso ai manuali in formato PDF, spuntare il flag **Aggiorna documentazione** nella sottosezione **Documentazione in formato PDF** sotto la selezione delle lingue.



10.11.3.5. 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 della società Doctor Web scaricate nella sezione del menu principale del Pannello di controllo  **Supporto** → **Notizie**.

10.11.3.6. Pacchetti di installazione Dr.Web

- Nella scheda **Prodotti aziendali Dr.Web** nella lista a cascata selezionare quali prodotti verranno aggiornati da SAM:
 - **Aggiorna tutti i prodotti** — durante l'aggiornamento del repository da SAM verranno aggiornati tutti i prodotti aziendali disponibili.
 - **Aggiorna solo i prodotti selezionati** — durante l'aggiornamento del repository da SAM verranno aggiornati solo i prodotti per cui sono impostati i flag nella lista sottostante.

Dopo il caricamento da SAM i prodotti aziendali Dr.Web diventeranno disponibili nella sezione **Amministrazione** → **Funzioni aggiuntive** → [Prodotti aziendali](#) e sulla pagina di installazione sull'indirizzo:

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

dove *<indirizzo_Server_Dr.Web>* è l'indirizzo IP o il nome DNS del computer su cui è installato il Server Dr.Web; *<numero_porta>* è il numero di porta 9081 (o 9080 per http).

- Nella scheda **Utility di amministrazione Dr.Web** nella lista a cascata selezionare quali utility verranno aggiornate da SAM:
 - **Aggiorna tutti i prodotti** — durante l'aggiornamento del repository da SAM verranno aggiornate tutte le utility di amministrazione disponibili.
 - **Aggiorna solo i prodotti selezionati** — durante l'aggiornamento del repository da SAM verranno aggiornate solo le utility per cui sono impostati i flag nella lista sottostante.

Dopo essere state scaricate da SAM, le utility di amministrazione saranno disponibili nella sezione **Amministrazione** → **Funzioni aggiuntive** → [Utility](#).

10.11.3.7. Server proxy Dr.Web

Nella scheda **Server proxy Dr.Web** indicare per quali sistemi operativi verrà eseguito l'aggiornamento dei file di Server proxy Dr.Web:

- Per ricevere gli aggiornamenti per i Server proxy Dr.Web sotto tutti i sistemi operativi supportati, spuntare il flag **Aggiorna tutte le piattaforme disponibili su SAM**.
- Per ricevere gli aggiornamenti per il Server proxy Dr.Web solo sotto alcuni dei sistemi operativi supportati, spuntare i flag solo di fronte a questi sistemi operativi.

10.11.4. Configurazione dettagliata del repository

La sezione **Configurazione dettagliata del repository** consente di configurare revisioni separatamente per ciascun prodotto nel repository.

Per modificare la configurazione del repository

1. Selezionare la voce **Amministrazione** nel menu principale del Pannello di controllo.
2. Nella finestra che si è aperta nella sottosezione del menu di gestione **Configurazione dettagliata del repository** selezionare il prodotto che si vuole modificare.
3. Configurare tutti i parametri necessari del repository del prodotto selezionato, che vengono descritti [di seguito](#).
4. Nella barra degli strumenti sono disponibili le seguenti opzioni studiate per gestire l'intero repository del prodotto:
 - **Rimuovi prodotto dal repository** — per rimuovere completamente il prodotto dal repository. Verranno rimosse tutte le revisioni del prodotto e verrà disattivato l'aggiornamento del prodotto da SAM. Il pulsante è disponibile se il prodotto non è ancora stato rimosso dal repository. Dopo la rimozione del prodotto il pulsante cambia nome per **Ripristina prodotto nel repository**.



Dopo la rimozione del prodotto dal repository la scheda **Lista delle revisioni** sarà vuota, le altre schede in questa sezione rimarranno nello stato normale, però le loro impostazioni non verranno applicate in quanto il prodotto è assente nel repository.

- **Ripristina prodotto nel repository** — per ripristinare il prodotto nel repository, se è stato rimosso in precedenza tramite il pulsante **Rimuovi prodotto dal repository**. Verrà attivato l'aggiornamento del prodotto da SAM. Nel repository verrà caricata la revisione del prodotto più recente disponibile in SAM. Prestare attenzione alla possibile quantità di dati da scaricare. Il download di aggiornamenti viene configurato nella sezione [Configurazione generale del repository](#). Dopo il ripristino del prodotto il pulsante cambia nome per **Rimuovi prodotto dal repository**.
- **Salva e ricarica da disco** — per salvare tutte le modifiche apportate. La versione corrente del repository viene ricaricata da disco (v. inoltre sezione [Stato del repository](#)).

10.11.4.1. Lista delle revisioni

Nella scheda **Lista delle revisioni** vengono riportate le informazioni su tutte le revisioni di questo prodotto disponibili su questo Server Dr.Web.

Per rimuovere alcune delle revisioni, spuntare i flag di fronte a queste revisioni e premere nella barra degli strumenti il pulsante **Rimuovi le revisioni selezionate**.










Non è possibile rimuovere tutte le revisioni di un prodotto. Il prodotto deve contenere almeno una revisione.

Per rimuovere un prodotto per intero, utilizzare il pulsante **Rimuovi prodotto dal repository**.

La rimozione delle revisioni è un'operazione irreversibile.

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 Dr.Web e il software antivirus su postazioni.</p> <p>La revisione da distribuire viene selezionata nel seguente modo:</p> <ol style="list-style-type: none">Viene distribuita la revisione che è contrassegnata dal marcatore  nella colonna Corrente. Può essere contrassegnata solo una revisione.Se nella colonna Corrente nessuna revisione è contrassegnata, viene distribuita la revisione più recente. <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 Dr.Web. Per le azioni in caso di congelamento della revisione v. sottosezione Aggiornamenti differiti.</p> <p>Se è presente una revisione congelata, la revisione da distribuire viene selezionata nel seguente modo:</p> <ol style="list-style-type: none">Se è impostato il marcatore  nella colonna Corrente, su postazioni viene distribuita la revisione corrente.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 del prodotto da utilizzare per l'aggiornamento degli Agent Dr.Web 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> <p>Vedere inoltre Rollback della revisione del prodotto alla versione precedente.</p>
Conservata	<p>Impostare il marcatore  per conservare questa revisione alla pulizia automatica del repository (v. inoltre Sincronizzazione).</p>



Nome di colonna	Descrizione dei contenuti
	<p>Il marcatore può essere impostato per più revisioni alla volta.</p> <p>Il marcatore può anche essere non impostato per nessuna revisione.</p> <p>Se una revisione di un prodotto funziona in modo stabile, può essere contrassegnata come conservata. Se da SAM arriverà una revisione instabile, sarà possibile eseguire il rollback a quella precedente conservata.</p>
Trattenuta	<p>Un marcatore automatico determina che i componenti da questa revisione sono installati sulle postazioni con limitazione di aggiornamento (nella sezione Limitazione degli aggiornamenti delle postazioni sono impostate le opzioni Aggiorna soltanto i database o Proibisci tutti gli aggiornamenti).</p> <p>Tale revisione non viene rimossa alla pulizia automatica del repository e può essere utilizzata se sarà necessario reinstallare componenti falliti su una postazione o installare ulteriori componenti da questa revisione.</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>

Rollback della revisione del prodotto alla versione precedente

La possibilità di eseguire il rollback dei prodotti installati sulle postazioni alle versioni precedenti è determinata dalle seguenti disposizioni:

- I prodotti con i database dei componenti (database dei virus, database di SpIDer Gate, database di Antispam, database di Dr.Web per Android) possono sempre essere riportati alla versione precedente.
- Per eseguire il rollback di Agent Dr.Web per Windows, è necessario consentire l'opzione **Consenti il passaggio a revisioni precedenti** nella sezione [Limitazione degli aggiornamenti delle postazioni](#).



Nel caso di rollback della versione di Agent Dr.Web per Windows alla revisione precedente (per installare sulle postazioni Agent Dr.Web di una versione precedente), verrà eseguito un riavvio forzato delle postazioni con un intervallo di cinque minuti. Non è possibile modificare l'intervallo o annullare il riavvio. Gli utenti della postazione vengono notificati del prossimo riavvio in una notifica a comparsa.

- Gli altri prodotti (in particolare, Applicazioni affidabili del componente Controllo delle applicazioni) verranno riportati alla versione precedente se è spuntato il flag **Ricevi gli aggiornamenti più recenti** nella sezione [Limitazione degli aggiornamenti delle postazioni](#), o il rollback viene eseguito alla revisione contrassegnata dal marcatore **Corrente** nella configurazione dettagliata del repository. In tutti gli altri casi, il rollback non viene eseguito, il Server Dr.Web attende la comparsa di una versione più recente.



10.11.4.2. Sincronizzazione

Nella scheda **Sincronizzazione** vengono configurati i parametri di aggiornamento del repository di Server Dr.Web da SAM:

- Nel campo **Numero di revisioni temporaneamente conservate** viene impostato il numero di revisioni del prodotto che vengono temporaneamente conservate su disco, senza contare le revisioni contrassegnate almeno in una delle colonne nella scheda **Lista delle revisioni**. Se è arrivata una nuova revisione e il numero di revisioni del prodotto temporaneamente conservate ha già raggiunto il valore massimo ammissibile, viene rimossa la revisione più vecchia tra quelle temporaneamente conservate. Le revisioni contrassegnate come **Corrente**, **Conservata**, **Distribuita** e **Trattenuta** non sono soggette a rimozione automatica e non sono incluse nel calcolo delle revisioni temporaneamente conservate.

Questa impostazione verrà sovrascritta da un singolo valore per tutti i prodotti se viene modificata la sezione [SAM Dr.Web](#).

- Spuntare il flag **Disattiva l'aggiornamento del prodotto** per disattivare la ricezione degli aggiornamenti di questo prodotto dai server SAM. Gli Agent Dr.Web in tale caso verranno aggiornati alla revisione corrente sul Server Dr.Web (o secondo la [procedura di selezione](#) della revisione da distribuire).
- Spuntare il flag **Aggiorna solo su richiesta** affinché il prodotto venga aggiornato da SAM solo quando questo prodotto viene richiesto dalle postazioni. Altrimenti, gli aggiornamenti del prodotto non vengono scaricati da SAM.

Se il Server Dr.Web è connesso a internet per la ricezione automatica degli aggiornamenti del repository da SAM, con l'utilizzo di questa opzione non è richiesta alcuna azione aggiuntiva da parte dell'amministratore: gli aggiornamenti verranno scaricati automaticamente non appena una delle postazioni richiederà l'aggiornamento di questo prodotto dal Server Dr.Web.

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



Se è installato il Server Dr.Web versione 13 o subito dopo l'aggiornamento del Server Dr.Web alla versione 13, di default gli aggiornamenti dei prodotti del repository **Database di Dr.Web per Android**, **Agent Dr.Web per UNIX** e **Server proxy Dr.Web** vengono scaricati da SAM solo quando questi prodotti vengono richiesti dalle postazioni.

- Nella sottosezione **Distribuzione attraverso le relazioni tra i server** vengono configurati i seguenti parametri:
 - Spuntare il flag **Vieta il trasferimento degli aggiornamenti ai Server Dr.Web adiacenti** per vietare l'invio degli aggiornamenti del prodotto attraverso le relazioni tra i server. Questa opzione non influisce sulle impostazioni dell'aggiornamento del prodotto da SAM.



- Spuntare il flag **Vieta la ricezione degli aggiornamenti dai Server Dr.Web adiacenti** per vietare la ricezione degli aggiornamenti del prodotto attraverso le relazioni tra i server. Questa opzione non influisce sulle impostazioni dell'aggiornamento del prodotto da SAM.

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.

10.11.4.3. Avvisi

Nella scheda **Avvisi** vengono configurati gli avvisi sugli aggiornamenti del repository:

- Spuntare il flag **Non avvisare soltanto dei seguenti file**, per disattivare l'invio degli avvisi solo per gli eventi relativi ai file indicati nella lista di seguito.
- Spuntare il flag **Avvisa soltanto dei seguenti file** per inviare avvisi solo per gli eventi relativi ai file indicati nella lista di seguito.

Le liste dei file vengono impostate nel formato di espressioni regolari.

Se le liste delle eccezioni non sono impostate, verranno inviati tutti gli avvisi attivati sulla pagina [Configurazione degli avvisi](#).

Gli avvisi sugli aggiornamenti del repository vengono configurati sulla pagina di configurazione degli avvisi nella sottosezione **Repository**.

10.11.4.4. 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.



L'uso del congelamento di revisioni nel caso di passaggio tra versioni principali non è raccomandato. Dopo che il congelamento viene annullato, possono insorgere problemi durante l'aggiornamento del software antivirus su postazioni.

Per utilizzare le funzionalità degli aggiornamenti differiti



1. Per un prodotto che si vuole congelare impostare gli aggiornamenti differiti come 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 gli aggiornamenti più recenti** nella sezione **Rete antivirus** → [Limitazione degli aggiornamenti delle postazioni](#). Sulle altre postazioni verrà distribuita la revisione che è stata contrassegnata come corrente nel passaggio 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 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 il congelamento

- Nella scheda **Lista delle revisioni** premere  **Esegui subito** per annullare il congelamento 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 il congelamento del prodotto e per vietare questa revisione. Si riprende il processo dell'ottenimento degli aggiornamenti da SAM. La revisione scongelata verrà rimossa dall'elenco delle revisioni del prodotto. Quando arriverà 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](#).

10.11.5. 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 i file nella versione corrente del repository con l'elenco di tutte le revisioni disponibili di ciascun prodotto.

Visualizzazione delle informazioni sul repository

Per visualizzare informazioni sugli oggetti del repository, selezionare un oggetto nell'albero gerarchico dei contenuti del repository. Si apre il pannello delle proprietà con le seguenti informazioni:


- Nella sottosezione **Oggetti selezionati** vengono riportate 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 informazioni generali su tutti gli oggetti del repository: la lista corrente degli oggetti e la data del loro 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 possibilità di recupero.

Esportazione del repository

Per salvare i file del repository in un archivio zip

- Per salvare in archivio l'intero repository nel suo insieme, premere il pulsante  **Esporta i file del repository in archivio** → **Tutti i contenuti del repository** nella barra degli strumenti. In tale caso verrà esportato l'intero repository indipendentemente da quello quale oggetto è selezionato nell'albero gerarchico.



- Per salvare in archivio solo le ultime revisioni di tutti i prodotti, premere il pulsante  **Esporta i file del repository in archivio** → **Le ultime revisioni di tutti i prodotti** nella barra degli strumenti.
- Per salvare in archivio tutti i file di configurazione del repository, premere il pulsante  **Esporta i file del repository in archivio** → **File di configurazione** nella barra degli strumenti. In tale caso verranno esportati tutti i file situati nella directory radice del repository e quelli di tutti i prodotti.
- Per salvare in archivio singoli oggetti del repository, selezionarli nell'albero gerarchico utilizzando i tasti CTRL o MAIUSCOLO e premere il pulsante  **Esporta i file del repository in archivio** → **Oggetti selezionati** nella barra degli strumenti.



Nel caso di una grande quantità di dati il tempo di esportazione può superare la durata della sessione. Se la sessione scade prima del completamento dell'esportazione, il processo di esportazione verrà terminato automaticamente, e l'archivio con i dati di esportazione non verrà generato.

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 oggetti 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 singoli file 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**.

Importazione del repository

Per caricare i file del repository da un archivio zip

1. Premere il pulsante  **Importa archivio con i file del repository** nella barra degli strumenti.
2. Nella finestra che si è aperta nella sezione **Selezione del file** selezionare tramite il pulsante  un archivio zip con i file del repository.



Possono essere importati solo gli archivi zip ottenuti tramite l'esportazione di 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 di importazione** impostare i seguenti parametri:

- **Aggiungi soltanto le revisioni mancanti** — in questa modalità di importazione vengono aggiunte le sole revisioni di 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.

10.11.6. Hash di minacce conosciuti

La sezione **Hash di minacce conosciuti** consente di eseguire la ricerca nel bollettino con gli hash di minacce conosciuti, che è fornito dal centro FinCERT ed è incluso nel prodotto 15-drwhashdb.

Questa sezione è disponibile solo se è stato concesso in licenza l'uso dei bollettini degli hash di minacce conosciuti. La presenza di una licenza è riportata nelle informazioni sulla chiave di licenza che possono essere visualizzate nella sezione [Gestione licenze](#), parametro **Liste consentite dei bollettini di hash** (è sufficiente una licenza in almeno una delle chiavi di licenza utilizzate dal Server Dr.Web).



L'assenza della licenza per i bollettini degli hash non riduce il livello di protezione antivirus. Questa licenza consente di aggiungere un avviso all'amministratore su quello che la minaccia rilevata è presente nei bollettini specializzati degli hash di minacce conosciuti.



Il prodotto 15-drwhashdb viene gestito nella sezione **Amministrazione > Configurazione dettagliata del repository > Hash di minacce conosciuti**.

La tabella della sezione contiene i seguenti dati:

- **Hash di minaccia** — hash di minaccia conosciuto.
- **Nome del bollettino** — FinCERT_IOC.

Per la ricerca per campo della tabella degli hash premere il pulsante



Quando viene rilevata una minaccia su una postazione (da controllo delle applicazioni, protezione preventiva o durante una scansione) e le informazioni su di essa vengono inviate al Server Dr.Web, il server fa il riscontro del suo hash con l'hash nella lista FinCERT, e in caso di corrispondenza, la contrassegna come presente nel bollettino FinCERT. Queste informazioni sono disponibili nelle tabelle delle statistiche con le minacce rilevate se è attivata la visualizzazione della colonna **Bollettino** nella sezione **Rete antivirus > Statistiche**.

Il database con gli hash è conservato nel file unico `hash-db` nella seguente directory:

- in caso di SO Windows: `C:\Program Files\DrWeb Server\var\hash-db\\hash.db`,
- in caso di SO Linux: `/var/opt/drwcs/hash-db/<numero della revisione>/hash.db`,
- in caso di SO FreeBSD: `/var/drwcs/hash-db/<numero della revisione>/hash.db`.

Notifiche sul rilevamento di minacce in base agli hash di minacce conosciuti

È possibile configurare l'invio di notifiche sulle corrispondenze trovate con gli hash di minacce conosciuti nella sezione [Configurazione degli avvisi](#).

Sono disponibili le seguenti notifiche:

- **Controllo delle applicazioni ha bloccato un processo dalla lista degli hash di minacce conosciuti.**
- **È stata rilevata una minaccia alla sicurezza in base agli hash di minacce conosciuti.**
- **Errore di scansione al rilevamento di una minaccia in base agli hash di minacce conosciuti.**
- **Report di Protezione preventiva sul rilevamento di minacce in base agli hash di minacce conosciuti.**

In caso di utilizzo di diversi Server Dr.Web, spuntare il flag **Invia avvisi sugli eventi del Server Dr.Web adiacente al rilevamento di minacce in base agli hash conosciuti** per inviare all'amministratore gli avvisi su eventi ricevuti dal Server Dr.Web subordinato che viene configurato nel caso di rilevamento di minacce alla sicurezza in base agli hash di minacce conosciuti. Se il flag è deselezionato, l'amministratore riceverà avvisi solo sugli eventi sul proprio Server Dr.Web.

Il flag è disponibile solo se l'uso dei bollettini degli hash di minacce conosciuti è concesso in licenza.

È anche possibile configurare le notifiche tramite le [procedure personalizzate](#).



In assenza della licenza del prodotto, le notifiche corrispondenti sono automaticamente disattivate.

