Dr.WEB®
Enterprise Security Suite

Proteggi ciò che hai creato

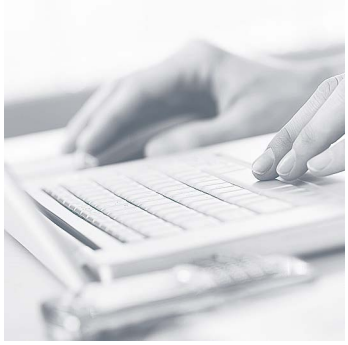
Dr.Web® Enterprise Security Suite

Guida rapida all'installazione e al deployment

Versione 6.0

Versione del software	6.0.4
Versione del documento	1.0
Data dell'ultima modifica	15 gennaio 2013

Sommario



1. Introduzione

Questo documento è una guida all'installazione e al deployment rapidi della soluzione antivirale Dr.Web Enterprise Security Suite (di seguito Dr.Web ESS) progettata per la protezione di postazioni e file server Windows, nonché del Pannello di controllo della rete antivirale.

In primo luogo, questo documento è pensato per gli utenti principianti di Dr.Web ESS. Ciononostante, si presume che l'utente che esegue il deployment di Dr.Web ESS nella rete aziendale sia un amministratore in possesso delle seguenti conoscenze:

- conoscenza di base della struttura dei calcolatori inclusi nella rete locale dell'azienda;
- buona conoscenza dei sistemi operativi e degli altri programmi utilizzati nella rete locale dell'azienda;
- conoscenza di base della gestione di reti locali;
- conoscenza delle particolarità della struttura e del funzionamento della rete locale in cui si vuole implementare una rete antivirale basata su Dr.Web ESS;
- buona conoscenza della struttura e del funzionamento dei componenti della suite antivirale Dr.Web per Windows (postazioni e server);
- conoscenza della lingua inglese a livello tecnico (desiderabile).

Questa guida non fornisce informazioni esaustive su Dr.Web ESS, è piuttosto un punto di partenza per cominciare l'implementazione di una rete antivirale completa nella rete locale dell'azienda.

Inoltre, il documento può essere usato per esercitazioni pratiche nei corsi messi a disposizione da Doctor Web per addetti alla sicurezza informatica aziendale.

2. Principali definizioni

Rete antivirale — rete locale aziendale in cui è installato, è configurato e funziona il software antivirale Dr.Web ESS (di seguito Rete antivirale).

Server antivirale — computer nella rete locale aziendale su cui è installato il software Dr.Web Enterprise Server (di seguito Enterprise Server). Il server antivirale coordina il funzionamento della rete antivirale. In una rete locale aziendale possono funzionare uno o più Enterprise Server.

Agent antivirale — componente di Dr.Web ESS installato su ogni oggetto protetto della rete. L'agent antivirale (di seguito Enterprise agent) riceve e invia tutte le informazioni necessarie per il funzionamento della rete antivirale, controlla l'esecuzione normale del software antivirale su ciascun oggetto protetto ed esegue task impostati dal server e dall'utente sull'oggetto protetto.

Pannello di controllo — componente di Dr.Web ESS che può essere utilizzato insieme ai web browser (Microsoft Internet Explorer 7 o superiore, Mozilla Firefox 3.0 o superiore, Opera, Safari o Chrome) su qualsiasi computer nella rete locale o fuori e che permette di svolgere le funzioni di amministrazione della rete antivirale (è possibile amministrare sia gli Enterprise server, che gli Enterprise agent). La disponibilità di uno di questi browser è necessaria e sufficiente; altro software non è richiesto.

Repository dell'Enterprise server — un deposito dei file sul disco locale del server che contiene tutti gli aggiornamenti dei programmi inclusi in Dr.Web ESS.

Amministratore della rete antivirale — dipendente dell'azienda, a cui appartiene la rete locale protetta, responsabile per il corretto funzionamento della rete antivirale.

3. Prima di installare

Prima di decidere di acquistare Dr.Web ESS, potete provare il software con una chiave di dimostrazione che può essere richiesta nell'apposita sezione del nostro sito ufficiale http://download.drweb.com/demo o direttamente nel corso dell'installazione del server antivirale.

Prima di effettuare il deployment della rete antivirale sulla base di Dr.Web ESS, si consiglia vivamente di provare la soluzione su un tratto piccolo della rete locale aziendale o utilizzando un software specializzato (per esempio, VMware — http://www.vmware.com).

La rete antivirale ha l'aspetto generale rappresentato sulla *figura 1*.