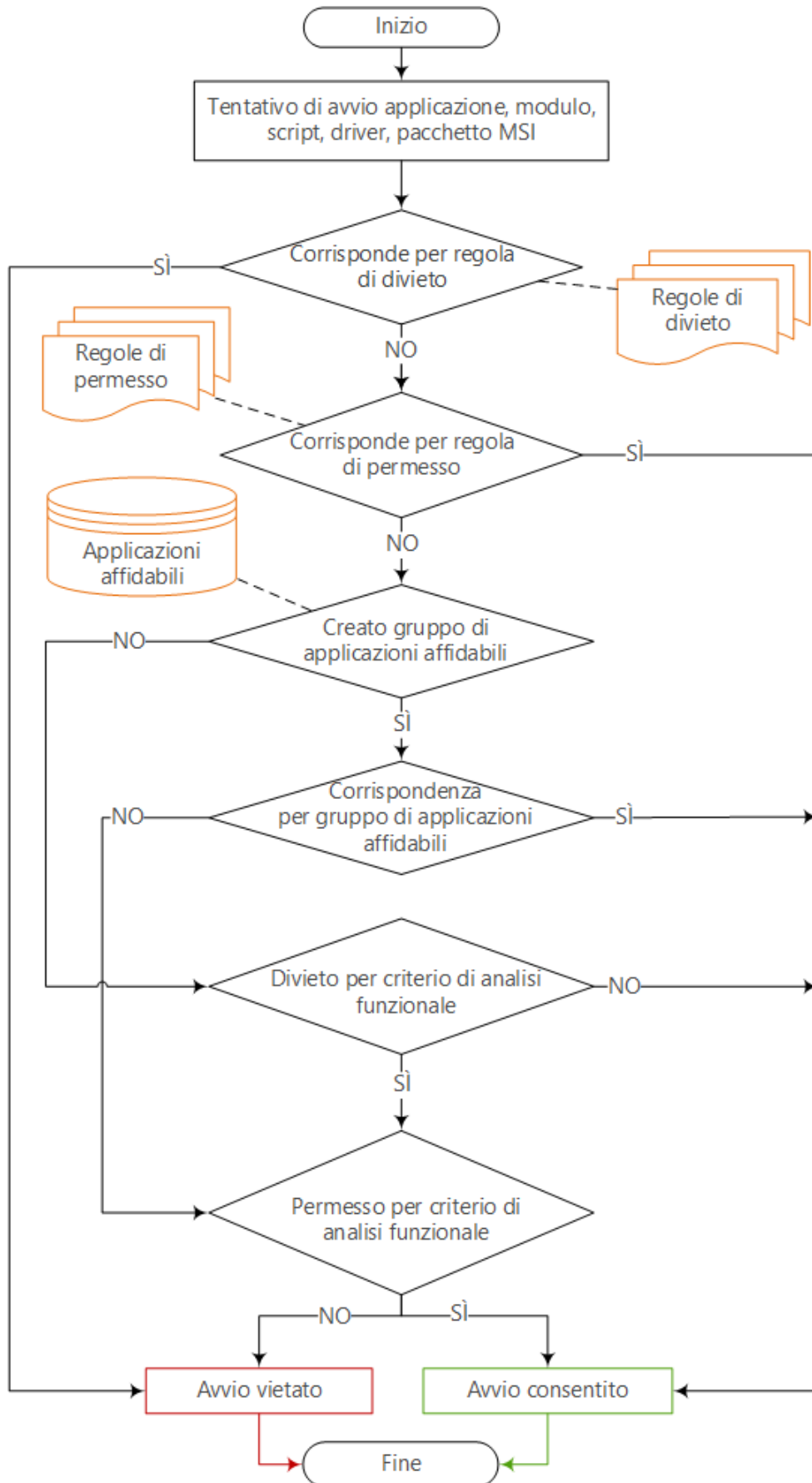


10.12. Controllo delle applicazioni

Tramite il componente Controllo delle applicazioni è possibile consentire o vietare l'avvio di determinate applicazioni, moduli, interpreti di script, driver e pacchetti MSI sulle postazioni protette della rete antivirus su cui è installato Agent Dr.Web per Windows.



Lo schema di funzionamento di Controllo delle applicazioni è riportato di seguito.





I principali strumenti di Controllo delle applicazioni:

- **Profili** — lista di regole che determinano quali applicazioni sulle postazioni possono essere avviate e quali sono proibite. I profili vengono creati dall'amministratore e vengono assegnati a criteri, postazioni e utenti, inclusi gruppi di postazioni e utenti. I profili determinano la **modalità di funzionamento** di Controllo delle applicazioni.
I profili vengono configurati attraverso l'albero della rete nella sezione **Rete antivirus**.
- Le liste delle applicazioni:
 - **Applicazioni affidabili** — lista di applicazioni che viene compilata in base alle regole impostate e viene raccolta su postazioni selezionate per decisione dell'amministratore. Nel caso di funzionamento in **modalità di permesso** l'avvio di queste applicazioni sarà sempre consentito. I gruppi specifici di applicazioni affidabili vengono selezionati nelle impostazioni individualmente per ciascun profilo.
 - **Prontuario applicazioni** — lista di tutte le applicazioni installate sulle postazioni protette. Il prontuario viene generato automaticamente in background e non può essere modificato dall'amministratore.

Le liste delle applicazioni vengono configurate attraverso la sezione **Amministrazione**.

- **Eventi di Controllo delle applicazioni** — informazioni sugli eventi registrati sulle postazioni dal componente Controllo delle applicazioni.

Gli eventi di Controllo delle applicazioni vengono visualizzati attraverso la sezione **Rete antivirus** → **Statistiche**.

Le principali modalità di funzionamento di Controllo delle applicazioni:

- **Analisi funzionale** — un set di regole predefinite in base a cui l'avvio delle applicazioni viene consentito o vietato in base alle funzionalità eseguite.
- **Modalità di permesso** — significa che su tutte le postazioni controllate è consentito solo l'avvio delle applicazioni dalla lista **Applicazioni affidabili** e delle applicazioni che corrispondono alle regole di permesso. Tutte le altre applicazioni vengono bloccate.
- **Modalità di divieto** — significa che su tutte le postazioni controllate è vietato solo l'avvio delle applicazioni che corrispondono alle regole di divieto. Tutte le altre applicazioni vengono consentite.



Le modalità di permesso e di divieto possono essere attivate o disattivate sia entrambe insieme che separatamente.

L'analisi funzionale deve sempre essere attivata. Se tutte le regole di analisi funzionale sono disattivate, il controllo dell'avvio delle applicazioni non viene eseguito.

Per configurare Controllo delle applicazioni

1. [Creare un nuovo profilo](#).



2. [Selezionare postazioni, utenti e gruppi](#) a cui si applicheranno le impostazioni del profilo creato.
3. [Configurare le impostazioni del profilo.](#)




Si consiglia di configurare il funzionamento dei profili in modalità test.


10.12.1. Modalità test

Per accertarsi dell'operatività di un profilo o una regola configurata, è possibile utilizzare la *modalità test* in cui viene simulato il funzionamento di Controllo delle applicazioni. In questa modalità le applicazioni non vengono effettivamente bloccate, ma viene compilato il log delle attività (v. [Eventi di Controllo delle applicazioni](#)) — come se il profilo o la regola funzionassero normalmente. La modalità test è utile per la configurazione di Controllo delle applicazioni da parte dell'amministratore durante il dispiegamento della rete aziendale.

Per attivare la modalità test per un profilo

1. Nella sezione **Generali** delle proprietà del profilo spuntare il flag **Attiva profilo** per iniziare a utilizzare questo profilo (di default è disattivato).
2. Spuntare il flag **Metti il profilo in modalità test globale.**
3. Premere **Salva.**

In modalità test il relativo profilo nel gruppo **Profiles** nell'albero della rete antivirus avrà l'icona . Sulle postazioni cui è assegnato tale profilo le applicazioni avviate non verranno bloccate secondo i criteri di analisi funzionale, impostati nel profilo, le regole di permesso o di divieto. Invece di questo, verranno raccolte le statistiche nella sezione **Rete antivirus** → **Statistiche** → **Eventi di Controllo delle applicazioni**. In questo log vengono visualizzate informazioni dettagliate su ciascuna applicazione avviata, analizzando le quali, è possibile modificare le impostazioni del profilo in base alle proprie esigenze.

Dopo essersi convinti che il profilo testato funzioni come previsto, è necessario trasferirlo dalla modalità test alla modalità di funzionamento attiva. Un profilo attivo ha l'icona  nel gruppo **Profiles** nell'albero della rete antivirus.

Per disattivare la modalità test per un profilo

1. Nella sezione **Generali** delle proprietà del profilo togliere il flag **Metti il profilo in modalità test globale**
2. Premere **Salva.**

La modalità test può anche essere utilizzata per controllare il funzionamento di singole regole di permesso e divieto in un profilo senza trasferire l'intero profilo alla modalità test.




Per attivare la modalità test per una regola di permesso o divieto inclusa in un profilo

1. Nella sezione delle proprietà del profilo **Regole di permesso** o **Regole di divieto** selezionare la regola creata di cui il funzionamento si vuole testare.
2. Nelle impostazioni della regola che si sono aperte spuntare i flag **Attiva regola** e **Metti la regola in modalità test**.
3. Premere **Salva**.

In questa modalità i programmi avviati sulle postazioni *verranno bloccati*, ma solo secondo i criteri di analisi funzionale e quelle regole che non sono state trasferite alla modalità test. Le regole di permesso e divieto in modalità test funzionano in modo simile ai profili in questa modalità: le loro impostazioni non influiscono sul blocco dei programmi, ma il risultato di ciascuna attivazione vengono scritti nel log delle attività nella sezione **Eventi di Controllo delle applicazioni**.



A differenza della modalità test dei profili, la presenza di regole in modalità test non si rispecchia in nessun modo nell'icona del relativo profilo nell'albero della rete antivirus. Un profilo attivo con regole in modalità test avrà l'icona .

Quando si è stati convinti che la regola testata funzioni correttamente, è necessario trasferirla dalla modalità test alla modalità di funzionamento attiva.

Per disattivare la modalità test per una regola di permesso o divieto inclusa in un profilo

1. Nella sezione delle proprietà del profilo **Regole di permesso** o **Regole di divieto** selezionare la regola testata.
2. Nelle impostazioni che si sono aperte togliere il flag **Metti la regola in modalità test**.
3. Premere **Salva**.

10.12.2. Applicazioni affidabili

Gestione delle applicazioni affidabili

Gruppo di applicazioni affidabili o (white list di applicazioni) è una lista di applicazioni raccolte in base a criteri specificati da una postazione selezionata o un gruppo di postazioni. L'avvio di queste applicazioni sarà consentito sulle postazioni della rete antivirus per le quali esse sono aggiunte a un [profilo](#) del componente Controllo delle applicazioni nel caso di funzionamento in [modalità di permesso](#).

La raccolta di informazioni per la formazione di un gruppo di applicazioni affidabili è un processo ad alta intensità di risorse che, a seconda dei criteri impostati, può influire in modo significativo sulle prestazioni del computer in questione. Per ridurre il carico sulle postazioni della rete antivirus, la raccolta di informazioni deve essere eseguita su una o più postazioni *modello* — computer selezionati appositamente per questo obiettivo. Un candidato ideale per



questo ruolo è un computer con un sistema operativo recentemente installato, gli ultimi aggiornamenti e tutti i software necessari per il lavoro.

Per gestire le applicazioni affidabili sui Server Dr.Web che raccolgono informazioni, andare alla sezione **Amministrazione** → **Controllo delle applicazioni** → **Applicazioni affidabili**.

La tabella della sezione contiene la lista di tutti i gruppi di applicazioni affidabili attuali.


Nella barra degli strumenti sono disponibili i seguenti pulsanti di gestione:

 [Crea il gruppo di applicazioni affidabili](#)

 [Riavvia la creazione del gruppo di applicazioni affidabili](#)

 [Rimuovi il gruppo di applicazioni affidabili](#)

Per creare un nuovo gruppo di applicazioni affidabili

1. Nella sezione **Applicazioni affidabili** nella barra degli strumenti premere il pulsante  **Crea il gruppo di applicazioni affidabili**.

2. Nella finestra **Generali** configurare le seguenti impostazioni:

- **Nome del gruppo** — nome del gruppo di applicazioni affidabili che viene creato.
- **Descrizione** — una descrizione arbitraria facoltativa del gruppo che viene creato.

Premere il pulsante **Avanti**.

3. Nella finestra **Parametri di aggiunta di applicazioni a quelle affidabili** configurare le impostazioni in base a cui le applicazioni sulle postazioni verranno aggiunte al gruppo di applicazioni affidabili che viene creato (almeno un'impostazione deve essere selezionata in ciascuna categoria):

Spuntare il flag **Imposta una priorità bassa per il processo di raccolta delle informazioni** se la raccolta di informazioni per il gruppo di applicazioni affidabili che viene creato verrà eseguita su una postazione le cui risorse di sistema non devono essere completamente occupate da questa attività.



L'attivazione di questo parametro può risparmiare le risorse del computer impiegate per la raccolta di informazioni, però la durata dell'esecuzione di questa operazione può aumentare notevolmente.

- **Area di ricerca** — spuntare i flag per le aree per cui verranno raccolte informazioni sulle applicazioni.



Per l'opzione **Cerca per percorso indicato** è possibile impostare diversi percorsi per la ricerca delle applicazioni. Utilizzare ";" come delimitatore.

- **Tipo di hash aggiunti** — spuntare i flag accanto agli oggetti i cui hash verranno scritti nel gruppo di applicazioni affidabili che viene creato.



- **Categorie di file** — spuntare i flag per i file che verranno presi in considerazione durante la ricerca.

Premere il pulsante **Avanti**.

4. Nell'albero della rete selezionare le postazioni e i gruppi di postazioni in cui verranno raccolte informazioni sulle applicazioni da includere nella lista di quelle affidabili. Per selezionare più gruppi e postazioni, utilizzare i tasti CTRL e MAIUSCOLO.

Spuntare il flag **Non includere i gruppi nidificati** per raccogliere informazioni sulle postazioni solo nel gruppo selezionato. Se il flag è tolto, vengono raccolte informazioni su tutte le postazioni nel gruppo selezionato e nei sottogruppi.

5. Premere il pulsante **Salva**.
6. Inizierà la raccolta di informazioni sulle applicazioni sulle postazioni in base alle impostazioni specificate. Il processo può richiedere molto tempo.


Informazioni sullo stato e sull'aggiornamento di un gruppo di applicazioni affidabili possono essere visualizzate:

- nella tabella principale della sezione **Applicazioni affidabili**,
- nelle informazioni aggiuntive sul gruppo che si aprono quando si fa clic sulla riga corrispondente al gruppo nella tabella principale della sezione **Applicazioni affidabili**.




Le informazioni sulle applicazioni vengono raccolte nei limiti della sessione corrente sulla postazione in questione. Se la raccolta di informazioni non è terminata, ma la postazione viene spenta o riavviata, dopo l'accensione l'operazione ricomincerà daccapo. I dati su applicazioni parzialmente raccolti non vengono salvati.

Per avviare l'aggiornamento di un gruppo di applicazioni affidabili

1. Nella sezione **Applicazioni affidabili** nella tabella della sezione spuntare i flag di fronte ai gruppi che si desidera aggiornare.
2. Nella barra degli strumenti premere il pulsante  **Riavvia la creazione del gruppo di applicazioni affidabili**.

Per rimuovere un gruppo di applicazioni affidabili

1. Nella sezione **Applicazioni affidabili** nella tabella della sezione spuntare i flag di fronte ai gruppi che si desidera rimuovere.
2. Nella barra degli strumenti premere il pulsante  **Rimuovi il gruppo di applicazioni affidabili**.
3. Le applicazioni di questo gruppo verranno rimosse dalla lista di quelle il cui avvio è consentito sulle postazioni, e la raccolta delle applicazioni per la lista di applicazioni affidabili secondo i criteri di questo gruppo verrà interrotta.




Non è possibile rimuovere un gruppo di applicazioni affidabili assegnato a profili del Controllo applicazioni.



Quando viene rimosso un gruppo di applicazioni affidabili, una nuova revisione del prodotto **Applicazioni affidabili** viene creata nel repository e viene propagata sui Server Dr.Web adiacenti. In tale caso ciò può interferire con il funzionamento dei profili Controllo applicazioni cui questo gruppo è assegnato sui Server Dr.Web adiacenti.

Per rimuovere le informazioni sulle applicazioni su una postazione specifica dal gruppo di applicazioni affidabili

1. Nella sezione **Applicazioni affidabili** nella tabella della sezione premere la riga con il gruppo di applicazioni da cui si desidera rimuovere le informazioni sulle applicazioni su una postazione.
2. Nella finestra che si è aperta nella tabella delle postazioni spuntare i flag per le postazioni di cui le informazioni sulle applicazioni si desidera rimuovere.
3. Nella barra degli strumenti premere il pulsante  **Rimuovi le postazioni selezionate**.



Quando vengono rimosse tutte le postazioni, verrà rimosso il gruppo di applicazioni affidabili stesso.

Repository di applicazioni affidabili



Quando viene configurata la modalità di permesso per un [profilo](#) di Controllo applicazioni, i gruppi di applicazioni affidabili vengono selezionati dalla lista dei gruppi disponibili nel repository per il prodotto **Applicazioni affidabili**.

Se nella rete antivirus sono utilizzati diversi Server Dr.Web uniti dalla comunicazione tra i server, per facilitare la raccolta di informazioni, è possibile distribuire il carico tra i Server Dr.Web nel seguente modo:

- Su uno dei Server Dr.Web l'amministratore raccoglie informazioni dalle postazioni protette. Le informazioni vengono automaticamente inserite nel repository del Server Dr.Web nel prodotto **Applicazioni affidabili** e distribuite secondo le [impostazioni definite](#) attraverso la comunicazione tra i server.

Informazioni su applicazioni affidabili possono essere raccolte su diversi Server Dr.Web della rete, ma i segmenti della rete appartenenti a questi Server Dr.Web devono essere isolati gli uni dagli altri.

- Gli altri Server Dr.Web ricevono l'aggiornamento del prodotto **Applicazioni affidabili** attraverso la comunicazione tra i server secondo le [impostazioni definite](#). Non è necessario configurare su questi Server Dr.Web la raccolta di informazioni su applicazioni affidabili in quanto nel repository saranno collocate le revisioni del prodotto ricevute dal Server Dr.Web adiacente.



Il prodotto **Applicazioni affidabili** non viene aggiornato da SAM. Questo prodotto può solo essere distribuito tra i Server Dr.Web adiacenti attraverso la comunicazione tra i server.

Prima di iniziare a raccogliere Applicazioni affidabili, determinare quali Server Dr.Web raccoglieranno le informazioni e le invieranno ai Server Dr.Web adiacenti, e quali le riceveranno attraverso la comunicazione tra i server. A seconda di ciò, è necessario configurare le impostazioni corrispondenti su ciascuno dei Server Dr.Web.

Per configurare i Server Dr.Web che raccolgono e inviano applicazioni affidabili

1. Aprire la sezione **Amministrazione**.
2. Andare alla sezione **Configurazione dettagliata del repository** → **Applicazioni affidabili**.
3. Nella scheda **Sincronizzazione** togliere il flag **Vieta il trasferimento degli aggiornamenti ai Server Dr.Web adiacenti** e spuntare il flag **Vieta la ricezione degli aggiornamenti dai Server Dr.Web adiacenti**.
4. Premere **Salva**.
5. Andare alla sezione **Amministrazione** → **Controllo delle applicazioni** → **Applicazioni affidabili** e configurare la raccolta di applicazioni affidabili, come descritto [di seguito](#).
6. Una nuova revisione del prodotto **Applicazioni affidabili** viene scritta nel repository dopo che vengono ricevute informazioni da tutte le postazioni specificate nelle impostazioni di raccolta del gruppo di applicazioni affidabili. Dopo essere scritta nel repository, la revisione del prodotto viene distribuita ai Server Dr.Web adiacenti attraverso la comunicazione tra i server.

Per configurare i Server Dr.Web che ricevono applicazioni affidabili

1. Aprire la sezione **Amministrazione**.
2. Andare alla sezione **Configurazione dettagliata del repository** → **Applicazioni affidabili**.
3. Nella scheda **Sincronizzazione** togliere il flag **Vieta la ricezione degli aggiornamenti dai Server Dr.Web adiacenti**.

Se il Server Dr.Web deve trasferire il prodotto **Applicazioni affidabili** ad altri Server Dr.Web attraverso la comunicazione tra i server, togliere anche il flag **Vieta il trasferimento degli aggiornamenti ai Server Dr.Web adiacenti**.

4. Premere **Salva**.

10.12.3. Prontuario applicazioni

Per visualizzare il prontuario applicazioni, andare alla sezione **Amministrazione** → **Controllo delle applicazioni** → **Prontuario applicazioni**.

Il prontuario applicazioni contiene informazioni sulle applicazioni installate su postazioni protette con SO Windows connesse al Server Dr.Web.



Il prontuario viene generato automaticamente in background e dopo essere stato raccolto non può essere modificato dall'amministratore. Le informazioni su ciascuna applicazione vengono inviate dall'Agent Dr.Web sul Server Dr.Web una volta sola al momento della prima attività di tale applicazione.

Il prontuario può essere utilizzato nei seguenti casi:

- Per ottenere informazioni sulle applicazioni installate sulle postazioni della rete.
- Per creare le regole [di divieto](#) e [di permesso](#). L'uso del prontuario semplifica il processo di creazione delle regole in quanto tutte le informazioni sull'applicazione vengono compilate automaticamente in base ai dati su un'applicazione conosciuta selezionata.