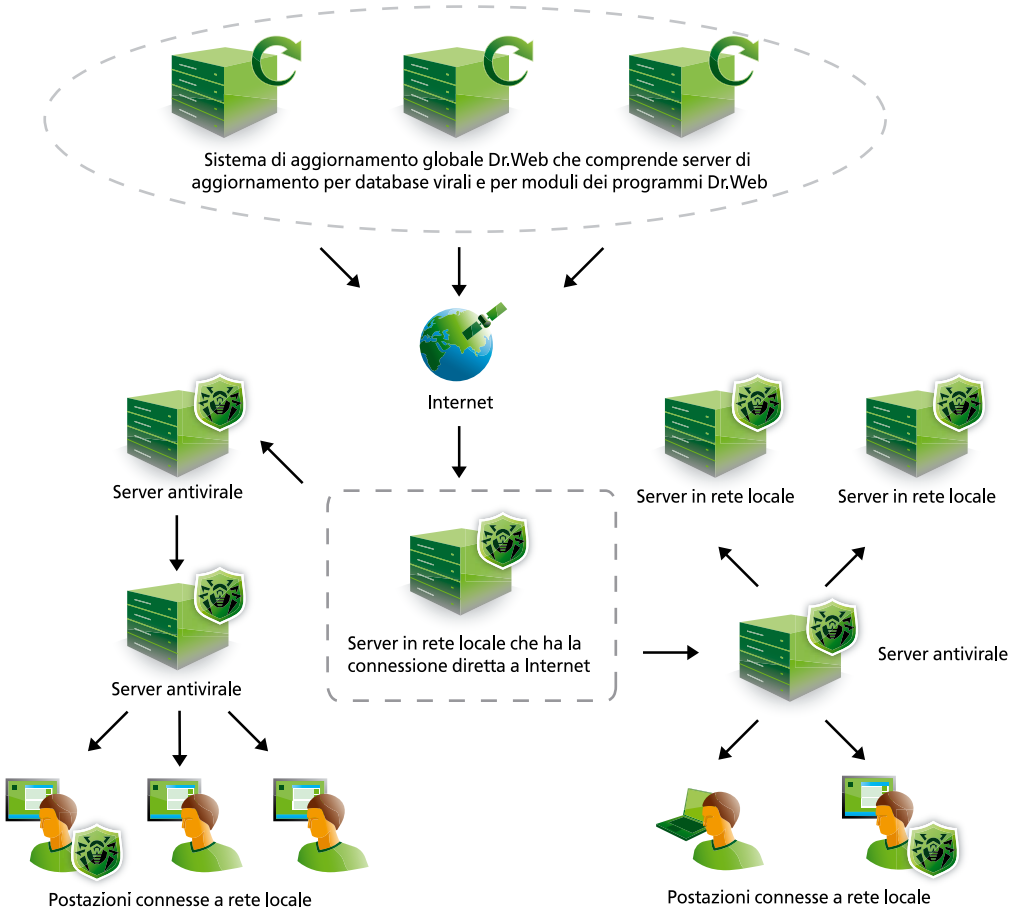


Figura 1. Schema generale della rete antivirale

Sulla *figura 1*, con le frecce è mostrato come le postazioni protette ricevono aggiornamenti dei database virali e dei moduli del software antivirale.

Pianificando la rete antivirale dovete decidere come disporre diversi componenti della rete antivirale sui computer della rete locale tenendo presente la topologia della rete locale. Le informazioni necessarie sono:

- numero e posizione degli Enterprise server;
- nodi protetti della rete antivirale;
- numero di computer protetti Windows Server 2000/2003/2008/2012 (è importante per ricevere chiavi di licenza corrette);
- tipo di database utilizzato dall'Enterprise server (database interno o esterno).

Dovete progettare la rete antivirale **prima** di acquistare il software Dr.Web ESS perché dal progetto della rete da attuare dipende maggiormente quali elementi devono essere inclusi nella licenza e quindi dipende il prezzo della licenza. Per determinare gli elementi da includere e il prezzo della licenza di Dr.Web ESS, si prendono in considerazione le seguenti informazioni:

- numero di Enterprise server nella rete;
- numero di oggetti protetti nella rete (compresi server);
- numero di Windows Server 2000/2003/2008/2012.

Queste informazioni devono essere comunicate al venditore della licenza al momento di acquisto di Dr.Web ESS.

Ciò quanti Enterprise server sono necessari per una rete antivirale dipende da più parametri, quali: velocità di trasferimento dati nella rete locale, topologia della rete, configurazione e carico dei server. Ciononostante, si ritiene che un Enterprise server installato su un Windows Server (se questo computer non svolge alcune altre funzioni nella rete locale) sia capace di coordinare fino a 300 Enterprise agent se utilizza il database interno. Se il database utilizzato è esterno, la quantità di Enterprise agent può aumentare diverse volte. In tale caso, la quantità di computer protetti dipende dalle capacità del concreto DBMS. È consigliabile installare gli Enterprise server sui computer che non svolgeranno altre funzioni nella rete locale o avranno un carico addizionale piccolo. Determinando il numero di postazioni protette, è necessario tenere presente che gli Enterprise agent si installano sia sulle postazioni, che sui server, e il software per le postazioni e quello per i server sono diversi. Se nel futuro immediato l'azienda pensa di ampliare la sua rete locale, si consiglia di acquistare in anticipo una licenza per un numero di computer maggiore rispetto a quello attuale.

Si deve tenere presente che:

- tra il computer dell'amministratore e l'Enterprise server deve esistere una connessione tramite il protocollo HTTP/HTTPS;
- tra gli Enterprise agent e l'Enterprise server deve esistere una connessione tramite uno dei seguenti protocolli: TCP/IP, IPX o NetBIOS.

È necessario determinare lo schema di aggiornamento della rete antivirale. Variante ideale è considerata la disponibilità nella rete locale di un Server proxy che gestisce l'accesso a Internet degli utenti e del software che necessita di tale accesso. Tuttavia, è possibile aggiornare la rete antivirale manualmente, anche se nessun computer della rete locale aziendale ha una connessione a Internet (le informazioni dettagliate sulle varianti di aggiornamento possibili sono riportate nel Manuale dell'amministratore).

È necessario tener conto dei requisiti di sistema minimi per gli Enterprise server e gli Enterprise agent.

Requisiti di sistema per gli Enterprise server: un computer con il processore non inferiore a Pentium III con la frequenza di 667 MHz, almeno 512 MB di RAM (1 GB se si usa il database interno), fino a 12 GB di spazio libero sul disco fisso: fino a 8 GB per il database incorporato (cartella di installazione), fino a 4 GB nella cartella temporanea di sistema (per file operativi); SO Windows 2000/XP/2003/Vista/7/2008/2012, Linux, FreeBSD o Solaris.

Requisiti di sistema per gli Enterprise agent: un computer con il processore non inferiore a Pentium IV con la frequenza di 1,6 GHz, almeno 512 MB di RAM, almeno 182 MB di spazio libero sul disco fisso per i file eseguibili + uno spazio addizionale per i log di funzionamento, SO Windows 98/Me/NT4/2000/XP/2003/Vista/7/2008.

Attenzione! Ai fini di sicurezza, prima di installare Dr.Web ESS, è necessario installare su tutti i computer (sia server antivirali, che postazioni protette) tutti gli aggiornamenti critici attuali dei sistemi operativi.

Prima di cominciare l'installazione e il deployment della rete antivirale basata su Dr.Web ESS nella rete locale aziendale, è necessario:

- accertarsi che si abbia la versione attuale del software Dr.Web ESS visitando la sezione corrispondente del sito ufficiale (http://download.drweb.com/esuite);
- scollegare la rete antivirale da Internet per prevenire penetrazioni dei virus da fuori nella rete locale durante l'installazione;
- rimuovere il software antivirus eventualmente installato in precedenza da ogni computer nella rete locale, compresi i prodotti Dr.Web per workstation e server Windows. Se i componenti di protezione installati in precedenza sono stati disinstallati parzialmente, dopo aver eseguito la disinstallazione con gli strumenti del sistema operativo, si consiglia di eseguire utility speciali, messe a disposizione dai produttori degli antivirus, sulle postazioni su cui si vuole installare il software Dr.Web ESS.

4. Deployment e configurazione della rete antivirale

Il deployment della rete antivirale include le seguenti fasi:

- installazione dell'Enterprise server;
- configurazione iniziale dell'Enterprise server;
- installazione degli Enterprise agent;
- configurazione delle postazioni protette;
- connessione di più Enterprise server (se necessario).