Riempimento del prontuario applicazioni

Per attivare l'invio di informazioni dalle postazioni per il prontuario applicazioni

1. Nella sezione **Rete antivirus** selezionare nell'albero la postazione o il gruppo di postazioni con il Controllo applicazioni installato, da cui si desidera ricevere informazioni sulle applicazioni installate.
2. Nel menu di gestione selezionare la voce **Windows** → **Agent Dr.Web**, se è stato selezionato un gruppo, o **Agent Dr.Web**, se è stata selezionata una postazione.
3. Nella scheda **Generali** spuntare il flag **Monitora eventi di Controllo applicazioni** per monitorare tutta l'attività dei processi sulle postazioni, registrata dal Controllo applicazioni, e inviare gli eventi sul Server Dr.Web. Se la connessione al Server non è disponibile, gli eventi vengono accumulati e inviati quando la connessione viene stabilita. Se il flag è tolto, possono essere inviati solo gli eventi di blocco (a seconda delle impostazioni nella configurazione del Server Dr.Web).
4. Premere **Salva**.

Per attivare la raccolta delle informazioni da parte del Server Dr.Web per il prontuario applicazioni

1. Aprire la sezione **Amministrazione** → **Configurazione del Server Dr.Web**.
2. Andare alla scheda **Statistiche** e impostare una delle seguenti opzioni:
 - **Statistiche di Controllo applicazioni sull'attività dei processi**, per ricevere e registrare informazioni su qualsiasi attività di tutti i processi: sia quelli il cui avvio è consentito che quelli vietati da Controllo applicazioni. Quando questa opzione è selezionata, le applicazioni verranno inserite nel prontuario a condizione che sia stato creato e assegnato almeno un [profilo](#) con una o più categorie selezionate di [criteri di analisi funzionale](#). Fino a quando profili non vengono creati e assegnati a postazioni della rete antivirus, l'avvio di tutte le applicazioni è consentito.
 - **Statistiche di Controllo applicazioni sul blocco dei processi**, per ricevere e registrare informazioni sull'attività di tutti i processi il cui avvio è vietato da Controllo applicazioni.



Quando questa opzione è selezionata, applicazioni verranno inserite nel prontuario solo dopo che vengono creati [profili](#) secondo le cui impostazioni l'avvio delle applicazioni verrà bloccato e vengono assegnati a postazioni della rete antivirus.



Il flag **Statistiche di Controllo applicazioni sull'attività dei processi** può aumentare significativamente l'intensità d'uso delle risorse per la raccolta delle statistiche su tutta la rete antivirus.

3. Premere il pulsante **Salva**.
4. Riavviare il Server Dr.Web.
5. Dopo il riavvio il Server Dr.Web inizierà a registrare le statistiche di avvio applicazioni basate sulle impostazioni specificate, che vengono inviate da tutte le postazioni con il Controllo applicazioni installato.

Creazione delle regole dal prontuario applicazioni

Per creare una nuova regola basata sui dati dal prontuario applicazioni

1. Nella sezione **Prontuario applicazioni** selezionare la riga relativa all'applicazione per cui si desidera creare una regola di controllo dell'avvio.
2. Dopo un click su una riga della tabella si aprirà una finestra con informazioni sull'applicazione selezionata.
3. Premere il pulsante **Crea regola**.
4. Si apre una finestra per la creazione di una nuova regola. Configurare le seguenti impostazioni:
 - a) Dalla lista a cascata **Nome del profilo** selezionare un [profilo](#) di Controllo delle applicazioni in cui verrà creata la regola.
 - b) Nel campo **Nome della regola** specificare un nome per la regola che viene creata.
 - c) Per l'opzione **Tipo di regola** selezionare il tipo di regola creata: quella [di divieto](#) o [di permesso](#).
 - d) Per l'opzione **Modalità di funzionamento** selezionare in quale modalità funzionerà la regola creata (corrisponde al flag **Metti la regola in modalità test** disponibile durante la creazione di una regola da un profilo):

Se si vuole testare la regola, selezionare la modalità **Test**. Le applicazioni non verranno controllate sulle postazioni, tuttavia, la registrazione del log delle attività verrà eseguita come con le impostazioni attivate. I risultati degli avvisi e dei blocchi delle applicazioni in modalità test di funzionamento della regola verranno visualizzati nella sezione [Eventi di Controllo delle applicazioni](#).

In modalità **Attivo** la regola funzionerà in modalità attiva in cui le applicazioni sulle postazioni vengono bloccate in base alle impostazioni della regola specificate (vedi inoltre [modalità di funzionamento dei profili](#)).
 - e) Nella sezione **Proibisci l'avvio di applicazioni secondo i seguenti criteri/Consenti l'avvio di applicazioni secondo i seguenti criteri** (a seconda del tipo di regola



selezionato nel passaggio 4c) i campi verranno automaticamente compilati in conformità all'applicazione sulla base della quale viene creata la regola. Se necessario, è possibile modificare i valori delle impostazioni.

5. Premere **Salva**. La regola verrà creata nel profilo specificato di Controllo applicazioni.

10.13. Funzioni aggiuntive

10.13.1. Gestione del database

La sezione **Gestione del database** permette di gestire direttamente il database con cui interagisce il Server Dr.Web.

La sezione **Generali** contiene i seguenti parametri:

- Il campo **Ultima manutenzione del database** — la data dell'ultima esecuzione dei comandi di gestione 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 Dr.Web (i task corrispondenti del calendario sono descritti nella tabella [Tipi di task e i loro parametri](#)).
 - Il comando **Analisi del database**. È studiato per ottimizzare il database di Server Dr.Web attraverso l'esecuzione del comando `analyze`.
 - Il comando **Pulizia delle postazioni non attivate**. È progettato per rimuovere gli account delle postazioni che sono state create nella rete antivirus, ma non si sono mai connesse al Server Dr.Web. È necessario indicare un periodo dopo cui gli account inutilizzati verranno rimossi.
La lista degli account postazioni non utilizzati può essere visualizzata nella lista gerarchica della rete antivirus, nel gruppo **Status** → **New**.

Per eseguire i comandi di manutenzione 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 Dr.Web.
2. Premere il pulsante **Applica adesso**. Tutti i comandi selezionati verranno eseguiti immediatamente.
Per un'esecuzione automatica differita e/o periodica di questi comandi (eccetto il comando **Analisi del database**) utilizzare lo [Scheduler del Server Dr.Web](#).

Per gestire il database, utilizzare i seguenti pulsanti nella barra degli strumenti:


 [Importazione](#),

 [Esportazione](#).



Esportazione del database

Per salvare le informazioni dal database in file

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 del database che viene ottenuto quando si avvia il file eseguibile di Server Dr.Web dalla riga di comando con l'opzione `modexecdb database-export-xml`. Questo file di esportazione può essere importato quando si avvia il file eseguibile di Server Dr.Web dalla riga di comando con l'opzione `modexecdb database-import`. Una descrizione dettagliata di questi comandi è riportata in documento **Allegati, G3.3. Comandi di gestione del database**.
 - **Esporta le informazioni circa le postazioni e i gruppi** per salvare le informazioni sugli oggetti della rete antivirus in un archivio zip. Come risultato dell'esecuzione di questa operazione, in un file di formato specifico vengono salvate tutte le informazioni sui gruppi di postazioni e sugli account di postazioni stessi della rete antivirus collegata a questo Server Dr.Web. Il file di esportazione include le seguenti informazioni sulle postazioni: proprietà, configurazione dei componenti, permessi, impostazioni delle limitazioni degli aggiornamenti, calendario, lista dei componenti da installare, statistiche, informazioni sulle postazioni rimosse; sui gruppi: proprietà, configurazione dei componenti, permessi, impostazioni delle limitazioni degli 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**.
 - Nell'albero **Rete antivirus** è possibile selezionare uno o più gruppi custom. In questo caso nell'esportazione verranno incluse solo le informazioni sui gruppi selezionati e sulle postazioni per cui i gruppi selezionati sono primari. Se nessun gruppo è selezionato, verranno esportate le informazioni su tutte le postazioni e su tutti i gruppi custom della rete antivirus.
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.



Nel caso di una grande quantità di dati il tempo di esportazione può superare la durata della sessione. Se la sessione scade prima del completamento dell'esportazione, il processo di esportazione verrà terminato automaticamente, e il file con i dati di esportazione non verrà generato.



Importazione del database

La procedura di importazione del file di database contenente informazioni su oggetti della rete antivirus può essere utilizzata per trasferire informazioni sia su un Server Dr.Web nuovo che su un Server Dr.Web già funzionante nella rete antivirus, in particolare, per unire le liste delle postazioni collegate a due Server Dr.Web.



Al Server Dr.Web su cui viene effettuata l'importazione potranno connettersi tutte le postazioni, le informazioni su cui vengono importate. Quando si effettua l'importazione, prestare attenzione alla necessità del numero corrispondente di licenze disponibili per la connessione delle postazioni trasferite. Per esempio, se necessario, nella sezione [Gestione licenze](#) aggiungere una chiave di licenza dal Server Dr.Web da cui sono state trasferite le informazioni sulle postazioni.

Per caricare il database da file

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 solo gli archivi zip che sono stati ottenuti tramite l'esportazione del database per la variante **Esporta le informazioni circa le postazioni e i gruppi**.
3. Premere il pulsante **Importa** per iniziare il processo di importazione.
 4. Se durante l'importazione vengono rilevate postazioni e/o gruppi con identificatori uguali che fanno parte sia dei dati importati che del database del Server Dr.Web corrente, si apre la sezione **Collisioni** per l'impostazione di azioni su 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:

- **Salva i dati dell'importazione per tutti** — per rimuovere tutte le informazioni su oggetti duplicati dal database del Server Dr.Web corrente e sovrascriverle con le informazioni dal database che viene importato. L'azione viene applicata contemporaneamente a tutti gli oggetti duplicati in questa tabella.
- **Salva i dati correnti per tutti** — per salvare tutte le informazioni su oggetti duplicati dal database del Server Dr.Web corrente. Le informazioni su oggetti duplicati dal database che viene importato verranno ignorate. L'azione viene applicata contemporaneamente a tutti gli oggetti duplicati in questa tabella.
- **Seleziona manualmente** — per impostare manualmente un'azione per ciascun oggetto duplicato separatamente. In questa modalità la lista degli oggetti duplicati sarà disponibile per la modifica. Impostare le opzioni di fronte agli oggetti da salvare.

Premere il pulsante **Salva**.



10.13.2. Statistiche di Server Dr.Web

Tramite il Pannello di controllo è possibile visualizzare le statistiche di funzionamento di Server Dr.Web, riguardanti 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** nel 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 di statistiche:
 - **Attività dei client** — informazioni sul numero di client connessi a questo Server Dr.Web: Agent Dr.Web, Server Dr.Web adiacenti e installer di Agent Dr.Web.
 - **Traffico di rete** — parametri del traffico di rete in entrata e uscita durante la comunicazione con il Server Dr.Web.
 - **Utilizzo delle risorse di sistema** — parametri di utilizzo delle risorse di sistema del computer su cui è installato il Server Dr.Web.
 - **Microsoft NAP** — parametri di funzionamento di [NAP Validator](#).
 - **Utilizzo del database** — parametri di utilizzo del database di Server Dr.Web.
 - **Utilizzo della cache di file** — parametri di utilizzo della cache dei file del computer su cui è installato il Server Dr.Web.
 - **Utilizzo della cache DNS** — parametri di utilizzo della cache di richieste a server DNS sul computer su cui è installato il Server Dr.Web.
 - **Avvisi** — parametri di funzionamento del sottosistema che invia [avvisi](#) all'amministratore.
 - **Repository** — parametri di comunicazione del repository di Server Dr.Web con i server SAM.
 - **Statistiche web** — parametri di invio delle statistiche sulle infezioni sui server Doctor Web.
 - **Statistiche del web server** — parametri di utilizzo di Web server.
 - **Cluster** — parametri di comunicazione attraverso il protocollo di sincronizzazione tra i server se viene utilizzato un cluster di Server Dr.Web in una configurazione di rete con diversi server.
 - **Trasmissione degli aggiornamenti multicast** — parametri di comunicazione durante la [trasmissione degli aggiornamenti multicast](#) sulle postazioni attraverso il protocollo multicast.
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 di aggiornamento dei dati, selezionare l'intervallo desiderato nella lista a cascata **Frequenza di aggiornamento** nel pannello di controllo. Il nuovo intervallo verrà applicato automaticamente ai dati numerici e grafici.
8. Quando il puntatore del mouse passa sopra i dati grafici, viene visualizzato il valore numerico del punto selezionato nella forma:
 - **Abs** — 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.

10.13.3. Copie di backup

La sezione **Copie di backup** consente di visualizzare a livello di directory e file, nonché salvare localmente i contenuti delle copie di backup dei dati critici del Server Dr.Web.

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 Dr.Web vengono salvati nei seguenti casi:

- Come risultato dell'esecuzione del task **Backup dei dati critici del Server** secondo il [calendario](#) di Server Dr.Web.
- Come risultato della copiatura di backup eseguita quando si avvia il file eseguibile di Server Dr.Web dalla riga di comando con l'opzione `backup`. Una descrizione dettagliata di questo comando è riportata in documento **Allegati**, [G3.5. Backup dei dati critici del Server Dr.Web](#).

Visualizzazione delle informazioni sulle copie di backup

Per visualizzare le informazioni su una copia di backup, selezionare nell'albero gerarchico l'oggetto relativo alla copia di backup richiesta. Le copie di backup sono collocate nell'albero secondo le directory di conservazione:

- per Server Dr.Web per SO Linux — `/var/opt/drwcs/backup`,



- per Server Dr.Web per SO FreeBSD — `/var/drwcs/backup`,
- per Server Dr.Web per SO Windows — `C:\DrWeb Backup`,
- e tutti i percorsi di salvataggio dei backup indicati nei task del calendario di Server Dr.Web.

Se nei task di Server Dr.Web per SO Windows è indicato un percorso vuoto, di default verrà utilizzata la directory `C:\Program Files\DrWeb Server\var\backup`. Sarà possibile visualizzare le informazioni solo per le copie di backup che sono conservate all'interno delle directory di Server Dr.Web.





Se si modifica la directory per il salvataggio del backup in un task già creato, la directory creata in precedenza non verrà visualizzata nell'interfaccia web. In questo caso, per la nuova directory sarà necessario creare un nuovo task.


Alla selezione di directory e file di backup, si apre il pannello delle proprietà con informazioni sull'oggetto: **Tipo**, **Dimensione** (solo per file separati), **Data di creazione** e **Data di modifica**.

Gestione delle copie di backup

Per gestire le copie di backup, utilizzare i seguenti pulsanti nella barra degli strumenti:

 **Esporta** — per salvare una copia di backup dell'oggetto selezionato sul computer su cui è aperto il Pannello di controllo.

 **Backup** — per creare una copia di backup dei dati critici del Server Dr.Web.

 **Rimuovi gli oggetti selezionati** — per rimuovere gli oggetti selezionati nell'albero, senza possibilità di recupero.

Esportazione di una copia di backup

Per salvare localmente una copia di backup

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.

Copiatura di backup

Per creare una copia di backup dei dati critici del Server Dr.Web, 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 Dr.Web dalla riga di comando con l'opzione `backup`.

Una descrizione dettagliata di questo comando è riportata in documento **Allegati**, [G3.5. Backup dei dati critici del Server Dr.Web](#).

10.13.4. Utility



La lista delle utility disponibili dipende dalle impostazioni del repository di Server Dr.Web. Per attivare o disattivare la ricezione degli aggiornamenti da SAM per le utility disponibili in questa sezione, andare alla sezione **Amministrazione** → **Configurazione generale del repository** → **Pacchetti di installazione Dr.Web** → [Utility di amministrazione Dr.Web](#).

Nella sezione **Utility** è possibile caricare le utility aggiuntive per l'utilizzo di Dr.Web Enterprise Security Suite:

- [Loader di repository Dr.Web](#)

Si usa per scaricare i prodotti Dr.Web Enterprise Security Suite dal Sistema di aggiornamento mondiale. La versione grafica di Loader di repository Dr.Web è disponibile solo in SO Windows.

- **Utility Dr.Web per la raccolta di informazioni sul sistema**

L'utility è progettata per generare un report sullo stato del sistema e di tutti i programmi installati, incluse le soluzioni antivirus Dr.Web per le postazioni protette e il software Server Dr.Web. L'archivio del report può essere utilizzato da parte dell'amministratore della rete antivirus per la diagnostica, nonché per essere fornito al servizio di supporto tecnico dell'azienda Doctor Web.

- **Utility di generazione delle chiavi e dei certificati digitali**

Consente di generare chiavi di crittografia e certificati digitali, e inoltre, di effettuare e verificare la firma digitale dei file. È uno strumento importante per fornire la sicurezza delle connessioni tra i componenti della rete antivirus.



- **Utility di diagnostica remota del Server Dr.Web**

Consente di connettersi al Server Dr.Web su remoto per effettuare la gestione di base e visualizzare le statistiche di funzionamento. La versione grafica dell'utility è disponibile solo per SO Windows. V. inoltre p. [Accesso remoto al Server Dr.Web](#).

- **Utility di diagnostica remota di Server Dr.Web per l'uso degli script**

Consente di connettersi al Server Dr.Web su remoto per effettuare la gestione di base e visualizzare le statistiche di funzionamento. Questa versione dell'utility è adattata per l'uso negli script. V. inoltre p. [Accesso remoto al Server Dr.Web](#).

- **Utility di rimozione di Dr.Web per Windows**

Strumento di emergenza per rimuovere installazioni errate/danneggiate dei software Agent Dr.Web per Windows nei casi quando l'uso di strumenti di rimozione standard non è disponibile o non funziona. L'utility non è destinata a essere utilizzata come strumento standard principale di disinstallazione del software Dr.Web.

- **Utility per l'installazione remota di Agent Dr.Web per UNIX**

L'utility è progettata per l'installazione remota di Agent Dr.Web su postazioni con i sistemi operativi della famiglia UNIX.

- **Utility per l'installazione remota di Agent Dr.Web per Windows**

L'utility è progettata per l'installazione remota di Agent Dr.Web su postazioni con il sistema operativo Windows.

- **Pannello di controllo mobile Dr.Web**

Si usa per gestire una rete antivirus costruita sulla base di Dr.Web Enterprise Security Suite. È progettato per l'installazione e l'avvio sui dispositivi mobili con iOS e SO Android.



Per informazioni sulle opzioni della riga di comando per l'uso delle utility, consultare documento **Allegati**, sezione **G7. Utility**.

10.13.5. Prodotti aziendali



La lista dei prodotti disponibili nella sezione dipende dalle impostazioni del repository di Server Dr.Web. Per attivare o disattivare la ricezione degli aggiornamenti da SAM per determinati prodotti, andare alla sezione **Amministrazione** → **Configurazione generale del repository** → **Pacchetti di installazione Dr.Web** → [Prodotti aziendali Dr.Web](#).



Nella sezione **Prodotti aziendali** è possibile scaricare i pacchetti di installazione di una serie di programmi utilizzati nella rete antivirus Dr.Web Enterprise Security Suite:

- **Dr.Web per Android**

Pacchetto per installare Agent Dr.Web per Android sulle postazioni protette.

- **Dr.Web per IBM Lotus Domino**

Pacchetto per installare Dr.Web per IBM Lotus Domino sul server di posta aziendale.

- **Dr.Web per Linux**

Pacchetto per installare Agent Dr.Web per Linux sulle postazioni protette.

- **Dr.Web per macOS**

Pacchetto per installare Agent Dr.Web per macOS sulle postazioni protette.

- **Dr.Web per Microsoft Exchange Server**

Pacchetto per installare Dr.Web per Microsoft Exchange Server sul server di posta aziendale.

- **Dr.Web per Internet gateway UNIX**

Pacchetto per installare Dr.Web per gateway Internet UNIX sul gateway Internet o server proxy aziendale.

- **Dr.Web per mail server UNIX**

Pacchetto per installare Dr.Web per mail server UNIX sul server di posta aziendale.

- **Dr.Web per file server UNIX**

Pacchetto per installare Dr.Web per file server UNIX sul server di file aziendale.

- **Server proxy Dr.Web**

Pacchetto per installare Server proxy Dr.Web su un computer incluso nella rete antivirus aziendale che viene utilizzato come server proxy.

- **Server di scansione Dr.Web**

Pacchetto per installare Server di scansione Dr.Web progettato per l'elaborazione delle richieste di scansione antivirus provenienti dalle macchine virtuali negli ambienti virtuali.