4.1. Installazione del software Enterprise server

Il software viene fornito in due varianti a seconda del sistema operativo in cui funziona l'Enterprise server:

1. Per i sistemi operativi della famiglia UNIX, vengono forniti archivi compressi del formato bzip2 o pacchetti di installazione appropriati dei seguenti componenti:
   - Dr.Web Enterprise Server,
   - Server proxy.
2. Per il sistema operativo Windows, vengono forniti file eseguibili della procedura guidata di installazione dei seguenti componenti:
   - Dr.Web Enterprise Server,
   - Server proxy,
   - Dr.Web Enterprise Agent per Active Directory,
   - NAP Validator.

Dr.Web ESS viene fornito in due varianti:

1. Variante completa che include tutti i prodotti aziendali da installare sulle postazioni gestite da tutti i SO supportati.
2. Variante leggera che include elementi analoghi a quelli delle versioni precedenti di Dr.Web ESS.

È adatta per installare la protezione antivirale Dr.Web ESS solo sulle postazioni Windows.

Il software Enterprise Server include i seguenti componenti:

- Dr.Web Enterprise Server per il SO corrispondente,
- Pannello di controllo Dr.Web,
- Dr.Web Enterprise Agent e pacchetti antivirali per i SO supportati,
- Database dei virus,
- Documentazione, template, esempi.

Insieme al software, possono essere forniti il file della chiave di licenza per il server e il file della chiave di licenza per l'agent.

4.1.1. Installazione dell'Enterprise server per Windows

La versione dell'Enterprise server per Windows viene fornita come un file eseguibile (utilizzato dalla Procedura guidata di installazione).

La versione attuale può essere scaricata da questo link: http://download.drweb.com/esuite.

La presente guida usa immagini catturate da schermo in Windows Server 2008 R2.

Il processo dell'installazione consiste dei seguenti passi:

1. Fare doppio clic sul file appropriato nell'Esplora risorse di Windows. Si apre una finestra in cui è necessario selezionare la lingua del processo di installazione. Di default, la lingua è quella della localizzazione del sistema operativo. Cliccare sul pulsante **OK** e attendere il caricamento della Procedura guidata di installazione.
2. Se nel sistema operativo è installato uno dei prodotti antivirali Dr.Web con il modulo di autoprotezione Dr.Web SelfPROtect, il programma di installazione informerà della necessità di disattivare temporaneamente l'autoprotezione. In questo caso, disattivare l'autoprotezione nel prodotto antivirale installato dopo di che cliccare sul pulsante **OK**.
3. Una volta caricata la Procedura guidata di installazione, si apre la finestra del benvenuto. Cliccare su **Avanti**.
4. Si apre una finestra con il testo del contratto di licenza. Per continuare l'installazione, è necessario accettare i termini del contratto di licenza. Nella parte inferiore della finestra selezionare **Accetto i termini del contratto di licenza** e cliccare su **Avanti**.
5. Si apre una finestra in cui si possono selezionare i file della chiave di licenza (*figura 2*).

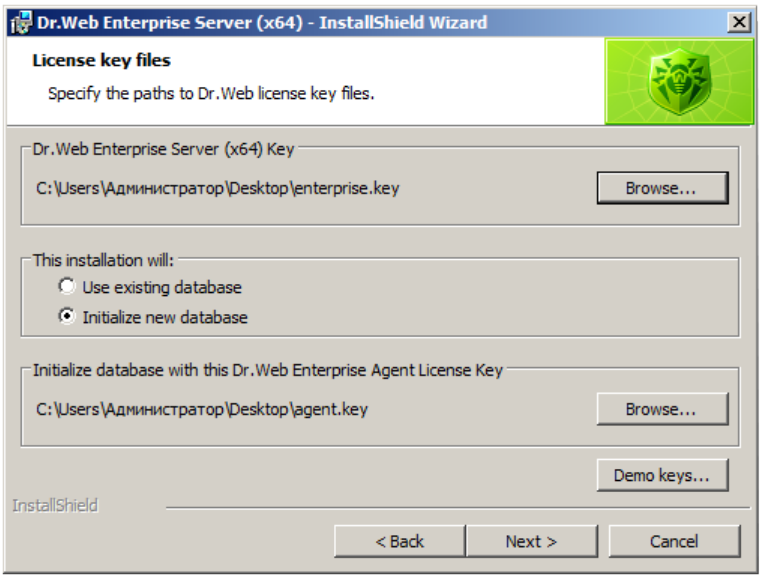


Figura 2. Selezionare i file della chiave di licenza

Nel campo **Chiave per Dr.Web Enterprise Server** cliccare su Sfoglia, poi nella finestra standard di Windows selezionare il file della chiave di licenza per il server `enterprise.key`.

Nello stesso modo, nel campo **Creare database utilizzando questa chiave per Dr.Web Enterprise Agent**, selezionare il file della chiave per il software per la postazione (agent e pacchetti di antivirus).

Selezionare l'opzione **L'installazione deve utilizzare: il database esistente**, se si vuole conservare il database del server di un'installazione precedente o l'opzione creare un database nuovo se è necessario un database nuovo. Di default, si crea un database nuovo.

Cliccare su **Avanti**.

6. Nella finestra **Tipo di installazione** scegliere una variante di installazione — **Completa** o **Personalizzata**. In caso dell'installazione completa, vengono installati tutti i componenti inclusi in Dr.Web ESS, e nella finestra successiva **Cartella di destinazione** sarà possibile selezionare una cartella per l'installazione. Di default, l'Enterprise server viene installato nella cartella `C:\Program Files \ DrWeb Enterprise Server`. In caso dell'installazione personalizzata, oltre alla cartella di destinazione sarà necessario scegliere quali componenti di Dr.Web ESS devono essere installati (*figura 3*).

Cliccare su **Avanti**.