- **Dr.Web NAP Validator**

Pacchetto per installare Dr.Web NAP Validator su un computer incluso nella rete antivirus aziendale che viene utilizzato come server di protezione dell'accesso alla rete.

- **Agent Dr.Web per Active Directory**

Strumento per installare Agent Dr.Web con l'utilizzo del servizio Active Directory.

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

Pacchetto per installare contemporaneamente Agent Dr.Web per Windows e il pacchetto antivirus sulle postazioni protette.

- **Utility per la modifica degli attributi degli oggetti Active Directory**

Strumento per modificare gli attributi degli oggetti per l'autenticazione con l'utilizzo del servizio Active Directory.

- **Utility per la modifica dello schema Active Directory**

Strumento per creare una nuova classe di oggetti e descriverne gli attributi per l'autenticazione con l'utilizzo del servizio Active Directory.

10.14. Caratteristiche di una rete con diversi Server Dr.Web

Dr.Web Enterprise Security Suite consente di creare una rete antivirus con diversi Server Dr.Web. In questo caso, ciascuna postazione viene registrata su uno specifico Server Dr.Web, il che consente di distribuire il carico tra di essi.

Le relazioni tra i Server Dr.Web possono avere una struttura gerarchica, il che consente di distribuire in modo ottimale il carico sui Server Dr.Web.

Per lo scambio di informazioni tra i Server Dr.Web viene utilizzato uno specifico *protocollo di sincronizzazione tra i server*.

Possibilità fornite dal protocollo di sincronizzazione tra i server:

- Distribuzione degli aggiornamenti tra i Server Dr.Web all'interno della rete antivirus.
- Trasferimento veloce degli aggiornamenti ricevuti dai server SAM Dr.Web.
- Trasferimento tra i Server Dr.Web associati delle informazioni statistiche sullo stato delle postazioni protette.
- Trasferimento delle licenze per postazioni protette tra i Server Dr.Web adiacenti.



10.14.1. 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 Dr.Web. Ogni Server Dr.Web insieme alle postazioni antivirus connesse funziona come una rete antivirus separata, come descritto nelle sezioni precedenti.

Dr.Web Enterprise Security Suite permette di collegare 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 sugli eventi di virus, statistiche di operazione ecc.;
- licenze per postazioni protette (il trasferimento di licenze tra Server Dr.Web viene configurato in [Gestione licenze](#)).

Dr.Web Enterprise Security Suite distingue due tipi di relazione tra i Server Dr.Web:

- *tipo di relazione server principale-subordinato* con cui il server principale trasmette aggiornamenti su quello subordinato e riceve da esso informazioni su eventi,
- *relazione tra server paritari* con cui le direzioni di trasmissione di informazioni e i tipi di informazione vengono configurati in maniera individuale.

In [immagine 10-1](#) è presentato un esempio di struttura di una rete con diversi Server Dr.Web.

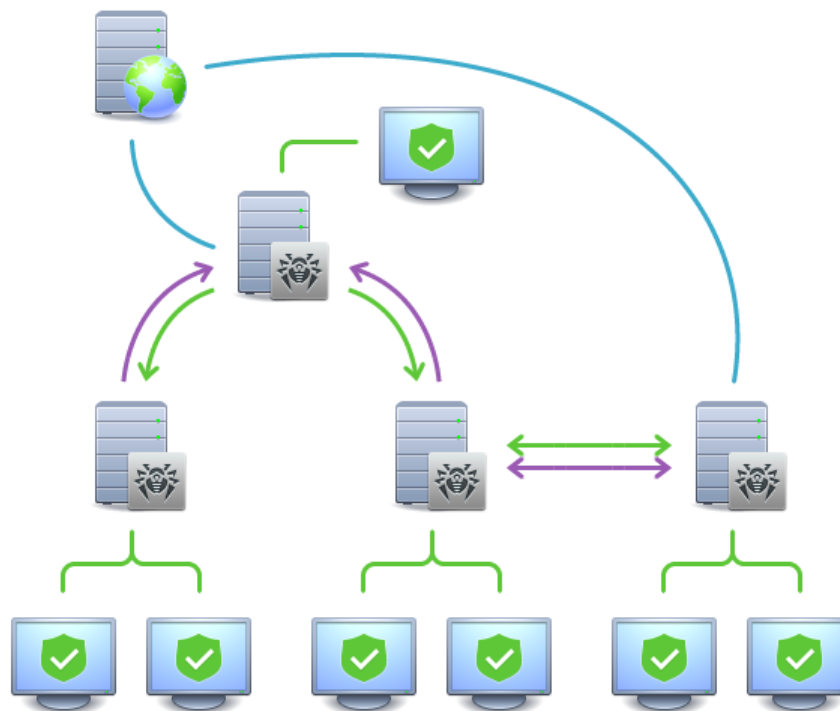


Immagine 10-1. Rete con diversi Server Dr.Web

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 Dr.Web direttamente o attraverso collegamenti intermedi.



I Server Dr.Web che ricevono aggiornamenti da un Server Dr.Web superiore non ricevono aggiornamenti da SAM, anche se tale task è presente nel calendario.



Tuttavia, per il caso in cui il Server Dr.Web principale sia temporaneamente non disponibile, si consiglia di lasciare nel calendario del Server Dr.Web subordinato il task di aggiornamento dai server SAM. Questo consentirà agli Agent Dr.Web connessi al Server Dr.Web subordinato di ricevere aggiornamenti dei database dei virus e dei moduli software (v. inoltre [Configurazione generale del repository](#)).



Nel task di aggiornamento da SAM sul Server Dr.Web principale che distribuisce aggiornamenti è necessario configurare la ricezione degli aggiornamenti del software server per tutti i sistemi operativi installati su tutti i Server Dr.Web subordinati che ricevono aggiornamenti da questo Server Dr.Web principale (v. p. [Configurazione generale del repository](#)).

2. Possibilità di distribuire le postazioni tra diversi Server Dr.Web riducendo il carico su ognuno di essi.
3. Unione delle informazioni da diversi Server Dr.Web su uno di essi; possibilità di ottenerle in forma consolidata in una sessione del Pannello di controllo su questo Server Dr.Web.



Dr.Web Enterprise Security Suite traccia e blocca autonomamente percorsi ciclici di trasmissione delle informazioni.

4. Possibilità di trasferire licenze disponibili per la protezione di postazioni su un Server Dr.Web adiacente. In questo caso, la chiave di licenza stessa rimane a disposizione del Server Dr.Web che la distribuisce, le licenze disponibili vengono rilasciate al Server Dr.Web adiacente per un determinato periodo di tempo, scaduto il quale vengono revocate.

10.14.2. Configurazione delle relazioni tra i Server Dr.Web

Per approfittare delle possibilità di utilizzo di diversi Server Dr.Web, è necessario configurare le relazioni tra di essi.

Si consiglia di progettare prima la struttura della rete antivirus indicando tutti i flussi di informazione attesi e prendendo la decisione quali relazioni saranno di tipo "tra i paritari" e quali di tipo "principale-subordinato". Quindi per ciascun Server Dr.Web che fa parte della rete antivirus è necessario configurare le relazioni con i Server Dr.Web "adiacenti" (i Server Dr.Web "adiacenti" sono collegati da almeno un flusso di informazione).

Se ci sono relazioni inter-server tra i Server Dr.Web, per il nome utente amministratore al menu principale vengono aggiunte [nuove funzionalità](#).

Un esempio della configurazione della comunicazione dei Server Dr.Web principale e subordinato:



I valori dei campi contrassegnati con il carattere * sono da impostare.




1. Assicurarsi che tutti e due Server Dr.Web funzionino normalmente.
2. Dare un nome "parlante" a ciascuno dei Server Dr.Web in quanto questo aiuterà a non commettere errori durante la configurazione della connessione dei Server Dr.Web e la successiva gestione. Si può farlo nel menu del Pannello di controllo **Amministrazione** → **Configurazione del Server Dr.Web** nella scheda **Generali** nel campo **Nome**. In questo esempio chiamiamo il Server Dr.Web principale `MAIN` e quello subordinato — `AUXILIARY`.







I nomi indicati durante la configurazione verranno automaticamente sostituiti con i nomi dei computer dopo la connessione dei Server Dr.Web in base alla relazione creata.

3. Su entrambi i Server Dr.Web attivare 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. [Moduli](#)).
4. Riavviare entrambi i Server Dr.Web.
5. Attraverso il Pannello di controllo del Server Dr.Web subordinato (`AUXILIARY`) aggiungere il Server Dr.Web principale (`MAIN`) alla lista dei Server Dr.Web adiacenti.

Per farlo, selezionare la voce **Rete antivirus** nel menu principale. Si apre una finestra contenente la lista gerarchica della rete antivirus. Per aggiungere un Server Dr.Web adiacente, nella barra degli strumenti selezionare **+ Aggiungi oggetto della rete** →  **Crea relazione**.


Si apre la finestra di configurazione della relazione tra il Server Dr.Web corrente e quello che viene aggiunto. Impostare i seguenti parametri:

- **Tipo** di relazione che viene creata — **Principale**.
- **Nome** — nome del Server Dr.Web principale (`MAIN`).
- **Password*** — password arbitraria per l'accesso al Server Dr.Web principale.
- **Certificati propri del Server Dr.Web** — lista dei certificati SSL del Server Dr.Web che viene configurato. Premere il pulsante  e selezionare il file di certificato `drwcsd-certificate.pem` che corrisponde al Server Dr.Web corrente. Per aggiungere un altro certificato, premere  e aggiungere un certificato al nuovo campo.
- **Certificati del Server Dr.Web adiacente*** — lista dei certificati SSL del Server Dr.Web principale che viene connesso. Premere il pulsante  e selezionare il file di certificato `drwcsd-certificate.pem` che corrisponde al Server Dr.Web principale. Per aggiungere un altro certificato, premere  e aggiungere un certificato al nuovo campo.
- **Indirizzo*** — indirizzo di rete del Server Dr.Web principale e la porta per la connessione. Viene impostato nel formato `<indirizzo_di_Server_Dr.Web> : <porta>`.

È possibile la ricerca della lista dei Server Dr.Web disponibili nella rete. A questo scopo:

- 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 Dr.Web disponibili.
- d) Selezionare un Server Dr.Web nella lista dei Server Dr.Web disponibili. Il suo indirizzo verrà scritto nel campo **Indirizzo** per la creazione della relazione.
- **Indirizzo del Pannello di controllo della sicurezza Dr.Web** — può essere indicato l'indirizzo della pagina iniziale del Pannello di controllo del Server Dr.Web principale (v. [Pannello di controllo della sicurezza Dr.Web](#)).
 - Nella lista a cascata **Parametri di connessione** viene impostato il principio di connessione dei Server Dr.Web della relazione che viene creata.
 - Nelle liste a cascata **Crittografia** e **Compressione** impostare i parametri di cifratura e di compressione del traffico dati tra i Server Dr.Web che vengono collegati (v. [Cifratura e compressione del traffico dati](#)).
 - **Periodo di rinnovo automatico delle licenze rilasciate** — periodo di tempo per cui vengono rilasciate le licenze dalla chiave su questo Server Dr.Web. Dopo la fine di questo periodo viene eseguito il rinnovo automatico delle licenze rilasciate per lo stesso periodo. Il rinnovo automatico verrà eseguito fino a quando durerà il periodo di distribuzione della licenza. L'impostazione viene utilizzata se il Server Dr.Web principale rilascerà licenze al Server Dr.Web corrente.
 - **Intervallo per il rinnovo preliminare delle licenze ricevute** — l'impostazione non viene utilizzata se viene creata una relazione al Server Dr.Web principale.
 - **Periodo di sincronizzazione delle licenze** — periodicità di sincronizzazione delle informazioni sulle licenze rilasciate tra i Server Dr.Web.
 - I flag nelle sezioni **Licenze**, **Aggiornamenti** e **Eventi** sono spuntati in conformità al principio di relazione *principale-subordinato* e non possono essere modificati:
 - il Server Dr.Web principale invia licenze sul Server Dr.Web subordinato;
 - il Server Dr.Web principale invia aggiornamenti sul Server Dr.Web subordinato;
 - il Server Dr.Web principale accetta informazioni su eventi dal Server Dr.Web subordinato.
 - Configurare la ricezione degli avvisi da parte dell'amministratore:
 - Spuntare il flag **Invia avvisi sugli eventi del Server Dr.Web adiacente** per inviare all'amministratore avvisi sugli eventi ricevuti dal Server Dr.Web subordinato che viene configurato. Se il flag è deselezionato, l'amministratore riceverà avvisi solo sugli eventi sul proprio Server Dr.Web. Può essere configurato l'invio di avvisi specifici nella sezione [Configurazione degli avvisi](#).
 - Spuntare il flag **Invia avvisi sugli eventi del Server Dr.Web adiacente al rilevamento di minacce in base agli hash conosciuti** per inviare all'amministratore avvisi sugli eventi ricevuti dal Server Dr.Web subordinato che viene configurato nel caso di rilevamento di minacce alla sicurezza in base agli hash di minacce conosciuti. Se il flag è deselezionato, l'amministratore riceverà avvisi solo sugli eventi sul proprio Server Dr.Web. Può essere configurato l'invio di avvisi specifici nella sezione [Configurazione degli avvisi](#).
Il flag è disponibile solo se è stato concesso in licenza l'uso dei bollettini degli hash di minacce conosciuti. La presenza di una licenza è riportata nelle informazioni sulla



chiave di licenza che possono essere visualizzate nella sezione [Gestione licenze](#), parametro **Liste consentite dei bollettini di hash** (è sufficiente una licenza in almeno una delle chiavi di licenza utilizzate dal Server Dr.Web).

- Spuntare il flag **Sincronizza le informazioni sugli hardware e sui programmi sulle postazioni attraverso le comunicazioni interserver** per inviare sul Server Dr.Web subordinato che viene configurato i dati raccolti sugli hardware, i software e i pacchetti di aggiornamento del sistema operativo Windows installati sulle postazioni connesse. I dati verranno inviati immediatamente dopo la creazione della relazione e la connessione al Server Dr.Web principale e in seguito verranno aggiornati in caso di modifiche all'hardware e al software delle postazioni. Queste statistiche vengono raccolte solo dalle postazioni su cui è installato Agent Dr.Web per Windows e solo a condizione che l'opzione corrispondente sia attivata nella configurazione di Server Dr.Web e di Agent Dr.Web, come descritto nella sezione [Hardware e software sulle postazioni SO Windows](#).



Con queste opzioni attivate, è possibile un aumento significativo del numero di avvisi ricevuti.

Nel caso di configurazione di Server Dr.Web paritari queste opzioni saranno disponibili solo se è spuntato il flag **Ricevi** nella sezione **Eventi**.

Sono disponibili i seguenti avvisi sugli eventi sul Server Dr.Web adiacente: **È stata rilevata una minaccia alla sicurezza, Report di protezione preventiva, Errore di scansione, Statistiche di scansione.**

Sono forniti avvisi separati sugli eventi sul Server Dr.Web adiacente nel caso di rilevamento di minacce alla sicurezza in base agli hash di minacce conosciuti: **È stata rilevata una minaccia alla sicurezza in base agli hash di minacce conosciuti, Errore di scansione al rilevamento di una minaccia in base agli hash di minacce conosciuti, Report di Protezione preventiva sul rilevamento di minacce in base agli hash di minacce conosciuti.**

- Nella sezione **Limitazioni di aggiornamento** → **Eventi** è possibile impostare un calendario di trasmissione degli eventi dal Server Dr.Web corrente a quello principale (la modifica della tabella **Limitazioni di aggiornamento** viene effettuata allo stesso modo della modifica della tabella di calendario nella sezione [Limitazione degli aggiornamenti delle postazioni](#)).

Premere il pulsante **Salva**.

Come risultato, il Server Dr.Web principale (MAIN) viene incluso nelle cartelle **Parents** e **Offline** (v. [immagine 10-2](#)).

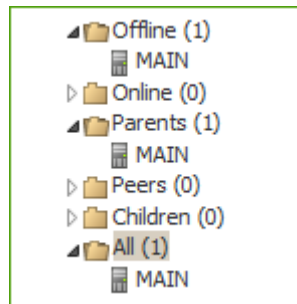


Immagine 10-2.

6. Aprire il Pannello di controllo del Server Dr.Web principale (MAIN) e aggiungere il Server Dr.Web subordinato (AUXILIARY) alla lista dei Server Dr.Web adiacenti.

Per farlo, selezionare la voce **Rete antivirus** nel menu principale. Si apre una finestra contenente la lista gerarchica della rete antivirus. Per aggiungere un Server Dr.Web adiacente, nella barra degli strumenti selezionare **+ Aggiungi oggetto della rete** → **Crea relazione**.

Si apre la finestra di configurazione della relazione tra il Server Dr.Web corrente e quello che viene aggiunto. Impostare i seguenti parametri:

- **Tipo** di relazione che viene creata — **Subordinato**.
- **Nome** — nome del Server Dr.Web subordinato (AUXILIARY).
- **Password*** — inserire la stessa password che è stata indicata nella voce **5**.
- **Certificati propri del Server Dr.Web** — lista dei certificati SSL del Server Dr.Web che viene configurato. Premere il pulsante e selezionare il file di certificato `drwcsd-certificate.pem` che corrisponde al Server Dr.Web corrente. Per aggiungere un altro certificato, premere e aggiungere un certificato al nuovo campo.
- **Certificati del Server Dr.Web adiacente*** — lista dei certificati SSL del Server Dr.Web subordinato che viene connesso. Premere il pulsante e selezionare il file di certificato `drwcsd-certificate.pem` che corrisponde al Server Dr.Web subordinato. Per aggiungere un altro certificato, premere e aggiungere un certificato al nuovo campo.
- **Indirizzo del Pannello di controllo della sicurezza Dr.Web** — può essere indicato l'indirizzo della pagina iniziale del Pannello di controllo del Server Dr.Web subordinato (v. [Pannello di controllo della sicurezza Dr.Web](#)).
- Nella lista a cascata **Parametri di connessione** viene impostato il principio di connessione dei Server Dr.Web della relazione che viene creata.
- Nelle liste a cascata **Crittografia** e **Compressione** impostare i parametri di cifratura e di compressione del traffico dati tra i Server Dr.Web che vengono collegati (v. [Cifratura e compressione del traffico dati](#)).
- **Periodo di rinnovo automatico delle licenze rilasciate** — l'impostazione non viene utilizzata se viene creata una relazione al Server Dr.Web subordinato.
- **Intervallo per il rinnovo preliminare delle licenze ricevute** — intervallo di tempo prima della fine del periodo di rinnovo automatico delle licenze, a partire da cui questo Server Dr.Web subordinato richiede il rinnovo automatico preliminare di queste licenze.



L'impostazione viene utilizzata se il Server Dr.Web subordinato riceverà licenze dal Server Dr.Web corrente.

- **Periodo di sincronizzazione delle licenze** — l'impostazione non viene utilizzata se viene creata una relazione al Server Dr.Web subordinato.
- I flag nelle sezioni **Licenze**, **Aggiornamenti** e **Eventi** sono spuntati in conformità al principio di relazione *principale-subordinato* e non possono essere modificati:
 - il Server Dr.Web subordinato accetta licenze dal Server Dr.Web principale;
 - il Server Dr.Web subordinato accetta aggiornamenti dal Server Dr.Web principale;
 - il Server Dr.Web subordinato invia informazioni su eventi sul Server Dr.Web principale.
- Le opzioni **Invia avvisi sugli eventi del Server Dr.Web adiacente**, **Invia avvisi sugli eventi del Server Dr.Web adiacente al rilevamento di minacce in base agli hash conosciuti** e **Sincronizza le informazioni sugli hardware e sui programmi sulle postazioni attraverso le comunicazioni interserver** sono disattivate e non sono modificabili in quanto il Server Dr.Web subordinato non riceve eventi dal Server Dr.Web principale.
- Nella sezione **Limitazioni di aggiornamento** → **Aggiornamenti** è possibile impostare un calendario di trasmissione degli aggiornamenti dal Server Dr.Web corrente a quello subordinato (la modifica della tabella **Limitazioni di aggiornamento** viene effettuata allo stesso modo della modifica della tabella di calendario nella sezione [Limitazione degli aggiornamenti delle postazioni](#)).

Premere il pulsante **Salva**.

Come risultato, il Server Dr.Web subordinato (AUXILIARY) viene incluso nelle cartelle **Children** e **Offline** (v. [immagine 10-3](#)).

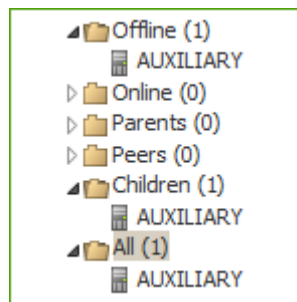


Immagine 10-3.