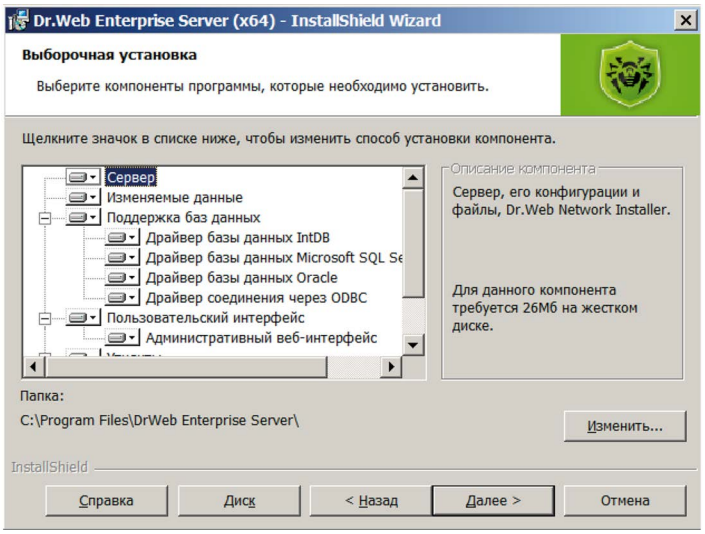


Figura 3. Installazione personalizzata

7. Nella finestra successiva (*figura 4*) è possibile:
   - scegliere la lingua dei template delle email (dall'elenco **Dr.Web Enterprise Server utilizzerà la lingua**);
   - impostare la modalità di uso e il nome della cartella di sistema condivisa in cui si installa l'agent (l'opzione **Condividere la cartella di installazione dell'agent**); si consiglia di mantenere le impostazioni predefinite (il flag è spuntato, il nome della cartella è `DRWESI$`);

Attenzione! *Se il server antivirale viene installato non su un sistema operativo per server, la cartella condivisa potrebbe non essere individuabile nella rete. In questo caso, si può copiare la cartella in un altro posto e condividerla manualmente.*

   - indicare se è necessario avviare il servizio Enterprise server durante l'installazione (il flag **Avviare il servizio durante l'installazione**);
   - indicare se è necessario aggiungere regole di eccezione per il firewall di Windows in modo da assicurare un funzionamento corretto dell'Enterprise server (il flag **Aggiungere alle eccezioni del firewall le porte e le interfacce del server**).

Si consiglia di mantenere le impostazioni predefinite in tutti i casi a parte dell'opzione lingua.

Cliccare su **Avanti**.

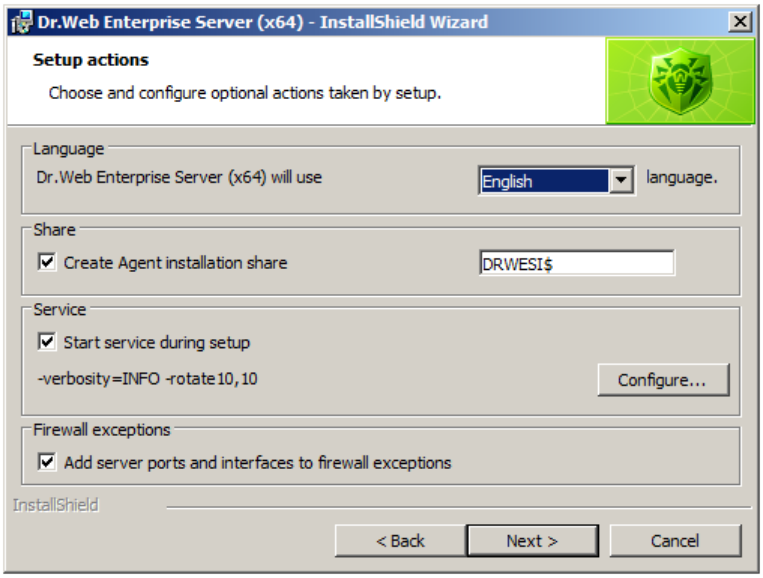


Figura 4. Configurare Dr.Web Enterprise Server

8. Si apre la finestra **Chiavi di crittografia per Dr.Web Enterprise Server** in cui si possono selezionare le chiavi esistenti di crittografia drwcsd.pub e drwcsd.pri, se rimaste dall'installazione precedente, affinché gli Enterprise agent già disponibili nella rete locale possano connettersi all'Enterprise server. Se l'Enterprise server viene installato per la prima volta, questo passo non è necessario. Cliccare su **Avanti**.
9. Nella finestra successiva **Scelta del driver del database**, si può selezionare il DBMS da utilizzare con l'Enterprise server (*figura 5*).

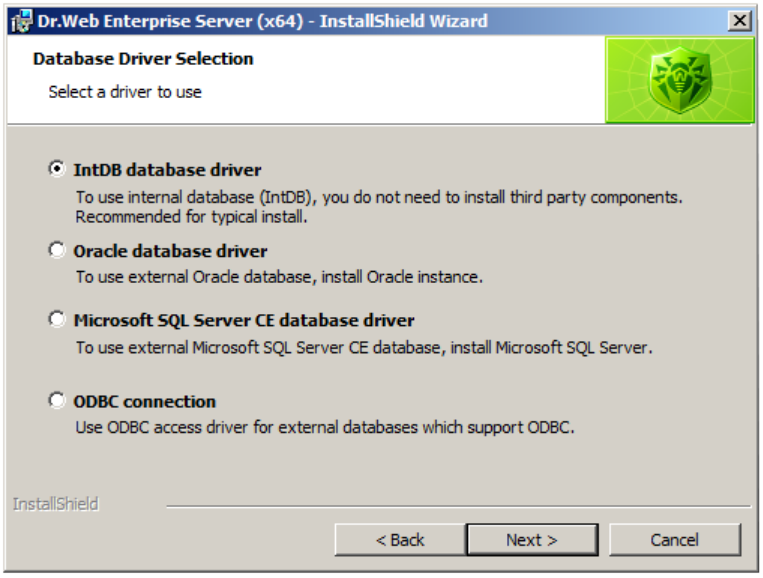


Figura 5. Finestra delle impostazioni del database

È possibile utilizzare sia il database interno dell'Enterprise server (Il driver del database è IntDB), che uno esterno. Come database esterni si possono utilizzare Oracle, Microsoft SQL Server CE, inoltre vengono supportati tutti i DBMS che interagiscono con ODBC. Se viene selezionato un database esterno, nella finestra successiva sarà necessario configurare l'accesso al database. Una volta compiuta la configurazione del database, cliccare sul pulsante Avanti.