7. Attendere che venga stabilita una connessione tra i Server Dr.Web (di solito ci vuole non più di un minuto). Per controllare, aggiornare periodicamente la lista dei Server Dr.Web tramite il tasto F5. Dopo che la connessione è stata stabilita, il Server Dr.Web subordinato (AUXILIARY) viene trasferito dalla cartella **Offline** nella cartella **Online** (v. [immagine 10-4](#)).

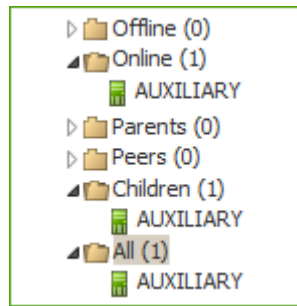


Immagine 10-4.

8. Aprire il Pannello di controllo del Server Dr.Web subordinato (AUXILIARY) e assicurarsi che il Server Dr.Web principale (MAIN) sia connesso a quello subordinato (AUXILIARY) (v. [immagine 10-5](#)).

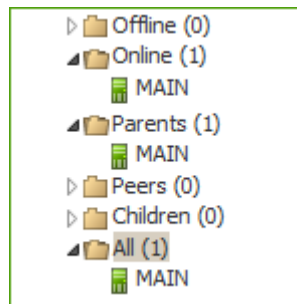


Immagine 10-5.



Non è possibile collegare più Server Dr.Web con una stessa coppia di parametri: password e certificato SSL.



Quando viene creata una relazione paritaria tra Server Dr.Web, si consiglia di indicare l'indirizzo del Server Dr.Web che viene connesso solo nelle impostazioni di uno di essi. Ciò non influirà sull'interazione tra i Server Dr.Web, però consentirà di evitare record di tipo **Link with the same key id is already activated** nel log di funzionamento dei Server Dr.Web.

Tuttavia, è obbligatorio impostare l'indirizzo del Server Dr.Web che viene connesso su uno dei lati.

Non è possibile stabilire una connessione tra i Server Dr.Web nei seguenti casi:

- Problemi di connessioni di rete.
- Durante la configurazione della relazione è stato impostato un indirizzo di Server Dr.Web principale errato.
- Sono stati impostati certificati pubblici non validi su uno dei Server Dr.Web.
- Una password di accesso non valida è stata impostata su uno dei Server Dr.Web (password non corrispondenti sono state impostate sui Server Dr.Web che vengono connessi).



Se è necessario stabilire una nuova relazione inter-server tra Server Dr.Web versione 10 e 13, eseguire in aggiunta le seguenti azioni:

1. Durante la creazione della relazione indicare la chiave pubblica del Server Dr.Web versione 13 sul Server Dr.Web versione 10.
2. Generare un certificato dalla chiave privata del Server Dr.Web versione 10 tramite l'utility `drwsign` (comando `gencert`) inclusa nel Server Dr.Web versione 13 (v. documento **Allegati**, [H7.1. Utility di generazione delle chiavi e dei certificati digitali](#)). Indicare questo certificato durante la creazione della relazione sul Server Dr.Web versione 13.

10.14.3. Utilizzo di una rete antivirus con diversi Server Dr.Web

Una caratteristica della rete con diversi Server Dr.Web è la ricezione di aggiornamenti dai server SAM Dr.Web attraverso una parte dei Server Dr.Web (di regola, uno o più Server Dr.Web principali). In questo caso solo su questi Server Dr.Web è necessario impostare un calendario contenente il task di aggiornamento (v. p. [Configurazione del calendario di Server Dr.Web](#)). Qualsiasi Server Dr.Web che abbia ottenuto un aggiornamento dai server SAM Dr.Web o da un altro Server Dr.Web lo trasmette immediatamente a tutti i Server Dr.Web per cui su di esso è configurata tale possibilità (cioè su tutti i Server Dr.Web collegati subordinati, nonché su quelli dei Server Dr.Web paritari per cui la possibilità di ricezione di aggiornamenti è impostata in modo esplicito).



Dr.Web Enterprise Security Suite automaticamente tiene traccia delle situazioni in cui, per una pianificazione della topologia rete e una configurazione Server Dr.Web imperfette, un aggiornamento già accettato da un'altra fonte arriva di nuovo sullo stesso Server Dr.Web, e tale aggiornamento non viene eseguito di nuovo.

L'amministratore può inoltre ottenere informazioni di riepilogo sugli eventi di virus più importanti nei segmenti della rete associati a uno specifico Server Dr.Web attraverso le relazioni tra i server.

Per visualizzare informazioni sugli eventi di virus su tutti i Server Dr.Web associati a questo Server

1. Selezionare la voce **Rete antivirus** nel menu principale del Pannello di controllo. Nell'albero della rete antivirus nel gruppo **Neighbors** selezionare il Server Dr.Web adiacente di cui le informazioni si vogliono visualizzare.
2. Selezionare nel menu di gestione la voce **Generali** → **Hardware e software** per visualizzare le statistiche sugli hardware e sui software sulle postazioni protette connesse al Server Dr.Web adiacente selezionato.

Le informazioni fornite in questa sezione sono analoghe alle informazioni nella sezione per le postazioni connesse al Server Dr.Web corrente (v. [Hardware e software sulle postazioni SO Windows](#)).



- Per visualizzare le statistiche di funzionamento dei componenti antivirus sulle postazioni protette connesse al Server Dr.Web adiacente selezionato, selezionare la voce corrispondente nella sezione del menu di gestione **Statistiche**.

Le informazioni fornite in questa sezione sono analoghe alle informazioni nella sezione per le postazioni connesse al Server Dr.Web corrente (v. [Statistiche](#)).

10.14.4. Cluster dei Server Dr.Web



Per informazioni sull'aggiornamento dei Server Dr.Web all'interno di un cluster v. sezione [Aggiornamento dei Server Dr.Web nel cluster](#).

Per informazioni sul ripristino di un nodo del cluster dopo un errore fatale di Server Dr.Web v. documento **Allegati**, sezione [Ripristino di un nodo del cluster di Server Dr.Web](#).

Se nella rete antivirus viene creato un cluster di Server Dr.Web, è necessario soddisfare i seguenti requisiti:

1. File di configurazione

`webmin.conf` — non richiede l'unificazione su tutti i server del cluster.

`drwcsd.conf` — una serie di impostazioni richiede l'unificazione:

- Sono disponibili solo nel file di configurazione stesso:

Parametri	Valori:
<pre><!-- Password encryption salt, keep it in safe place --></pre> Valore del salt crittografico per la cifratura della password amministratore nel database	uguali
<pre><!-- The server self id from license key. --></pre> Identificatore univoco del Server Dr.Web	diversi

- Può essere modificato dal Pannello di controllo (**Configurazione del Server Dr.Web**):

Schede	Parametri	Valori:
Generali	Nome del Server Dr.Web	non compilato o diverso
	Lingua del Server Dr.Web, Numero di richieste parallele dai client, Numero di copie di backup per le versioni del Server Dr.Web	non ha importanza
	altri	uguali



Schede	Parametri	Valori:
Traffico	Aggiornamenti, Installazioni	uguali
Rete	DNS, Proxy	non ha importanza
	Trasporto: Crittografia e Compressione; impostazioni relative alla modalità Multicasting	uguali
	Trasporto: altri	non ha importanza
	Posta elettronica, Cluster, Download	uguali
	Aggiornamenti per gruppi	si consiglia di lasciarlo su un server del cluster, disattivarlo sul resto dei server
Statistiche, Sicurezza, Cache, Moduli, Licenze	tutti	uguali
Posizione, Log	tutti	non ha importanza
Database	Numero di connessioni, Ripristina immagine corrotta in automatico	non ha importanza
	altri	uguali

2. Chiavi di crittografia e certificato Server Dr.Web

Su tutti i Server Dr.Web devono esserci le stesse chiavi di cifratura pubblica (*.pub) e privata (drwcsd.pri), e inoltre, il certificato di Server Dr.Web drwcsd-certificate.pem.

Se le chiavi di cifratura e il certificato non sono stati precedentemente creati, essi verranno generati automaticamente durante l'installazione del primo Server Dr.Web del cluster.

Le chiavi di cifratura e il certificato necessari per l'installazione dei successivi Server Dr.Web del cluster possono essere ottenuti attraverso il Pannello di controllo: menu

Amministrazione → **Chiavi di crittografia**. In seguito possono essere richiesti sia la chiave privata che il certificato: quando viene impostata la chiave privata drwcsd.pri durante l'installazione di un Server Dr.Web, la chiave pubblica *.pub e il certificato drwcsd-certificate.pem vengono generati automaticamente, però alla generazione del certificato viene creata una sua versione nuova, quindi il certificato deve essere sostituito con la stessa versione su tutti i Server Dr.Web di un cluster (v. [Strumenti per la connessione sicura](#)).



3. Lo stesso nome di Server Dr.Web

Per tutti i Server Dr.Web deve essere impostato lo stesso nome DNS di Server Dr.Web, utilizzato nella generazione dei file di installazione di Agent Dr.Web per le postazioni della rete antivirus.

Questo nome viene impostato attraverso il Pannello di controllo: **Amministrazione** → **Configurazione del Server Dr.Web** → scheda **Rete** → scheda [Download](#) → campo **Indirizzo di Server Dr.Web**. Le impostazioni di questa sezione sono conservate nel file di configurazione `download.conf` (la descrizione del file è riportata in documento **Allegati**, [F3. File di configurazione download.conf](#)).

4. Configurazione dell'uso del cluster

Sul server DNS nella rete è necessario registrare il nome di cluster comune per ogni singolo Server Dr.Web e impostare il metodo di bilanciamento del carico.

Affinché le impostazioni vengano applicate in modo automatico nel cluster di Server Dr.Web, è necessario utilizzare un apposito protocollo di cluster.

Per configurare il protocollo di cluster, per ciascuno dei Server Dr.Web nel Pannello di controllo è necessario passare al menu **Amministrazione** → **Configurazione del Server Dr.Web** e configurare le seguenti impostazioni:

- Per attivare il protocollo di cluster, nella scheda [Moduli](#) spuntare il flag **Protocollo di cluster dei Server Dr.Web**.
- Per configurare i parametri di interazione dei Server Dr.Web inclusi nel cluster, nella scheda [Cluster](#) configurare le impostazioni corrispondenti.

Per esempio:

- **Gruppo Multicast:** 232.0.0.1
- **Porta:** 11111
- **Interfaccia:** 0.0.0.0

In questo esempio per tutti i Server Dr.Web del cluster vengono configurati i trasporti per tutte le interfacce. In altri casi, per esempio quando una delle reti è esterna per il cluster e gli Agent Dr.Web si connettono attraverso di essa, mentre la seconda rete è una rete all'interno del cluster, è preferibile aprire il protocollo di cluster solo per le interfacce della rete interna. In questo caso come interfacce è necessario impostare gli indirizzi di tipo 192.168.1.1, ..., 192.168.1.N.

Dopo aver configurato tutti i parametri necessari, premere il pulsante **Salva** e riavviare i Server Dr.Web.

5. Database unico



Per poter utilizzare un database unico, tutti i Server Dr.Web devono essere della stessa versione.



Tutti i Server Dr.Web all'interno di un cluster devono utilizzare lo stesso database esterno. Come nel caso di utilizzo di un database senza organizzazione di un cluster, ciascuno dei Server Dr.Web si connette al database in modo indipendente, e tutti i dati dei Server Dr.Web vengono conservati separatamente. Ovunque sia pertinente, il Server Dr.Web prende dal database solo i record associati al suo ID che è univoco per ciascun Server Dr.Web. L'utilizzo del database unico consente ai Server Dr.Web di interagire con gli Agent Dr.Web inizialmente registrati su altri Server Dr.Web del cluster.

Quando viene creato un cluster di Server Dr.Web con database unico, è necessario tenere presente le seguenti caratteristiche:

- Il database può essere installato sia separatamente da tutti i Server Dr.Web che su uno dei computer su cui è installato un Server Dr.Web del cluster.
- Il database deve essere creato prima dell'installazione del primo Server Dr.Web del cluster o prima del momento della connessione del primo Server Dr.Web al database.
- Nel processo di aggiunta di nuovi nodi al cluster (ad eccezione del primo Server Dr.Web), durante l'installazione dei Server Dr.Web non è consigliabile impostare subito il database unico che viene utilizzato in questo cluster. Altrimenti questo potrebbe provocare l'eliminazione delle informazioni già memorizzate nel database. È consigliabile installare inizialmente i Server Dr.Web con il database interno e dopo l'installazione cambiarli al database esterno unico.

È possibile riconfigurare i Server Dr.Web all'utilizzo del database esterno attraverso il Pannello di controllo: nel menu **Amministrazione** → **Configurazione del Server Dr.Web** → nella scheda [Database](#) o attraverso il file di configurazione dei Server Dr.Web `drwcsd.conf`.

- Ad eccezione del primo Server Dr.Web del cluster, non è consigliabile introdurre nel cluster Server Dr.Web già funzionanti nella rete antivirus con un altro database esterno o quello interno. Questo provocherà una perdita di dati: informazioni sulle postazioni, statistiche, impostazioni (ad eccezione delle impostazioni conservate nei file di configurazione) in quanto durante l'importazione i dati nel database vengono completamente eliminati. In questo caso è possibile solo l'importazione parziale di alcune impostazioni.
- Di default durante l'installazione o l'aggiornamento dei Server Dr.Web dalle versioni precedenti, nel file di configurazione `drwcsd.conf` viene generato in modo casuale un valore del salt crittografico per la cifratura della password amministratore nel database. Per evitare problemi di autenticazione, è necessario impostare manualmente lo stesso valore salt su tutti i Server Dr.Web inclusi nel cluster. Il parametro necessario è descritto in documento **Allegati**, [F1. File di configurazione di Server Dr.Web](#).

6. Una versione del repository

Su tutti i Server Dr.Web del cluster i repository devono contenere aggiornamenti di versione uguale.

È possibile soddisfare questo requisito in uno dei seguenti modi:

- Aggiornare da SAM tutti i Server Dr.Web del cluster contemporaneamente. In questo caso tutti i Server Dr.Web conterranno la versione più recente degli aggiornamenti. Inoltre, è



possibile configurare l'aggiornamento dei repository di tutti i Server Dr.Web da una zona di aggiornamento locale (mirror di SAM) da cui verrà distribuita una versione uguale confermata degli aggiornamenti dei prodotti o la versione più recente in caso di creazione di un mirror di SAM.

- È possibile creare anche una struttura ibrida che combini in sé sia un cluster di Server Dr.Web che una struttura gerarchica basata su relazioni tra i server. In tale caso uno dei Server Dr.Web (può essere un Server Dr.Web del cluster o non incluso nel cluster) viene nominato principale e riceve gli aggiornamenti da SAM. Gli altri Server Dr.Web del cluster — quelli subordinati — ricevono gli aggiornamenti dal Server Dr.Web principale attraverso la comunicazione tra i server.

Se viene configurato l'aggiornamento dei Server Dr.Web del cluster da una zona locale o dal Server Dr.Web principale, è necessario monitorare l'operatività di questa zona o del Server Dr.Web principale. Se il nodo che distribuisce gli aggiornamenti va fuori servizio, è necessario rispettivamente riconfigurare uno degli altri Server Dr.Web al ruolo di Server Dr.Web principale o creare una nuova zona di aggiornamento per la ricezione degli aggiornamenti da SAM.

7. Le caratteristiche della distribuzione delle licenze per postazioni

Per la distribuzione delle licenze tra i Server Dr.Web di un cluster possono essere utilizzati i seguenti approcci:

- a) All'interno di un cluster non viene configurata alcuna struttura gerarchica dei Server Dr.Web. È sufficiente aggiungere una chiave (o più chiavi) di licenza su uno dei Server Dr.Web del cluster. Le informazioni su questa chiave di licenza verranno registrate nel database comune. Così, la chiave di licenza verrà utilizzata da tutti i Server Dr.Web del cluster contemporaneamente. Il numero totale di licenze memorizzate nel database comune deve corrispondere al numero totale di postazioni connesse a tutti i Server Dr.Web del cluster.



Per la possibilità di utilizzo della chiave di licenza su tutti i Server Dr.Web del cluster, e non solo su quello su cui la chiave è stata aggiunta, è necessario riavviare gli altri Server Dr.Web del cluster dopo l'aggiunta della chiave.

- b) È possibile creare una struttura ibrida che combini in sé sia un cluster di Server Dr.Web che una struttura gerarchica basata su relazioni tra server. Tale struttura sarà utile se per l'interazione con gli Agent Dr.Web vengono utilizzati i Server Dr.Web sia inclusi nel cluster che non inclusi. In questo caso il numero di licenze necessario viene distribuito dal file di licenza attraverso la comunicazione tra i server direttamente nel processo di funzionamento:
 - Da un Server Dr.Web che non è incluso nel cluster a uno dei Server Dr.Web del cluster. Le licenze distribuite verranno utilizzate da tutti i Server Dr.Web del cluster come descritto in p. a).
 - Da uno dei Server Dr.Web del cluster (cioè da una chiave utilizzata da tutti i Server Dr.Web del cluster) a un Server Dr.Web non incluso nel cluster.



La distribuzione di un numero di licenze necessario per un periodo necessario viene configurata manualmente dall'amministratore della rete antivirus (per maggiori informazioni v. sezione [Distribuzione delle licenze attraverso le relazioni tra i server](#)).

Per esempio, è possibile configurare una struttura gerarchica dei Server Dr.Web e nominare un Server Dr.Web principale (può essere un Server Dr.Web del cluster o non incluso nel cluster) che distribuirà sia gli aggiornamenti del repository che le licenze da un file di licenza.

8. I task nel calendario dei Server Dr.Web

Per escludere la duplicazione delle query al database, è consigliabile eseguire solo su uno dei Server Dr.Web le seguenti task dal calendario di Server Dr.Web: **Purge old records (Pulizia dei record vecchi)**, **Back up critical Dr.Web Server data (Backup dei dati critici del Server Dr.Web)**, **Purge old stations (Pulizia delle postazioni vecchie)**, **Purge unsent events (Pulizia degli eventi non inviati)**. Per esempio, essi possono essere eseguiti sul Server Dr.Web che si trova sullo stesso computer del database esterno unico. Ha senso eseguire i task sul computer del cluster con le maggiori prestazioni, se le configurazioni dei Server Dr.Web sono diverse e il database è installato su un computer separato.



Capitolo 11: Aggiornamento dei componenti di Dr.Web Enterprise Security Suite durante il funzionamento

In questo capitolo è descritto un aggiornamento dei componenti di Dr.Web Enterprise Security Suite che si esegue durante il funzionamento del prodotto e non è adatto per il passaggio a una nuova versione.

L'aggiornamento del prodotto e dei suoi componenti a una nuova versione è descritto in **Guida all'installazione**, in [Capitolo 7: Aggiornamento dei componenti di Dr.Web Enterprise Security Suite](#).



Prima dell'inizio dell'aggiornamento di Dr.Web Enterprise Security Suite e dei suoi singoli componenti, si consiglia vivamente di controllare la correttezza delle impostazioni del protocollo TCP/IP per la possibilità di accesso a internet. In particolare, il servizio DNS deve essere attivato e contenere le impostazioni corrette.

Prima di aggiornare il software, si consiglia di configurare il repository, compreso l'accesso a SAM Dr.Web (v. [Configurazione generale del repository](#)).

11.1. 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:

- Aggiornamento del software Server Dr.Web a una delle versioni disponibili caricate da SAM e memorizzate nel repository di Server Dr.Web. Le impostazioni di aggiornamento del repository da SAM sono descritte nella sezione [Gestione del repository di Server Dr.Web](#).
- Rollback del software Server Dr.Web a una copia di backup salvata. Le copie di backup del Server Dr.Web vengono create automaticamente durante il passaggio a una nuova versione nella sezione **Aggiornamenti del Server Dr.Web** (passo 4 della procedura sottostante).



L'aggiornamento di Server Dr.Web può inoltre essere eseguito tramite il pacchetto Server Dr.Web. La procedura è descritta in **Guida all'installazione**, 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 Dr.Web contengono il file di pacchetto. Alcuni di essi possono essere installati solo tramite il Pannello di controllo.



Quando il Server Dr.Web sotto SO della famiglia UNIX viene aggiornato tramite il Pannello di controllo, la versione di Server Dr.Web nella gestione pacchetti del sistema operativo non cambia.