Nota. *Una descrizione dettagliata di come creare e configurare database esterni si può leggere nella sezione 4.6 del presente documento. Se il software viene installato per la prima volta in una rete locale con meno di 200 postazioni, si consiglia di utilizzare il database interno.*

10. Si apre la finestra di configurazione rete per Dr.Web Enterprise Server (*figura 6*).

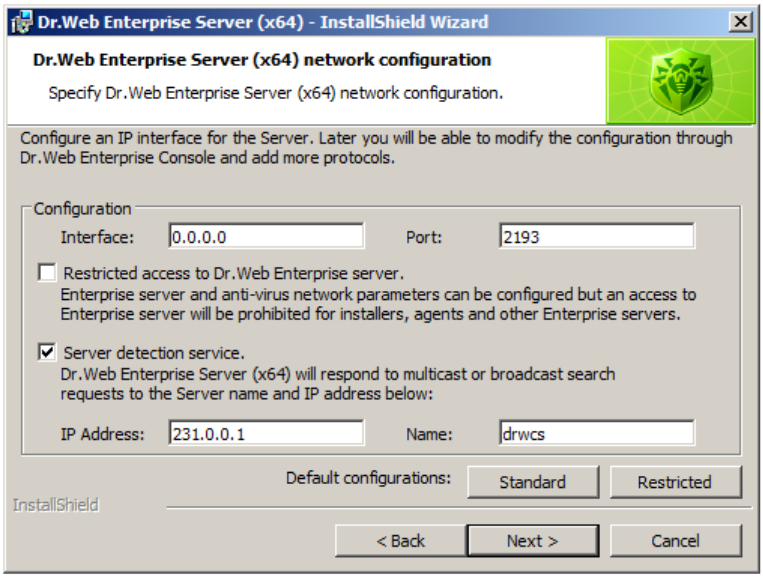


Figura 6. Configurazione delle interfacce di rete

In questa finestra è possibile configurare le interfacce di rete da essere utilizzate da parte dell'Enterprise server.

Nota. *Si consiglia di mantenere le impostazioni predefinite di questa scheda se si è appena cominciato a conoscere il prodotto Dr.Web Enterprise Security Suite.*

Dopo aver configurato questo passo, cliccare su **Avanti**.

11. Nella finestra **Configurazione del proxy e invio delle statistiche** (*figura 7*) è possibile decidere di inviare al server della società Doctor Web le informazioni statistiche raccolte dall'Enterprise server e inoltre definire i parametri del Server proxy per la connessione a Internet. Dopo aver configurato questo passo, cliccare sul pulsante **Avanti**.

Attenzione! *Analizzando le informazioni statistiche di rilevamento dei programmi malevoli la società Doctor Web può migliorare i suoi prodotti Dr.Web e le sue tecniche di rilevamento dei virus più moderni. Se l'utente accetta di inviare le informazioni statistiche alla società Doctor Web, contribuisce ad aumentare il grado di sicurezza procurata dal software Dr.Web e a lottare contro la criminalità informatica.*

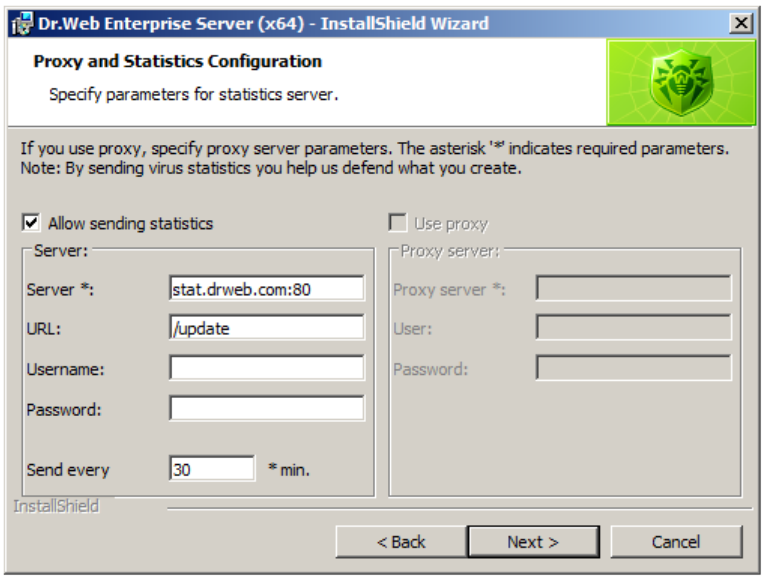


Figura 7. Invio delle statistiche e configurazione del Server proxy

12. Nella finestra **Password dell'amministratore** impostare la password dell'amministratore della rete antivirale. Poi cliccare sul pulsante **Avanti**.
13. Si apre una finestra in cui si può selezionare l'opzione **Aggiornare il repository** che permette al repository dell'Enterprise server di aggiornarsi automaticamente dopo la fine dell'installazione. Se quest'opzione è necessaria, spuntare il flag e poi cliccare sul pulsante **Avanti**.

Attenzione! *Se la banda è limitata, si consiglia di configurare l'aggiornamento del repository nella console web dopo l'installazione dell'Enterprise server e di aggiornare solo i componenti di protezione antivirale che si utilizzano effettivamente nella rete locale.*

14. A questo punto, si visualizza un messaggio che dice che la Procedura guidata di installazione dell'Enterprise server può cominciare l'installazione. Fare clic sul pulsante Installa.

Le azioni successive della Procedura guidata di installazione non richiedono alcuna partecipazione da parte dell'utente.

4.1.2. Installazione dell'Enterprise server per UNIX

Tutte le azioni necessarie per installare il software devono essere eseguite nella console a nome di superuser (root).

Per installare il server antivirale nei SO della famiglia UNIX, seguire le istruzioni qui sotto.

1. Per lanciare l'installazione del pacchetto drweb-esuite, eseguire il seguente comando:

   per FreeBSD: `pkg_add nome_file_software.tbz`

   per Solaris: `bzip2 -d nome_file_software.bz2`

   e quindi `pkgadd -d nome_file_software`

   per Linux:

   per Debian e Ubuntu: `dpkg -i nome_file_software.deb`

   per le distribuzioni RPM-based: `rpm -i nome_file_software.rpm`

Inoltre, esistono i cosiddetti pacchetti "generic" che possono essere installati su qualunque sistema, persino su uno che non rientra nella lista dei sistemi supportati ufficialmente. L'installazione si effettua mediante il programma di installazione incluso. Utilizzare il seguente comando:

```
tar -xjf nome_file_software.tar.bz2
```

In seguito, come superuser, eseguire lo script:

```
./drweb-esuite-install.sh
```

Nota. *Si può interrompere l'installazione del server in qualsiasi momento inviando al processo di installazione uno dei seguenti segnali:* `SIGHUP`, `SIGINT`, `SIGTERM`, `SIGQUIT` *e* `SIGWINCH` *(nel sistema operativo FreeBSD, una modifica della dimensione della finestra del terminale provoca l'invio del segnale* `SIGWINCH`*). Se il processo di installazione viene interrotto, le modifiche apportate al file system si ripristinano completamente allo stato prima dell'installazione. L'installazione di un pacchetto rpm può essere interrotta premendo i tasti* **CTRL + C**. *Il nome dell'amministratore della rete antivirale di default "admin".*

Premendo il tasto **ESC** nel corso dell'installazione, si può ritornare al passo precedente dell'installazione. Nello stesso tempo, al passo 2 (la prima finestra dell'installer che contiene il contratto di licenza), il tasto **ESC** interrompe il processo di installazione.

2. Le finestre successive (ciò quante finestre si visualizzano e in quale sequenza dipende dalla famiglia del sistema operativo) contengono le informazioni sul diritto d'autore e il testo del contratto di licenza. Per continuare l'installazione, è necessario accettare il contratto di licenza.
3. In seguito, si possono impostare il gruppo e l'utente a nome del quale funzionerà il software. Lo stesso utente sarà owner dei file del server antivirale.
4. Nelle due finestre successive, indicare il percorso completo ai file della chiave del server (`enterprise.key`) e dell'agent (`agent.key`).

Nota. *L'installazione in modalità console limita il numero di tentativi di impostare le chiavi (se è stato indicato un percorso non valido):*

- per il SO FreeBSD – `3 tentativi`;
- per il SO Solaris – `2 tentativi`.

Se il numero consentito di tentativi è stato superato e un percorso corretto alla chiave non è stato indicato, il funzionamento dell'installer si interrompe.

5. In seguito:

   - In caso di installazione nel SO Solaris: all'utente viene proposto di creare un nuovo database dell'Enterprise server. Se si sta eseguendo un aggiornamento dell'Enterprise server e si ha un database salvato, digitare "no", premere il tasto **INVIO** e indicare il percorso al file del database salvato.

   Se questa è la prima installazione dell'Enterprise server, premere il tasto **INVIO** e impostare la password dell'amministratore (utente "admin") che avrà l'accesso all'Enterprise server. Si può lasciare la password predefinita, cioè "root". Se viene impostata un'altra password, per motivi di sicurezza la password digitata non si visualizza sullo schermo in nessun modo. La password deve essere digitata due volte (se le stringhe digitate non sono uguali, si dovrà ripetere la procedura daccapo – seguire le istruzioni che appaiono). La password deve essere composta da almeno quattro caratteri.

   In seguito all'utente verrà chiesto di creare nuove chiavi di crittografia. Se si hanno chiavi salvate drwcsd.pri e drwcsd.pub, rifiutare di crearne nuove (digitare "no", premere **INVIO**) e indicare il percorso completo ai file esistenti. Se le chiavi non vi sono, premere **INVIO** per creare nuove chiavi di crittografia.

   - In caso di installazione tramite pacchetti deb: all'utente viene proposto di impostare la password dell'amministratore (utente "admin"). Si può lasciare la password predefinita, cioè "root". Se viene impostata un'altra password, per motivi di sicurezza la password digitata non si visualizza sullo schermo in nessun modo. La password deve essere digitata due volte (se le stringhe digitate non sono uguali, si dovrà ripetere la procedura daccapo – seguire le istruzioni che appaiono). La password deve essere composta da almeno quattro caratteri.
   - In altri casi: all'utente viene proposto di impostare la password dell'amministratore (utente "admin"). Quando viene impostata una password, per motivi di sicurezza la password digitata non si visualizza sullo schermo in nessun modo. La password deve essere digitata due volte (se le stringhe digitate non sono uguali, si dovrà ripetere la procedura daccapo – seguire le istruzioni che appaiono). La password deve essere composta da almeno otto caratteri.

Nota. *Nella password dell'amministratore non sono consentiti caratteri dell'alfabeto nazionale.*

6. Se è disponibile l'interprete perl, a seconda del sistema operativo, all'utente potrebbe essere chiesto di impostare alcuni parametri dell'Enterprise server. La richiesta di impostazione di un tipo di parametro prevede la variante "no" come predefinita (premendo il tasto **INVIO**), cioè per questi parametri verranno impostati i valori predefiniti. Se l'utente digita "yes", gli viene proposto di specificare i valori dei parametri (con questo, i valori predefiniti dei parametri sono riportati tra parentesi quadre e per accettarli, basta premere il tasto **INVIO**).

   La procedura di configurazione dell'Enterprise server può essere avviata anche manualmente (anche per questo è necessario che sia installato l'interprete perl). Per avviare la procedura di configurazione, lanciare lo script configure.pl che si trova nella:

   - directory `/usr/local/drwcs/bin/` in caso di FreeBSD,
   - directory `/opt/drwcs/bin/` in caso di Linux e Solaris.

7. In seguito, viene eseguita l'installazione del software durante la quale l'installer potrebbe richiedere conferme delle azioni a nome dell'amministratore.

   Nel corso dell'installazione del software in FreeBSD, si crea uno script `rc/usr/local/etc/rc.d/drwcsd.sh`. Per arrestare il server manualmente, usare il comando `/usr/local/etc/rc.d/drwcsd.sh stop`. Per avviare il server manualmente, usare il comando `/usr/local/etc/rc.d/drwcsd.sh start`.

   Nel corso dell'installazione dell'Enterprise server in Linux e Solaris, si crea uno script init da usare per l'avvio e per l'arresto del server `/etc/init.d/drwcsd`.

4.2. Configurazione iniziale dell'Enterprise server

La configurazione dell'Enterprise server può essere attuata in due modi: modificando il file di configurazione del server o modificando le impostazioni del server nel Pannello di controllo. La presente guida descrive solo la gestione del server mediante il Pannello di controllo

4.2.1. Avvio del Pannello di controllo e autorizzazione

Per avviare il Pannello di controllo, è necessario inserire nella barra indirizzi di uno dei browser supportati la stringa:

http://<Indirizzo_Server>:9080

o

https://<Indirizzo_Server>:9081

in cui per *<Indirizzo_Server>* indicare l'indirizzo IP o il nome di dominio del computer su cui è installato l'Enterprise server.

Si apre la finestra di registrazione sul server (*figura 8*).