Per gestire il software Server Dr.Web:

1. Selezionare la voce **Amministrazione** nel menu principale del Pannello di controllo, nella finestra che si è aperta selezionare la voce del menu di gestione **Server Dr.Web**.
2. Per passare alla lista delle versioni di Server Dr.Web, andare al link **Visualizza lista delle versioni**.
3. Si apre la sezione **Aggiornamenti del Server Dr.Web** con un elenco di aggiornamenti e backup di Server Dr.Web disponibili. In particolare:
 - Nella lista **Versione corrente** è indicata la versione di Server Dr.Web che viene utilizzata al momento. Nella sezione **Lista delle modifiche** sono riportati un breve elenco di nuove funzioni e un elenco di errori corretti in tale versione rispetto alla versione di aggiornamento precedente.
 - Nella lista **Aggiornamenti disponibili** è riportato un elenco di aggiornamenti per questo Server Dr.Web 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 Server Dr.Web iniziale da pacchetto di installazione, la sezione **Lista delle modifiche** è vuota.
 - Nella lista **Copie di backup** è riportato un elenco di copie di backup salvate per questo Server Dr.Web. Nella sezione **Data** sono disponibili informazioni sulla data di backup.
4. Per l'aggiornamento del software Server Dr.Web, impostare l'opzione di fronte alla versione di Server Dr.Web richiesta nella lista **Aggiornamenti disponibili** e premere il pulsante **Applica**.



È possibile effettuare l'aggiornamento solo a una versione di Server Dr.Web successiva a quella utilizzata al momento.

Nel processo di aggiornamento di Server Dr.Web, la versione corrente viene salvata come backup (viene messa nella sezione **Copie di backup**), mentre la versione a cui viene effettuato l'aggiornamento viene trasferita dalla sezione **Aggiornamenti disponibili** nella sezione **Versione corrente**.

I backup vengono salvati nella seguente directory:

```
var → update → backup → <versione_vecchia>-<versione_nuova>
```

Nel corso dell'aggiornamento viene creato o completato il file di log `var → dwupdater.log`.

5. Per il *rollback* del software Server Dr.Web a una copia di backup salvata, impostare l'opzione di fronte alla versione di Server Dr.Web richiesta nella lista **Copie di backup** e



premere il pulsante **Applica**. Nel processo di rollback del software Server Dr.Web, la copia di backup a cui viene effettuato il passaggio viene messa nella sezione **Versione corrente**.

6. Per il ripristino del software Server Dr.Web e il ritorno allo stato della revisione corrente, premere il pulsante **Ripristina Server**. Verrà ripristinata l'integrità del software server senza il salvataggio di una copia di backup e l'aggiornamento del database e dei file di configurazione. In assenza di tale revisione nel repository, il ripristino non è possibile.

11.2. Aggiornamento dei Server Dr.Web nel cluster

I Server Dr.Web all'interno di un cluster possono essere aggiornati in due modi:

Dai pacchetti di installazione

Con questo metodo è necessario arrestare tutti i Server Dr.Web e aggiornarli uno dopo l'altro.



La descrizione della procedura è riportata in **Guida all'installazione**, in [Capitolo 7: Aggiornamento dei componenti di Dr.Web Enterprise Security Suite](#).

Tramite il Pannello di controllo

Con questo metodo è necessario far uscire i nodi dal cluster uno per uno, cambiarli al database interno e aggiornarli in sequenza. Dopo aver aggiornato tutti i nodi, è necessario riconnetterli al cluster comune. Per fare questo:

1. Disconnettere dal cluster tutti i Server Dr.Web, tranne uno che aggiornerà il database operativo: su ciascuno dei Server Dr.Web nel cluster, tranne uno, andare ad **Amministrazione** → **Configurazione del Server Dr.Web** → scheda **Moduli** e togliere il flag **Protocollo di cluster dei Server Dr.Web**. Premere il pulsante **Salva** e riavviare la postazione.
2. Cambiare i Server Dr.Web disconnessi dal cluster a un altro database, per esempio, a quello incorporato: andare ad **Amministrazione** → **Configurazione del Server Dr.Web** → scheda **Database** e selezionare **SQLite3** nella lista a cascata **Database**. Per informazioni più dettagliate sulla connessione al database v. sezione [Database](#).
3. Vietare le connessioni degli Agent Dr.Web a questi Server Dr.Web: andare ad **Amministrazione** → **Configurazione del Server Dr.Web** → scheda **Moduli** e togliere il flag **Protocollo di Agent Dr.Web**. Premere il pulsante **Salva** e riavviare la postazione.
4. [Arrestare](#) tutti i Server Dr.Web disconnessi dal cluster.
5. [Aggiornare](#) il Server Dr.Web con il database di cluster.
6. Avviare e aggiornare uno dopo l'altro gli altri Server Dr.Web tramite il Pannello di controllo. Dopo aver aggiornato l'ultimo server, ricambiarli al database di cluster: andare ad **Amministrazione** → **Configurazione del Server Dr.Web** → scheda **Database** e selezionare il database di cluster nella lista a cascata **Database**. Per informazioni più dettagliate sulla connessione al database v. sezione [Database](#).



7. Consentire le connessioni degli Agent Dr.Web: andare ad **Amministrazione** → **Configurazione del Server Dr.Web** → scheda **Moduli** e spuntare il flag **Protocollo di Agent Dr.Web**. Premere il pulsante **Salva** e riavviare la postazione.
8. Riconnettere i Server Dr.Web al cluster: andare ad **Amministrazione** → **Configurazione del Server Dr.Web** → scheda **Moduli** e spuntare il flag **Protocollo di cluster dei Server Dr.Web**. Premere il pulsante **Salva** e riavviare la postazione.



Se i Server Dr.Web sono molti e il loro aggiornamento può richiedere molto tempo, per mantenere un funzionamento continuo, è possibile aggiornare solo una parte dei Server Dr.Web e assemblarne un cluster separato per il tempo in cui viene aggiornato il resto dei server.

La descrizione della procedura è riportata in sezione [Aggiornamento di Server Dr.Web e ripristino da copia di backup](#).

11.3. Aggiornamento del repository di Server Dr.Web manualmente

Per controllare lo stato attuale del repository o aggiornare i componenti della rete antivirus

1. Selezionare la voce **Amministrazione** nel 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 dei prodotti.



Nella colonna **Stato** è indicato lo stato dei prodotti nel repository di Server Dr.Web al momento dell'ultimo aggiornamento.

3. Per gestire i contenuti del repository, utilizzare i seguenti pulsanti nella barra degli strumenti:
 - Premere il pulsante **Verifica aggiornamenti** per verificare la disponibilità degli aggiornamenti di tutti i prodotti su SAM. Se un componente che viene verificato è obsoleto, esso verrà aggiornato in automatico.
 - Premere uno dei seguenti pulsanti nella barra degli strumenti per scaricare il log di aggiornamento del repository:
 - Registra le informazioni in file CSV,**
 - Registra le informazioni in file HTML,**
 - Registra le informazioni in file XML,**
 - Registra le informazioni in file PDF.**
 - Premere il pulsante **Ricarica il repository da disco** per ricaricare la versione corrente




del repository da disco.

Quando viene avviato, il Server Dr.Web carica i contenuti del repository nella memoria, e se nel processo di funzionamento del Server Dr.Web i contenuti del repository sono stati modificati dall'amministratore in un modo diverso da quello fornito dal Pannello di controllo, per esempio, aggiornati tramite un'utility esterna o manualmente, per utilizzare la versione del repository caricata sul disco, è necessario ricaricare il repository.

11.4. Aggiornamento del repository di Server Dr.Web secondo il calendario

È possibile configurare un calendario di task sul Server Dr.Web per l'esecuzione di aggiornamenti regolari del software (per maggiori informazioni sul calendario dei task v. p. [Configurazione del calendario di Server Dr.Web](#)).

Per configurare un calendario di aggiornamento del repository di Server Dr.Web

1. Selezionare la voce **Amministrazione** nel 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 la lista corrente dei task del Server Dr.Web.
2. Per aggiungere un nuovo task, nella barra degli strumenti premere il pulsante  **Crea task**. Si apre la finestra di modifica del task.
3. Nella scheda **Generali** impostare i seguenti parametri:
 - Nel campo **Nome** impostare il nome del task sotto cui esso verrà visualizzato nel calendario.
 - Spuntare il flag **Permetti l'esecuzione** per attivare l'esecuzione del task. Se il flag non è selezionato, il task sarà presente nella lista ma non verrà eseguito.
 - Spuntare il flag **Task critico** per eseguire il task in modo straordinario se l'esecuzione di questo task è stata persa nell'ora programmata per qualsiasi motivo. Scheduler controlla ogni minuto l'elenco dei task e se scopre un task critico perso, lo avvia. Se al momento dell'avvio il task è stato perso diverse volte, verrà eseguito solo 1 volta.
 - Se il flag **Avvia il task in modo asincrono** è deselezionato, il task verrà messo nella coda generale dei task di Scheduler eseguiti in sequenza. Spuntare il flag per eseguire questo task in modo parallelo al di fuori della coda.
4. Nella scheda **Azione** impostare i seguenti parametri:
 - Dalla lista a cascata **Azione** selezionare il tipo di task **Aggiornamento del repository**.
 - Nella lista **Prodotto** spuntare i flag di fronte ai prodotti del repository che verranno aggiornati secondo questo task.
 - Spuntare il flag **Aggiorna chiavi di licenza** per attivare la procedura per l'aggiornamento automatico delle chiavi di licenza durante l'aggiornamento del repository. Informazioni dettagliate sono riportate nella sezione [Aggiornamento automatico delle licenze](#).
5. Nella scheda **Tempo** impostare i seguenti parametri:



- Dalla lista a cascata **Periodicità** selezionare la modalità di avvio del task e impostare il tempo secondo la periodicità scelta.
 - 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.
6. Premere il pulsante **Salva** per creare il task con i parametri impostati.

11.5. Aggiornamento del repository di un Server Dr.Web non connesso a internet

Se Server Dr.Web non è connesso a internet per la ricezione degli aggiornamenti del repository dai server SAM, sono possibili le seguenti varianti di configurazione dell'aggiornamento:

- Se nella rete c'è un altro Server Dr.Web connesso a internet per la ricezione degli aggiornamenti, impostare una relazione tra i server con esso come server paritari o principale-subordinato in cui il Server Dr.Web non connesso a internet sarà subordinato. In tale caso, il Server Dr.Web non connesso a internet riceverà automaticamente tutti gli aggiornamenti dal Server Dr.Web principale.
La configurazione delle relazioni tra i server è descritta nella sezione [Caratteristiche di una rete con diversi Server Dr.Web](#).
- Se non è possibile configurare l'aggiornamento automatico da un altro Server Dr.Web tramite una relazione tra i server, è possibile aggiornare manualmente il repository del Server Dr.Web non connesso:
 - Se nella rete c'è un altro Server Dr.Web connesso a internet per la ricezione degli aggiornamenti, trasferire manualmente il contenuto del repository dal Server Dr.Web che viene aggiornato, come descritto nella sezione [Copiatura del repository di un altro Server Dr.Web](#).
 - Se nella rete non c'è la possibilità di connettere uno dei Server Dr.Web a internet per la ricezione degli aggiornamenti, è possibile scaricare il repository da SAM senza utilizzare il software Server Dr.Web. Per tale scopo è fornita un'utility standard [Loader di repository Dr.Web](#) che fa parte della lista dei prodotti del repository.



La [versione grafica](#) dell'utility è disponibile solo per SO Windows e può essere scaricata nei seguenti modi:

- dal sito <https://download.drweb.com>. Dopo l'inserimento del numero di serie e la selezione del tipo di prodotto si aprirà la tabella di **Download guidato**, dove è possibile selezionare il loader di repository Dr.Web richiesto.
- tramite il Pannello di controllo, nella sezione **Amministrazione** → **Utility**. L'utility si trova nella directory `webmin\utilities` della directory di installazione di Server Dr.Web (file eseguibile `drweb-reploder-gui-windows-<numero_di_bit>.exe`). Se è assente, è necessario scaricarla seguendo le [istruzioni](#).

È disponibile anche una versione [console](#) dell'utility.



11.5.1. 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 progettato per l'aggiornamento di Server Dr.Web a una nuova versione.

Per trasferire gli aggiornamenti di repository da un altro Server Dr.Web

1. Aggiornare il repository del Server Dr.Web connesso a internet utilizzando la sezione **Amministrazione** → [Stato del repository](#) nel Pannello di controllo.
2. Esportare il repository o una sua parte (i prodotti richiesti) tramite il Pannello di controllo, utilizzando la sezione [Contenuti del repository](#). È necessario esportare soltanto i tipi di oggetti che sono supportati per la successiva importazione.
3. Copiare l'archivio con il repository esportato sul computer con il Server Dr.Web che richiede l'aggiornamento.

Importare il repository caricato sul Server Dr.Web tramite il Pannello di controllo, utilizzando la sezione **Amministrazione** → [Contenuti del repository](#).



Se vengono utilizzate le impostazioni speciali del repository, quali il congelamento di revisioni o l'aggiornamento di Agent Dr.Web solo da una revisione impostata (diversa da quella ultima), nel processo di importazione del repository è necessario attivare l'opzione **Aggiungi soltanto le revisioni mancanti** e disattivare l'opzione **Importa i file di configurazione**.

11.5.2. Loader di repository Dr.Web

Se uno dei Server Dr.Web non può essere connesso a internet, è possibile scaricare il repository da SAM senza utilizzare il software Server Dr.Web. Per tale scopo viene fornita l'utility standard Loader di repository Dr.Web.

Caratteristiche dell'utilizzo

- Per il caricamento del repository da SAM è richiesta 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.



La lista dei prodotti di repository è riportata nella sezione [Gestione del repository di Server Dr.Web](#).

Con il cambio della versione di Server Dr.Web cambia anche la lista dei prodotti disponibili per il download. Premere il pulsante **Aggiorna l'elenco** nella lista dei prodotti e assicurarsi che siano selezionati tutti i prodotti richiesti.

Possibili varianti dell'utilizzo

Caricamento con la sostituzione manuale del repository

1. Caricare da SAM il repository di Server Dr.Web attraverso l'utility Loader di repository Dr.Web.

Al caricamento creare un archivio di repository:

- a) In caso dell'utility grafica: selezionare la modalità **Carica repository** e spuntare la casella **Archivia il repository** nella finestra principale dell'utility.
 - b) In caso dell'utility console: utilizzare l'opzione `--archive`.
2. Copiare l'archivio con il repository caricato sul computer con il Server Dr.Web che richiede gli aggiornamenti.

Importare il repository caricato sul Server Dr.Web tramite il Pannello di controllo, utilizzando la sezione **Amministrazione** → [Contenuti del repository](#).



Se vengono utilizzate le impostazioni speciali del repository, quali il congelamento di revisioni o l'aggiornamento di Agent Dr.Web solo da una revisione impostata (diversa da quella ultima), nel processo di importazione del repository è necessario attivare l'opzione **Aggiungi soltanto le revisioni mancanti** e disattivare l'opzione **Importa i file di configurazione**.

Creazione di un mirror del repository su un server della rete locale

1. Caricare da SAM il repository di Server Dr.Web attraverso l'utility grafica Loader di repository Dr.Web.

Al caricamento selezionare la modalità **Sincronizza mirror degli aggiornamenti** nella finestra principale dell'utility.

2. Mettere il repository caricato su un web server della propria rete locale, che verrà utilizzato per distribuire gli aggiornamenti del repository.
3. Nella sezione **Amministrazione** → [Configurazione generale del repository](#) configurare la ricezione di aggiornamenti da parte del Server Dr.Web dal mirror locale anziché dai server SAM Dr.Web. La scelta del protocollo di caricamento di aggiornamenti dipenderà dal tipo di server dal passaggio 2: HTTP/HTTPS per un web server, FTP/FTPS per un server FTP ecc. Un'eccezione è il protocollo FILE — non è disponibile per l'uso via rete (vedi [Creazione di un mirror di repository sul Server Dr.Web](#)).



Creazione di un mirror di repository sul Server Dr.Web

1. Caricare da SAM il repository di Server Dr.Web attraverso l'utility Loader di repository Dr.Web.

Al caricamento selezionare la modalità **Sincronizza mirror degli aggiornamenti** nella finestra principale dell'utility.

2. Mettere il mirror creato in una directory sul computer su cui è installato il Server Dr.Web.
3. Nella sezione **Amministrazione** → [Configurazione generale del repository](#) configurare la ricezione di aggiornamenti con l'utilizzo del protocollo FILE.

Nel campo **URI di base** è necessario indicare il completo percorso locale della directory in cui si trova il mirror. In questo caso il parametro **Lista dei server del Sistema di aggiornamento mondiale Dr.Web** non viene utilizzato.



Assicurarsi che il mirror si trovi nella directory con il nome 13.00. Il percorso nel campo **URI di base** deve essere indicato fino a questa directory senza comprendere la directory stessa.

11.5.2.1. Utility con interfaccia grafica

La versione con interfaccia grafica dell'utility Loader di repository Dr.Web è disponibile solo per SO Windows e può essere scaricata tramite il Pannello di controllo, nella sezione **Amministrazione** → **Utility**. Questa versione dell'utility può essere eseguita su qualsiasi computer SO Windows con accesso a internet.

L'utility si trova nella directory `webmin\utilities` della directory di installazione di Server Dr.Web. Il file eseguibile è `drweb-reploader-gui-windows-<numero_di_bit>.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** — indicare il file della chiave di licenza Dr.Web. Per fare ciò, premere **Sfoggia** e selezionare un file della chiave di licenza valido. Invece del file della chiave di licenza è possibile indicare solo l'hash MD5 della chiave di licenza che può essere visualizzato nel Pannello di controllo, nella sezione **Amministrazione** → **Gestione licenze**.
 - b) **Directory di caricamento** — 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 scaricato nel formato repository di Server Dr.Web. I file scaricati possono essere importati direttamente attraverso il Pannello di controllo come aggiornamento del repository di Server Dr.Web.



- **Sincronizza mirror di aggiornamento** — il repository viene scaricato nel formato zona di aggiornamento SAM. I file scaricati possono essere collocati su un mirror di aggiornamento nella rete locale. In seguito i Server Dr.Web possono essere configurati per ricevere gli aggiornamenti direttamente da questo mirror di aggiornamento che contiene l'ultima versione del repository, invece di ricevere gli aggiornamenti dai server SAM.
- d) Spuntare il flag **Archivia** affinché il repository venga automaticamente compresso in un archivio zip. Questa opzione permette di ottenere un file di archivio pronto per l'importazione del repository sul Server Dr.Web 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 i 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 di aggiornamento, 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** — le credenziali 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.

11.5.2.2. Versione console dell'utility

Si mettono a disposizione le seguenti versioni dell'utility console Loader di repository Dr.Web:

File eseguibile	Posizione	Descrizione
<code>drweb-reloader-<systema_operativo>-<numero_di_bit></code>	Pannello di controllo, sezione Amministrazione → Utility Directory di Server Dr.Web <code>webmin/utilities</code>	Versione indipendente dell'utility. Può essere avviata da qualsiasi directory e su qualsiasi computer con il sistema operativo corrispondente.
<code>drwreloader</code>	Directory di Server Dr.Web <code>bin</code>	La versione dell'utility dipende dalla disponibilità delle librerie del server. Può essere avviata solo dalla directory della sua posizione.



Le opzioni della riga di comando per la versione console dell'utility Loader di repository sono descritte in documento **Allegati**, [H7.5. Loader di repository Dr.Web](#).


11.6. Limitazione degli aggiornamenti delle postazioni

Tramite il Pannello di controllo è possibile impostare limitazioni al quantità di traffico di rete durante la trasmissione degli aggiornamenti tra il Server Dr.Web e gli Agent Dr.Web su postazioni protette in determinati intervalli di tempo.