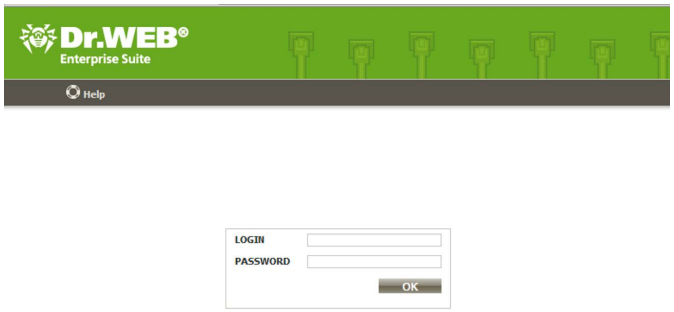


Figura 8. Registrazione sul server

Digitare il login e la password dell'amministratore del server (di default, si usa il login `admin`). Fare clic sul pulsante **OK**.

4.2.2. Finestra principale del Pannello di controllo

Se la registrazione sul server è riuscita, si apre la finestra principale del Pannello di controllo (*figura 9*). In questa finestra si visualizzano le informazioni sulla rete antivirale.

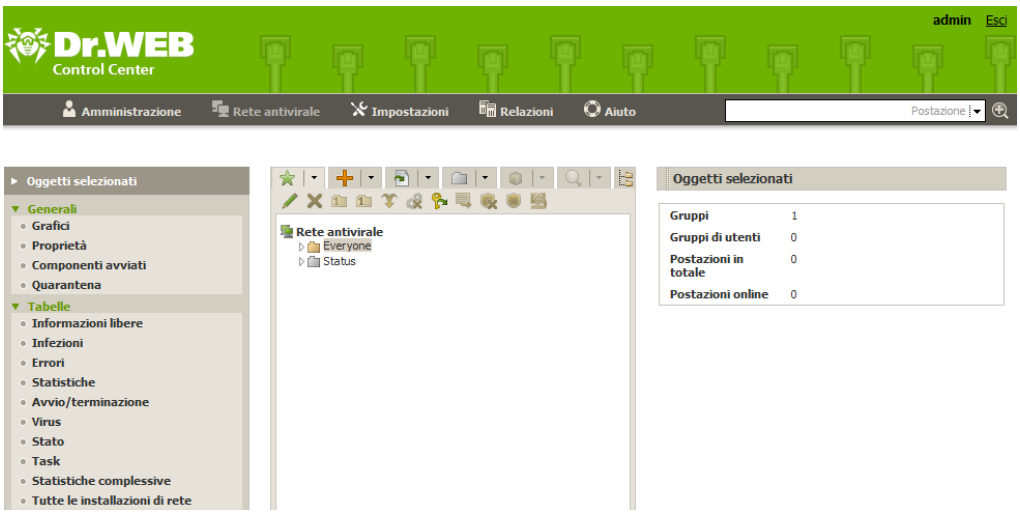


Figura 9. Finestra principale del Pannello di controllo

La finestra principale del Pannello di controllo include:

- una lista gerarchica (directory) della rete antivirale (parte centrale della finestra);
- un menu delle azioni che possono essere applicate alle postazioni e ai gruppi di postazioni nella rete antivirale (parte sinistra della finestra).

A seconda della voce selezionata dal menu di gestione, si visualizza un pannello aggiuntivo a destra. Il pannello contiene proprietà o impostazioni degli elementi della lista gerarchica della rete antivirale.

Sopra la directory della rete antivirale, si trova la barra degli strumenti. Per esempio, lo strumento **Importa chiave** permette di importare una nuova chiave da essere utilizzata da parte degli Enterprise agent.

4.2.3. Configurazione dell'aggiornamento del software antivirale

Attenzione! *Le raccomandazioni riportate in questo paragrafo devono essere attuate obbligatoriamente prima dell'installazione degli agent antivirali nella rete!*

Per configurare l'aggiornamento del software antivirale nel repository dell'Enterprise server, selezionare dalla sezione **Amministrazione** del Pannello di controllo la voce **Configurazione del repository**. Quindi selezionare la scheda **Sistema globale d'aggiornamento Dr.Web** (*figura 10*).

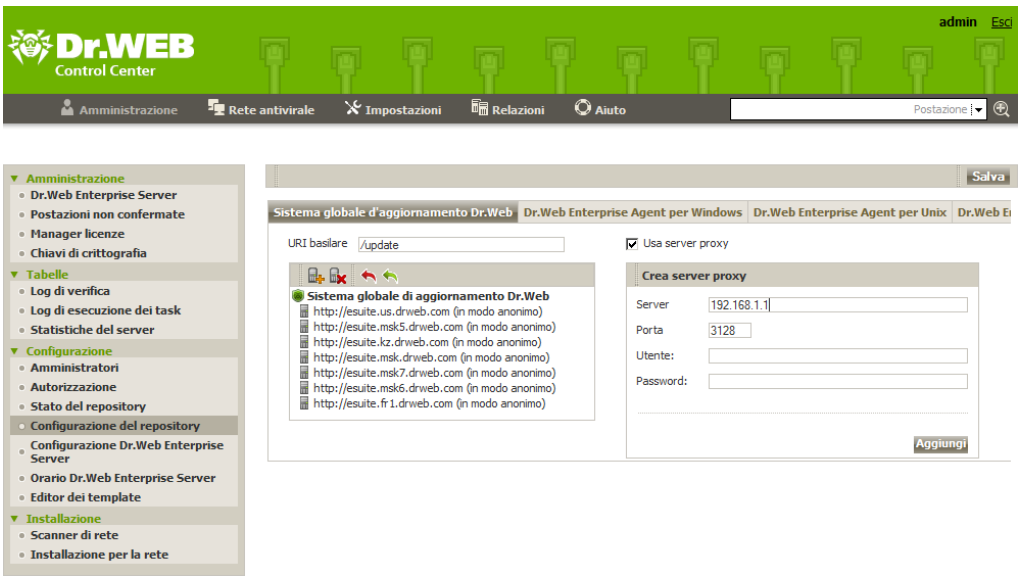


Figura 10. Sistema globale d'aggiornamento

Per impostare un Server proxy, è necessario spuntare il flag Usa server proxy. Appare un pannello in cui si può aggiungere un Server proxy impostando l'indirizzo e la porta del Server proxy e (se necessario) il nome utente e la password per l'autorizzazione sul Server proxy.

Si consiglia di mantenere inalterate le altre impostazioni nel gruppo Configurazione del repository.