Per maggiori informazioni v. p. [Limitazione del traffico dati delle postazioni.](#)



Le limitazioni alla velocità di aggiornamento non si applicano nel caso di installazione aggiuntiva di componenti nuovi, nonché nel caso di aggiornamento avviato dall'amministratore tramite l'opzione della barra degli strumenti  **Ripristina i componenti falliti.**

Per configurare la modalità di limitazione di traffico

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:
 - **Aggiorna tutti i prodotti** — per non impostare restrizioni alla distribuzione degli aggiornamenti alle postazioni.
 - **Proibisci tutti gli aggiornamenti** — per proibire la distribuzione di tutti gli aggiornamenti alle postazioni negli intervalli di tempo definiti di seguito nella tabella **Calendario dell'aggiornamento delle postazioni**.
 - **Aggiorna soltanto i database** — per proibire la distribuzione solo degli aggiornamenti dei moduli software negli intervalli di tempo definiti di seguito nella tabella **Calendario dell'aggiornamento delle postazioni**. I database dei virus verranno aggiornati senza cambiamenti in modalità normale.
3. Spuntare il flag **Riduci la gravità dello stato con i database dei virus non aggiornati** per ridurre la gravità degli stati delle postazioni con database dei virus non aggiornati. Se il flag è selezionato, le postazioni con database dei virus non aggiornati verranno visualizzate nella rete antivirus con un'icona comune , e nella sezione **Stato** le postazioni avranno la gravità **Bassa**. Se il flag è deselezionato, le postazioni con database dei virus non aggiornati verranno visualizzate nella rete antivirus con l'icona  (se è attivata l'opzione nella barra degli strumenti  **Impostazioni della vista albero** → **Mostra gravità dello stato delle postazioni**), e nella sezione **Stato** le postazioni avranno la gravità **Massima** o **Alta**.
4. Nel campo **Intervallo di stato aggiornato delle revisioni** viene impostato l'intervallo di tempo durante cui le revisioni dei prodotti installati sulle postazioni verranno considerate aggiornate nel caso di comparsa di nuove revisioni nel repository di Server Dr.Web.
5. Spuntare il flag **Ricevi gli aggiornamenti più 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 aggiornamenti attuali da distribuire.
6. Spuntare il flag **Consenti il passaggio a revisioni precedenti** per consentire la sostituzione delle nuove versioni dei componenti antivirus su postazioni con revisioni precedenti dal repository di Server Dr.Web secondo le impostazioni di distribuzione.



Vedere inoltre [Rollback della revisione del prodotto alla versione precedente](#).

7. Spuntare il flag **Limita la banda per gli aggiornamenti** per limitare la quantità di traffico di rete durante la trasmissione degli aggiornamenti tra il Server Dr.Web e gli Agent Dr.Web.

Se la spunta al flag è tolta, gli aggiornamenti vengono trasmessi agli Agent Dr.Web senza la limitazione della larghezza di banda.

Se il flag è spuntato, impostare i seguenti campi:

- Nel campo **Velocità di default** viene impostato il valore della velocità massima di trasmissione di aggiornamenti che viene utilizzato di default, cioè se nessun'altra limitazione è impostata (le celle vuote bianche nella tabella del calendario). Inoltre, il valore di velocità predefinita viene utilizzato per i periodi quando la trasmissione di dati è proibita, ma il processo di aggiornamento è già stato avviato (vedi di seguito).
- Nel campo **Velocità di trasmissione massima (KB/s)** viene indicato un valore della velocità massima di trasmissione degli aggiornamenti. Gli aggiornamenti verranno trasmessi nei limiti della larghezza di banda impostata per il traffico dati cumulativo degli aggiornamenti di tutti gli Agent Dr.Web..

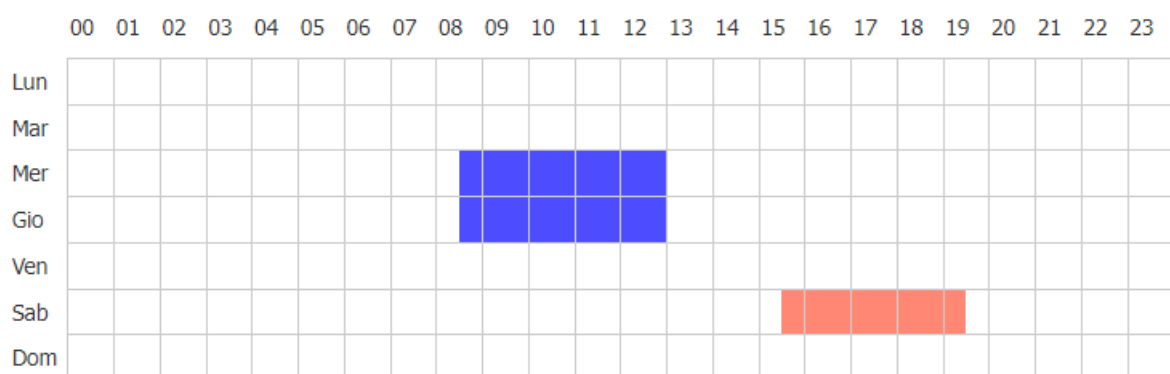
È possibile impostare fino a cinque limitazioni alla velocità di trasmissione di aggiornamenti. Per aggiungere un altro campo di limitazione di velocità, premere il pulsante **+**. Per rimuovere una limitazione, premere il pulsante **-** di fronte alla limitazione che si desidera rimuovere.



Per i valori dei campi **Velocità di default** e **Velocità di trasmissione massima (KB/s)** esistono le seguenti limitazioni:

- È vietato impostare il valore 0. Il valore minimo consentito della limitazione è 1 KB/s.
- Il valore vuoto (il campo non è compilato) elimina tutte le limitazioni al traffico degli aggiornamenti per il periodo corrispondente.

Nella tabella di calendario viene configurata una modalità di limitazione di trasmissione di dati separatamente per ogni 30 minuti di ogni giorno della settimana.



- Senza limitazioni
- La velocità è limitata a 1 KB/s
- La trasmissione di dati è proibita



Per modificare la modalità di limitazione di trasmissione di dati, fare clic sul relativo blocco della tabella. Inoltre, è supportata la selezione di più blocchi di tempo tramite trascinamento.

Il colore delle celle cambia ciclicamente secondo lo schema di colori riportato sotto la tabella.



Nei periodi di tempo che corrispondono al valore **la trasmissione di dati è proibita** è vietato iniziare una trasmissione di aggiornamenti. Se al verificarsi di tale periodo una trasmissione di aggiornamenti è già stata avviata, non verrà interrotta, ma la velocità massima di trasmissione verrà limitata dal valore indicato nel campo **Velocità di default**.


8. Dopo aver finito di modificare, premere il pulsante **Salva** per accettare le modifiche apportate.


Nella barra degli strumenti sono inoltre disponibili le seguenti opzioni per la gestione dei contenuti della sezione:


 **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 di 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, un gruppo o più gruppi e postazioni.

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

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

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

 **Importa impostazioni in questa sezione da file** — per sostituire tutte le impostazioni in questa sezione con le impostazioni salvate in un file di formato specifico.

11.7. Aggiornamento di Agent Dr.Web in modalità mobile

Se il computer, notebook o dispositivo mobile dell'utente per un lungo periodo non avrà la connessione con il Server Dr.Web, per la ricezione tempestiva degli aggiornamenti dai server SAM Dr.Web si consiglia di impostare la *Modalità mobile* di funzionamento dell'Agent Dr.Web sulla postazione.



La possibilità di attivare la Modalità mobile nelle impostazioni di Agent Dr.Web sarà disponibile a condizione che l'utilizzo di Modalità mobile sia consentito nel Pannello di controllo nella sezione **Rete antivirus** → **Permessi** → <systema_operativo> → **Generali** → **Modifica della configurazione di Agent Dr.Web** (in caso di SO Windows) o **Avvio in modalità mobile** (in caso di altri sistemi operativi).

In Modalità mobile l'Agent Dr.Web cerca di connettersi al Server Dr.Web, effettua tre tentativi, e se non ci è riuscito, esegue un aggiornamento HTTP dai server SAM. I tentativi di ricerca del Server Dr.Web si susseguono continuamente a intervallo di circa un minuto.

Durante il funzionamento dell'Agent Dr.Web in Modalità mobile, la connessione dell'Agent Dr.Web al Server Dr.Web si interrompe. Tutte le modifiche che vengono impostate sul Server Dr.Web per tale postazione avranno effetto non appena la Modalità mobile di funzionamento dell'Agent Dr.Web verrà disattivata, e la connessione dell'Agent Dr.Web al Server Dr.Web riprenderà.



In modalità mobile vengono aggiornati soltanto i database dei virus.

In Modalità mobile il funzionamento dell'Agent Dr.Web non è limitato nel tempo, però l'aggiornamento dei database dei virus da SAM viene effettuato solo fino alla scadenza della chiave di licenza della postazione, le informazioni su cui sono state salvate dall'Agent Dr.Web all'ultima connessione al Server Dr.Web (la chiave di licenza stessa si trova sul Server Dr.Web).

Le impostazioni della modalità mobile di funzionamento sul lato Agent Dr.Web sono descritte in **Manuale dell'utente**.



Capitolo 12: Configurazione dei componenti aggiuntivi

12.1. Server proxy Dr.Web

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

L'obiettivo principale del Server proxy Dr.Web è quello di provvedere alla comunicazione tra il Server Dr.Web e gli 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 nelle reti diverse tra cui non c'è l'instradamento dei pacchetti).

Il Server proxy Dr.Web consente di utilizzare qualsiasi computer facente parte della rete antivirus per i seguenti scopi:

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

Funzioni principali

Il server proxy Dr.Web svolge le seguenti funzioni:

1. È in ascolto e accetta connessioni secondo le impostazioni di protocollo e porta.
2. Conversione di 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 Dr.Web.
4. Memorizzazione nella cache degli aggiornamenti dell'Agent Dr.Web e del pacchetto antivirus, trasmessi dal Server Dr.Web. Se gli aggiornamenti vengono rilasciati dalla cache del Server proxy Dr.Web, questo permette di:
 - diminuire il traffico di rete,
 - diminuire il tempo di ricezione degli aggiornamenti da parte degli Agent Dr.Web.
5. Possibilità di cifratura del traffico tra i Server Dr.Web e gli Agent Dr.Web.



È possibile creare una gerarchia dei Server proxy Dr.Web.

Lo schema generale della rete antivirus con l'utilizzo del Server proxy Dr.Web è riportato in [immagine 12-1](#).

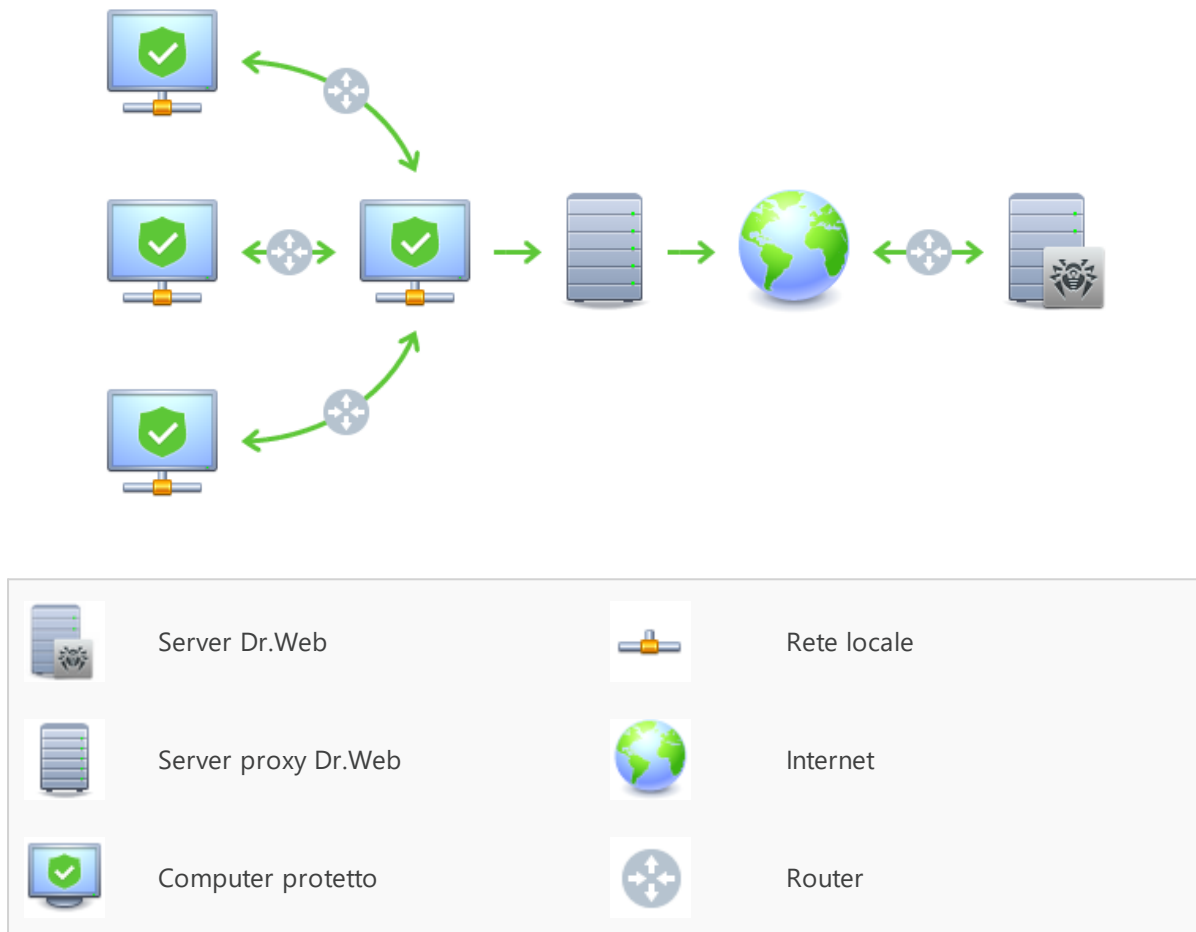


Immagine 12-1. Schema della rete antivirus con utilizzo di Server proxy Dr.Web

Principio di funzionamento

In caso di utilizzo del Server proxy Dr.Web, viene eseguita la seguente sequenza di azioni:

1. Se nell'Agent Dr.Web non è trascritto l'indirizzo del Server Dr.Web, l'Agent Dr.Web invia una richiesta multicast in conformità al protocollo della rete in cui si trova.
2. Se il Server proxy Dr.Web è configurato per la ritrasmissione di connessioni (il parametro `discovery="yes"`), all'Agent Dr.Web viene inviato un avviso di disponibilità di un Server proxy Dr.Web operativo.
3. L'Agent Dr.Web imposta i parametri di Server proxy Dr.Web ottenuti come parametri di Server Dr.Web. L'ulteriore interazione avviene in modo trasparente per l'Agent Dr.Web.
4. Secondo i parametri del file di configurazione, il Server proxy Dr.Web è in ascolto sulle porte impostate per le connessioni in ingresso attraverso i protocolli indicati.



5. Per ciascuna connessione in ingresso da un Agent Dr.Web il Server proxy Dr.Web stabilisce una connessione con il Server Dr.Web.

Algoritmo di reindirizzamento se è disponibile una lista dei Server Dr.Web:

1. Il Server proxy Dr.Web carica nella memoria operativa una lista di Server Dr.Web dal file di configurazione `drwcsd-proxy.conf` (v. documento **Allegati**, [F4. File di configurazione di Server proxy Dr.Web](#)).
2. L'Agent Dr.Web si connette al Server proxy Dr.Web.
3. Il Server proxy Dr.Web reindirizza il traffico dall'Agent Dr.Web sul primo Server Dr.Web dalla lista nella memoria operativa.
4. Il Server proxy Dr.Web ruota la lista caricata nella memoria operativa e sposta questo Server Dr.Web dal primo elemento della lista alla fine della lista.



Il Server proxy Dr.Web non memorizza nel suo file di configurazione la sequenza modificata dei Server Dr.Web. Quando il Server proxy Dr.Web viene riavviato, la lista dei Server Dr.Web viene caricata nella memoria operativa nella sua versione originale, conservata nel file di configurazione.

5. Quando un altro Agent Dr.Web si connette al Server proxy Dr.Web, la procedura si ripete dal passaggio 2.
6. Se il Server Dr.Web si disconnette dalla rete antivirus (per esempio, in caso di spegnimento o negazione del servizio), l'Agent Dr.Web si riconnette al Server proxy Dr.Web, e la procedura si ripete dal passaggio 2.



[Scanner di rete](#), se avviato su un computer da una rete che è esterna relativamente agli Agent, non può rilevare gli Agent Dr.Web installati.



Se nelle impostazioni del Server Dr.Web è selezionato il flag **Sostituisci i nomi NetBIOS**, e nella rete antivirus viene utilizzato un Server proxy Dr.Web, per tutte le postazioni connesse al Server Dr.Web attraverso il Server proxy Dr.Web come nomi di postazioni nel Pannello di controllo verrà visualizzato il nome del computer su cui è installato il Server proxy Dr.Web.

Cifratura e compressione del traffico dati

Il Server proxy Dr.Web 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 Dr.Web supporta la cifratura del traffico. Per supportare la cifratura, il Server proxy Dr.Web deve connettersi al Server Dr.Web (v. **Guida all'installazione**, [Connessione del Server proxy Dr.Web al Server Dr.Web](#)) e firmare il suo certificato con il certificato e la chiave privata del Server Dr.Web. La cifratura del traffico tra il Server proxy Dr.Web e il Server Dr.Web viene effettuata sulla base del certificato del Server Dr.Web; la cifratura del traffico tra il Server



proxy Dr.Web e gli Agent Dr.Web viene effettuata sulla base del certificato del Server proxy Dr.Web firmato con il certificato e la chiave privata del Server Dr.Web.

Memorizzazione nella cache

Il Server proxy Dr.Web supporta la memorizzazione nella cache del traffico dati.

I prodotti vengono memorizzati nella cache per revisione. Ciascuna revisione è conservata in una directory separata. Nella directory di ciascuna revisione successiva sono situati gli *hard link* dei file esistenti dalle revisioni precedenti e gli originali dei file modificati. Pertanto, i file per ciascuna versione sono conservati sul disco rigido in una sola copia, in tutte le directory delle revisioni successive sono riportati solo i link dei file non modificati.

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 dalla memoria periodicamente i file *memory mapped* non utilizzati. Di default — ogni 10 minuti.

Impostazioni

Il Server proxy Dr.Web non ha interfaccia grafica. Le impostazioni vengono configurate in uno dei seguenti modi:

1. In remoto attraverso il Pannello di controllo, se il Server proxy Dr.Web è connesso al Server Dr.Web (v. [Configurazione del Server proxy in remoto](#)).
2. Localmente tramite il file di configurazione. Il formato del file di configurazione del Server proxy Dr.Web è riportato nel documento **Allegati**, [Connessione del Server proxy Dr.Web al Server Dr.Web](#).



La gestione delle impostazioni (modifica del file di configurazione) del Server proxy Dr.Web può essere effettuata solo da un utente con i permessi dell'amministratore di tale computer.

Per il corretto funzionamento del Server proxy Dr.Web su SO della famiglia Linux, dopo il riavvio del computer è necessario effettuare la configurazione di sistema della rete senza utilizzare Network Manager.



Avvio e arresto

Su SO Windows il Server proxy Dr.Web viene avviato e arrestato tramite gli strumenti standard attraverso l'elemento **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.

Su SO della famiglia UNIX il Server proxy Dr.Web viene avviato e arrestato tramite i comandi `start` e `stop` applicati agli script creati nel corso dell'installazione del Server proxy Dr.Web (v. **Guida all'installazione**, [Installazione del Server proxy Dr.Web](#)).

Inoltre, per l'avvio del Server proxy Dr.Web su SO Windows e SO della famiglia UNIX, è possibile avviare il file eseguibile `drwcsd-proxy` con i parametri corrispondenti (v. [G5. Server proxy Dr.Web](#)).

12.1.1. Configurazione del Server proxy in remoto

Dopo la connessione del Server proxy Dr.Web al Server Dr.Web è fornita la possibilità di configurazione del Server proxy Dr.Web in remoto attraverso il Pannello di controllo.



Informazioni dettagliate sulle impostazioni di connessione, nonché sulla connessione rapida tramite riga di comando sono riportate in **Guida all'installazione**, sezione [Connessione del Server proxy Dr.Web al Server Dr.Web](#).



Il Server proxy Dr.Web può ricevere impostazioni solo da un determinato set di Server Dr.Web connessi ad esso che sono contrassegnati come server di gestione. Se nessun Server Dr.Web è contrassegnato come server di gestione, la connessione viene effettuata a tutti i Server Dr.Web uno dopo l'altro fino alla prima ricezione di una configurazione valida (non vuota).

Se un Server Dr.Web non è contrassegnato come server di gestione (per il parametro **Server Dr.Web di gestione** è impostato il valore **No**), il Server proxy Dr.Web non può ricevere alcuna impostazione da esso. Ciò significa inoltre che da questo Server Dr.Web non è possibile nominare quest'ultimo server di gestione per il Server proxy Dr.Web in remoto. In tale caso, è necessario modificare il valore del parametro `<forward to="" master="">` nel file di configurazione del Server proxy Dr.Web manualmente (v. documento **Allegati**, [F4. File di configurazione di Server proxy Dr.Web](#)).

Per configurare le impostazioni del Server proxy Dr.Web


1. Selezionare la voce **Rete antivirus** nel menu principale del Pannello di controllo, nella finestra che si è aperta nella lista gerarchica fare clic sul nome di un Server proxy Dr.Web o del gruppo **Proxies** e dei suoi sottogruppi.
2. Nel [menu di gestione](#) che si è aperto selezionare la voce **Server proxy Dr.Web**. Si aprirà la sezione delle impostazioni.



3. Nella scheda **Certificato** viene impostata una lista di certificati dei Server Dr.Web. È necessaria la presenza dei certificati di tutti i Server Dr.Web a cui si connette il Server proxy Dr.Web e su cui viene reindirizzato il traffico client.
 - Il certificato del Server Dr.Web è richiesto per la connessione al Server Dr.Web al fine di gestione delle impostazioni remota, nonché per il supporto della cifratura del traffico tra il Server Dr.Web e il Server proxy Dr.Web.
 - Il certificato del Server proxy Dr.Web, che viene firmato con il certificato e la chiave privata del Server Dr.Web (la procedura viene effettuata automaticamente sul Server Dr.Web dopo la connessione e non richiede l'intervento dell'amministratore), è richiesto per la connessione degli Agent Dr.Web e per il supporto della cifratura del traffico tra gli Agent Dr.Web e il Server proxy Dr.Web.
4. Nella scheda **Ascolto** vengono configurati i parametri di ricezione e reindirizzamento del traffico da parte del Server proxy Dr.Web.

Per impostazioni uniche di ascolto di rete è possibile definire impostazioni uniche di connessione di tutti i client e impostazioni definite separatamente per ciascuno dei Server Dr.Web.

Per aggiungere un altro blocco di impostazioni, fare clic sul pulsante .

Per rimuovere un blocco di impostazioni, fare clic su  accanto al blocco che si vuole rimuovere.

Per ciascun blocco è possibile configurare separatamente i seguenti parametri di funzionamento del Server proxy Dr.Web:

a) Nella sezione delle impostazioni di ascolto:

- Nel campo **Indirizzo per l'ascolto** impostare un indirizzo IP su cui il Server proxy Dr.Web "è in ascolto". Il valore 0.0.0.0 prescrive di "essere in ascolto" su tutte le interfacce.



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

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




b) Nella sezione **Parametri di connessione con i client**:



- Dalla lista a cascata **Crittografia** selezionare la modalità di cifratura del traffico per i canali tra il Server proxy Dr.Web e i relativi client: Agent Dr.Web ed installer di Agent Dr.Web.
 - Dalla lista a cascata **Compressione** selezionare la modalità di compressione del traffico per i canali tra il Server proxy Dr.Web e i relativi client: Agent Dr.Web ed installer di Agent Dr.Web. Dalla lista a cascata **Livello di compressione** selezionare un livello di compressione (da 1 a 9).
- c) Nella sezione **Parametri di connessione con i Server Dr.Web** viene impostata una lista dei Server Dr.Web su cui verrà reindirizzato il traffico.

Dall'ordine di sequenza dei Server Dr.Web nella lista dipendono l'ordine di reindirizzamento del traffico client e l'ordine di connessione del Server proxy Dr.Web ai Server Dr.Web per l'ottenimento delle impostazioni. Per modificare l'ordine di sequenza dei Server Dr.Web, trascinare le righe richieste tramite il mouse.

Per gestire i Server Dr.Web, utilizzare i pulsanti nella barra degli strumenti della lista dei Server Dr.Web:

-  modifica i parametri di connessione con il Server Dr.Web selezionato,
-  aggiungi i parametri di connessione con il Server Dr.Web,
-  rimuovi i parametri di connessione con il Server Dr.Web selezionato.

Alla modifica e creazione dei parametri di connessione con i Server Dr.Web si apre una finestra delle impostazioni con le seguenti opzioni:

- Dalla lista a cascata **Server Dr.Web di gestione** selezionare una delle varianti di nomina del Server Dr.Web server di gestione:
 - Si** — il Server Dr.Web sarà server di gestione incondizionato. È possibile nominare server di gestione qualsiasi numero di server, la connessione viene effettuata a tutti i Server Dr.Web di gestione nell'ordine di sequenza definito nelle impostazioni del Server proxy Dr.Web fino alla prima ricezione di una configurazione valida (non vuota).
 - No** — il Server Dr.Web non sarà server di gestione in nessun caso. È inoltre possibile non nominare server di gestione nessuno dei Server Dr.Web. In questo caso, l'impostazione dei parametri del Server proxy Dr.Web (compresa la nomina dei Server Dr.Web di gestione) è possibile solo localmente attraverso il file di configurazione del Server proxy Dr.Web (v. documento **Allegati**, [F4. File di configurazione di Server proxy Dr.Web](#)).
 - Possibile** — il Server Dr.Web sarà server di gestione solo nel caso in cui non ci sono server di gestione incondizionati (con il valore **Si** per questa impostazione).
- Nel campo **Indirizzo di reindirizzamento** impostare l'indirizzo del Server Dr.Web su cui verranno reindirizzate le connessioni stabilite dal Server proxy Dr.Web. Come indirizzo di Server Dr.Web è consigliato utilizzare il nome di Server Dr.Web in [formato FQDN](#).



Se nel campo **Indirizzo di reindirizzamento** non è impostato un indirizzo o è specificato il valore `udp://`, il Server proxy Dr.Web cercherà di trovare il Server Dr.Web attraverso il servizio di rilevamento — inviando richieste broadcast (v. passaggio 9).



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

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

Nella tabella è possibile configurare le impostazioni di limitazione del traffico trasmesso analogamente alle impostazioni del Server Dr.Web, riportate nelle sezioni [Aggiornamenti](#) e [Installazioni](#).

5. Nella scheda **Cache** impostare i seguenti parametri di memorizzazione nella cache del Server proxy Dr.Web:

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

- Nel campo **Periodo di rimozione delle revisioni (min)** impostare la periodicità di rimozione delle vecchie revisioni dalla cache nel caso in cui il loro numero ha superato il numero massimo consentito di revisioni conservate. Il valore viene impostato in minuti. Di default è di 60 minuti.
 - Nel campo **Numero di revisioni conservate** impostare il numero massimo di revisioni di ciascun prodotto che rimarranno nella cache dopo una pulizia. Di default vengono conservate le ultime 3 revisioni, le revisioni più vecchie vengono rimosse.
- Nel campo **Periodo di scaricamento da memoria dei file non utilizzati (min)** impostare l'intervallo di tempo in minuti tra gli scaricamenti di file non utilizzati dalla memoria operativa. Di default è di 10 minuti.
- Spuntare il flag **Utilizza la memorizzazione in cache proattiva** per caricare sul Server proxy Dr.Web dal Server Dr.Web le nuove revisioni dei prodotti selezionati secondo il calendario sottostante. Durante questo periodo le revisioni vengono caricate sul Server proxy Dr.Web subito dopo la loro ricezione da parte del Server Dr.Web da SAM. Se il flag è deselezionato, il caricamento delle nuove revisioni sul Server proxy Dr.Web viene effettuato solo quando l'Agent Dr.Web richiede queste revisioni dal Server Dr.Web.
 - Nella lista sotto spuntare i flag per i prodotti per cui verrà eseguita la sincronizzazione.
 - Nella sezione **Calendario di sincronizzazione dei repository** impostare un calendario secondo cui verrà eseguito il caricamento degli aggiornamenti per i prodotti selezionati.

Per modificare la modalità di limitazione di trasmissione di dati, fare clic sul relativo blocco della tabella. Inoltre, è supportata la selezione di più blocchi di tempo tramite trascinarsi.

Il colore delle celle cambia ciclicamente secondo lo schema di colori riportato sotto la tabella: la trasmissione di dati è consentita senza alcune limitazioni al traffico o la trasmissione di dati è completamente proibita.



6. Nella scheda **Eventi** impostare i seguenti parametri di trasmissione di eventi:
 - Spuntare il flag **Memorizza eventi in cache** per memorizzare nella cache gli eventi ricevuti dagli Agent Dr.Web. In tale caso gli eventi verranno inviati sul Server Dr.Web ogni 15 minuti durante il periodo consentito per l'invio degli eventi nel calendario sottostante. Se la memorizzazione nella cache è disattivata, gli eventi verranno inviati sul Server Dr.Web subito dopo la loro ricezione da parte del Server proxy Dr.Web.
 - Nella sezione **Calendario di trasmissione degli eventi** impostare un calendario secondo cui verrà eseguita la trasmissione degli eventi ricevuti dagli Agent Dr.Web. Per modificare la modalità di limitazione di trasmissione di dati, fare clic sul relativo blocco della tabella. Inoltre, è supportata la selezione di più blocchi di tempo tramite trascinamento.
Il colore delle celle cambia ciclicamente secondo lo schema di colori riportato sotto la tabella: la trasmissione di eventi è consentita senza alcune limitazioni al traffico o la trasmissione di eventi è completamente proibita.
7. Nella scheda **Dump** impostare i seguenti parametri:
 - Spuntare il flag **Crea memory dump** per creare memory dump in caso di errori critici nel funzionamento del Server proxy Dr.Web.
 - Nel campo **Numero massimo di dump** impostare il numero massimo di memory dump. Quando viene raggiunto il numero impostato, i dump più vecchi verranno rimossi alla creazione di quelli nuovi. La configurazione dei memory dump è disponibile solo per SO Windows.
8. Nella scheda **DNS** vengono configurati i parametri di comunicazione con il server DNS. Le impostazioni sono analoghe alle [impostazioni DNS per il Server Dr.Web](#).
9. Nella scheda **Rilevamento** vengono configurati i parametri di conservazione delle risposte alle richieste broadcast durante la ricerca dei Server Dr.Web per il reindirizzamento dei client (vedi passaggio 4c).
 - **Per le risposte positive, s** — periodo di conservazione (in secondi) della lista dei Server Dr.Web che hanno risposto alla richiesta broadcast durante la ricerca dei Server Dr.Web. Dopo la scadenza del periodo impostato la richiesta viene inviata di nuovo.
 - **Per le risposte negative, s** — periodo di conservazione (in secondi) delle informazioni sulla mancanza di Server Dr.Web che hanno risposto alla richiesta broadcast. Dopo la scadenza del periodo impostato la richiesta viene inviata di nuovo.
10. Nella scheda **Aggiornamenti** vengono configurati i parametri di aggiornamento automatico del software Server proxy Dr.Web dal Server Dr.Web:
 - Spuntare il flag **Attiva l'aggiornamento automatico** per scaricare automaticamente dal Server Dr.Web e installare le nuove revisioni del Server proxy Dr.Web. Il calendario di aggiornamento dipende dalle impostazioni di memorizzazione in cache proattiva del Server proxy Dr.Web (v. passaggio 5):
 - a) Se il Server proxy Dr.Web non è incluso nella lista per la memorizzazione in cache proattiva (anche nel caso in cui la memorizzazione nella cache non viene utilizzata), gli aggiornamenti del Server proxy Dr.Web verranno scaricati e installati secondo il calendario di aggiornamento automatico.



- b) Se il Server proxy Dr.Web è incluso nella lista per la memorizzazione in cache proattiva, gli aggiornamenti del Server proxy Dr.Web verranno scaricati secondo il calendario di memorizzazione in cache proattiva. Nel caso di ricezione di una nuova revisione del Server proxy Dr.Web, l'aggiornamento a questa revisione avverrà secondo il calendario di aggiornamento automatico.
- Nella sezione **Calendario di aggiornamento** impostare un calendario secondo cui verrà eseguito l'aggiornamento automatico.
Per modificare la modalità di limitazione di trasmissione di dati, fare clic sul relativo blocco della tabella. Inoltre, è supportata la selezione di più blocchi di tempo tramite trascinamento.
Il colore delle celle cambia ciclicamente secondo lo schema di colori riportato sotto la tabella: la trasmissione di aggiornamenti è consentita senza limitazioni al traffico o la trasmissione di aggiornamenti è completamente proibita.
11. Nella scheda **Log** è possibile modificare il livello di dettaglio del log di Server proxy Dr.Web. Sono disponibili i seguenti livelli:
- **Errore critico** — messaggi di errori di funzionamento critici;
 - **Errore** — messaggi di errori di funzionamento;
 - **Avvertimento** — avvertimenti di errori;
 - **Avviso** — messaggi di informazione importanti;
 - **Informazione** — messaggi di informazione;
 - **Tracciamento (0-3)** — tracciamento delle azioni in corso con diversi gradi di dettaglio (**Tracciamento3** — livello di dettaglio massimo);
 - **Debug (0-3)** — messaggi di debug con diversi gradi di dettaglio (**Debug3** — livello di dettaglio massimo);
 - **Tutti** — tutti i messaggi (analogo al valore **Debug3**)
12. Dopo aver finito di modificare, premere **Salva**.

12.2. NAP Validator

Informazioni generali

Microsoft Network Access Protection (NAP) è una piattaforma di criteri, incorporata nei sistemi operativi Windows, che fornisce una maggiore sicurezza della rete. La sicurezza viene raggiunta attraverso la soddisfazione dei requisiti per l'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 adattare computer per renderli conformi ai requisiti stabiliti.



Una descrizione dettagliata della tecnologia NAP è disponibile sul [sito Microsoft Docs](#).

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 server di correzioni che assicura l'operatività del software antivirus delle postazioni.

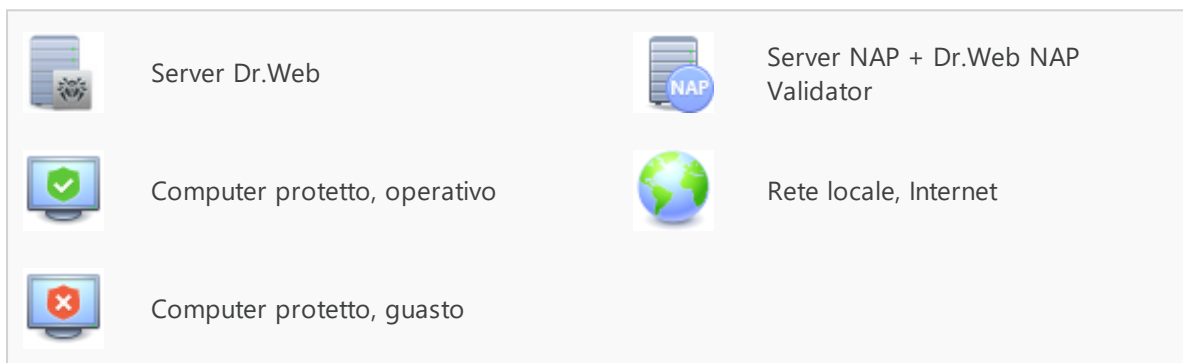


Immagine 12-2. Schema della rete antivirus con utilizzo di NAP

La procedura di controllo viene eseguita nel seguente modo:

1. L'attivazione del processo di controllo viene eseguita alla configurazione delle impostazioni corrispondenti 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 da esso stabilite 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 solo al Server Dr.Web e vengono isolate dal resto della rete. L'operatività della postazione viene ripristinata tramite il Server Dr.Web, dopodiché la procedura di controllo per la postazione viene rifatta.

Requisiti di operatività:

1. Stato operativo di Agent Dr.Web (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**, [Installazione di NAP Validator](#)) sul computer con il server NAP installato, è necessario eseguire le seguenti azioni:

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 degli 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

- Active Directory
 - autenticazione amministratore 105
 - informazioni generali 52
- Agent
 - aggiornamento 388
 - funzioni 63
 - modalità mobile 388
- aggiornamento
 - Agent 388
 - Dr.Web Enterprise Security Suite 375
 - forzato 378
 - manuale 378
 - modalità mobile 388
 - repository 378
 - secondo il calendario 379
- aggiornamento forzato 378
- aggiornamento manuale del repository 378
- amministratori
 - autenticazione 99
 - gestione 108
 - gruppi 108
 - permessi 110
- approvazione delle postazioni 153
- autenticazione
 - Active Directory 105
 - automatica 89
 - esterna 99
 - interna 100
 - LDAP 106
 - LDAP/AD 101
 - PAM 103
 - RADIUS 101
- autenticazione automatica 89
- avvio
 - Server Dr.Web, UNIX 62
 - Server Dr.Web, Windows 59
- avvisi
 - console web 313
 - impostazioni 306

B

- backup
 - Server, creazione 353
 - Server, ripristino 375

C

- calendario
 - degli aggiornamenti 379
 - delle postazioni 168
 - Server 278
- certificato 48
- chiave privata 48
- chiave pubblica 48
- chiavi
 - demo 26
 - di cifratura 48
 - di licenza 25
- chiavi demo 26
- chiavi di licenza
 - aggiornamento automatico 30
 - distribuzione tra i Server 27
 - gestione 176, 227
 - ottenimento 25
- cifratura
 - informazioni generali 41
- componenti
 - antivirus 179
 - di rete 95
- componenti antivirus 179
- compressione del traffico 41
- concessione delle licenze 25
 - caratteristiche 26
- configurazione
 - Server 248
 - web server 291
- controllo delle applicazioni 338
 - analisi funzionale 145
 - applicazioni affidabili 146, 342
 - modalità di divieto 151
 - modalità di permesso 146
 - modalità test 341
 - postazione modello 342
 - profili 141
 - prontuario applicazioni 346
 - regole di divieto 151
 - regole di permesso 146
- creazione
 - gruppo 128
- criteri
 - approvazioni delle postazioni 153



Indice analitico

criteri

impostazioni delle postazioni 138

D

directory di Server, contenuti, UNIX 60

directory di Server, contenuti, Windows 56

F

funzioni

Agent 63

Server 54

G

Gestione licenze 227

gruppi 124

aggiunzione di postazioni 131

impostazioni, copiatura 137

impostazioni, ereditarietà 121

primari 121

rimozione di postazioni 131

gruppi di sistema 124

gruppi predefiniti 124

gruppi primari 121

I

icone

procedure personalizzate 302

rete antivirus 73

impostazioni

delle postazioni, copiatura 137

Server 248

web server 291

interfaccia

Pannello di controllo 65

Server, UNIX 60

Server, Windows 56

L

lingua del Pannello di controllo 85, 114

loader di repository 381

log del Server 242

log di Server in tempo reale 238

M

messaggi

invio all'utente 213

log 247

modelli 305

modalità mobile dell'Agent 388

N

NAP Validator 399

impostazioni 402

nuovo arrivo 153

P

pacchetto 22

Pannello di controllo

barra degli strumenti 75

barra delle proprietà 81

descrizione 65

lista gerarchica 72

menu principale 66

permessi, amministratori 110

postazione 168

aggiunzione a gruppo 131

appartenenza al gruppo 134

approvazione 153

calendario 168

gestione 153

impostazioni, copiatura 137

impostazioni, ereditarietà 121

non confermata 153

nuovo arrivo 153

rimozione 155

rimozione da gruppo 131

ripristino 155

scansione 168, 183

statistiche 194

postazioni non confermate 153

privilegi, amministratori 110

protocollo SRV 41

Q

quarantena 206

R

registrazione

delle postazioni sul server 153

prodotto Dr.Web 25

relazioni tra i server

impostazione 361



Indice analitico

- relazioni tra i server
 - tipi 359
- repository
 - aggiornamento 378
 - configurazione dettagliata 328
 - configurazione generale 323
 - contenuti 334
 - stato 321, 378
- rete antivirus 358
 - componenti 95
 - configurazione delle relazioni 361
 - creazione 34
 - eventi di virus 368
 - struttura 95, 359
- rimozione
 - della postazione 155
 - gruppi 129
 - postazione, da gruppo 131
- ripristino
 - della postazione 155
 - password amministratore 116
- S**
- SAM
 - aggiornamento manuale 378
- scanner
 - antivirus 183
 - di rete 91
- scanner antivirus
 - avvio 185
- scansione
 - automatica 168
 - manuale 183
- scansione antivirus 183
- Scheduler
 - della postazione 168
 - Server 278
- Server Dr.Web
 - avvio, UNIX 62
 - avvio, Windows 59
 - calendario 278
 - configurazione delle relazioni 361
 - contenuti della directory, UNIX 60
 - contenuti della directory, Windows 56
 - funzioni 54
 - impostazioni 248
 - interfaccia, SO Windows 56
 - interfaccia, UNIX 60
 - log 242
 - log in tempo reale 238
 - tipi di relazioni 359
- Server proxy
 - avvio, arresto 394
 - configurazione in remoto 394
 - funzioni 390
- servizio di rilevamento Server 40
- statistiche
 - delle postazioni 194
 - Server 352
- T**
- traffico
 - cifratura 41
 - compressione 41
 - contenuti 97
- V**
- VDI 222
- W**
- web server 291
 - impostazioni 291