Attenzione! *Le raccomandazioni riportate in questo paragrafo devono essere attuate obbligatoriamente prima dell'installazione degli agent antivirali nella rete!*

4.2.4. Aggiornamento del repository del server

Attenzione: *si consiglia vivamente di non saltare questo passo durante la configurazione di Dr.Web Enterprise Server!*

Per controllare se sul server vi siano aggiornamenti di qualche prodotto della famiglia Dr.Web Enterprise Security Suite, selezionare dalla sezione **Amministrazione** del Pannello di controllo la voce **Stato del repository** (*figura 11*). Quindi cliccare sul pulsante **Verifica aggiornamenti** e attendere fino a quando l'aggiornamento del repository non sarà completato.

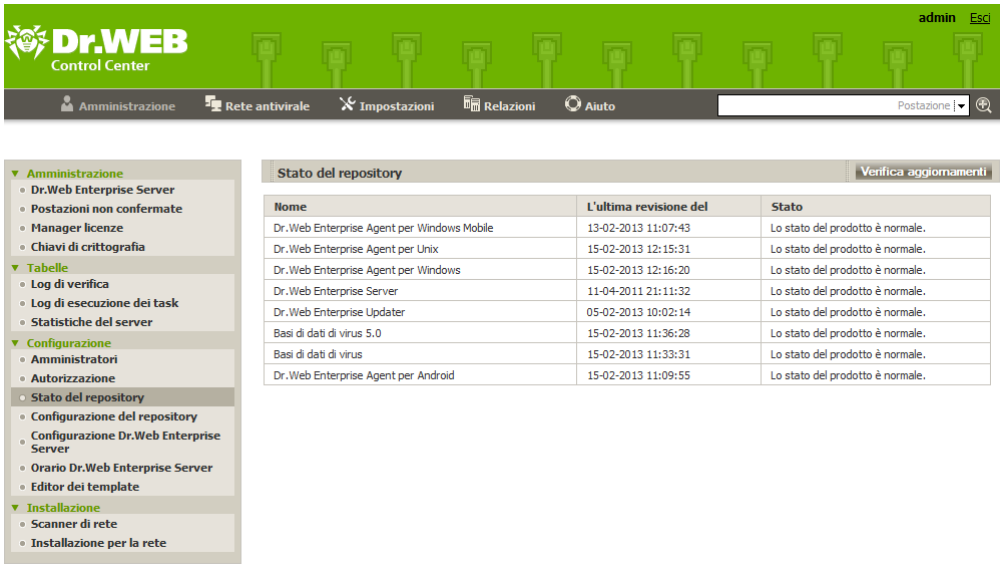


Figura 11. Verificare la disponibilità degli aggiornamenti

4.2.5. Configurazione del calendario del server

Subito dopo l'installazione del software Enterprise server, sul server si crea un calendario di task predefinito che probabilmente dovete modificare per adattarlo alle esigenze della Vostra azienda.

Il calendario può essere suddiviso in due parti essenziali: il calendario dell'Enterprise server e quello delle postazioni (o dei gruppi di postazioni).

4.2.5.1. Configurazione del calendario dell'Enterprise server

Per configurare il calendario dell'Enterprise server, selezionare nella sezione Amministrazione del Pannello di controllo la voce **Orario Dr.Web Enterprise Server** (*figura 12*). In seguito, viene visualizzato un elenco dei task attuali dell'Enterprise server.

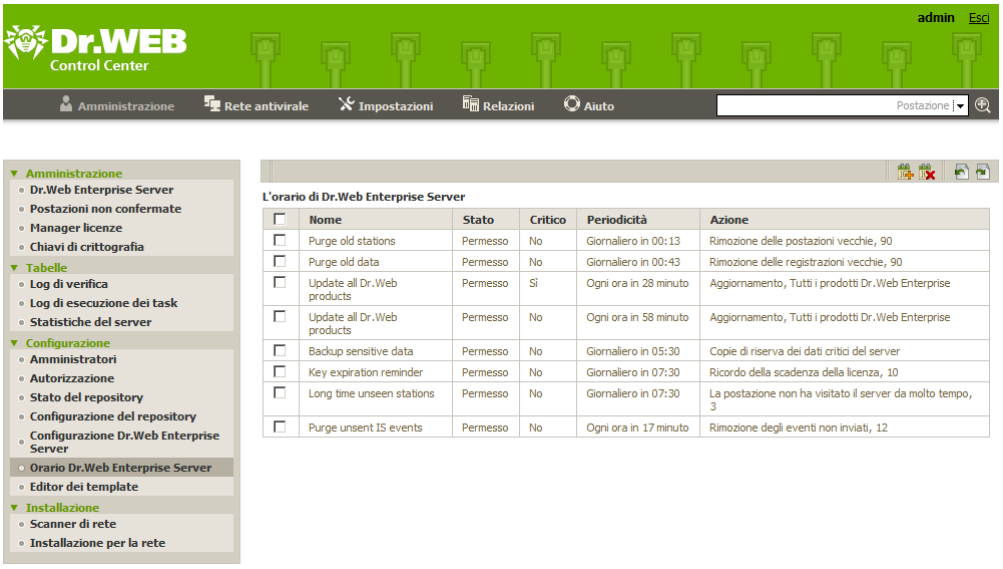


Figura 12. Calendario dell'Enterprise server

Per rimuovere un task dall'elenco, selezionarlo spuntando il flag corrispondente, dopo di che sulla barra degli strumenti cliccare sul pulsante **Rimuovi queste impostazioni**.

Per modificare parametri di un task, cliccare sul nome del task (che è un hyperlink). A questo punto si apre **l'Editor dei task** descritto più avanti.

Per aggiungere un task all'elenco, sulla barra degli strumenti cliccare sul pulsante Nuovo task. Si apre la sezione **Nuovo task**.

Quando viene creato un task nuovo o viene modificato uno esistente, si apre una finestra di inserimento dei parametri del task (la figura 13 mostra la finestra di inserimento paramenti per un task nuovo).

Figura 13. Aggiunzione di un task nuovo

Per modificare parametri del task, nella scheda **Generali**:

1. Nel campo **Nome** digitare il nome del task che verrà visualizzato nel calendario.
2. Tramite il flag **Permettere l'esecuzione**, stabilire se il nuovo task verrà eseguito.
3. Tramite il flag **Task critico**, stabilire se questo task sia critico per l'esecuzione.

Nella scheda **Azione** (*figura 14*), scegliere il tipo di task dal menu a discesa **Azione**. Con questo, cambierà l'aspetto della parte inferiore della finestra che contiene parametri di un task di questo tipo. Impostare questi parametri (più avanti i parametri dei tipi di task vengono descritti separatamente secondo i tipi).

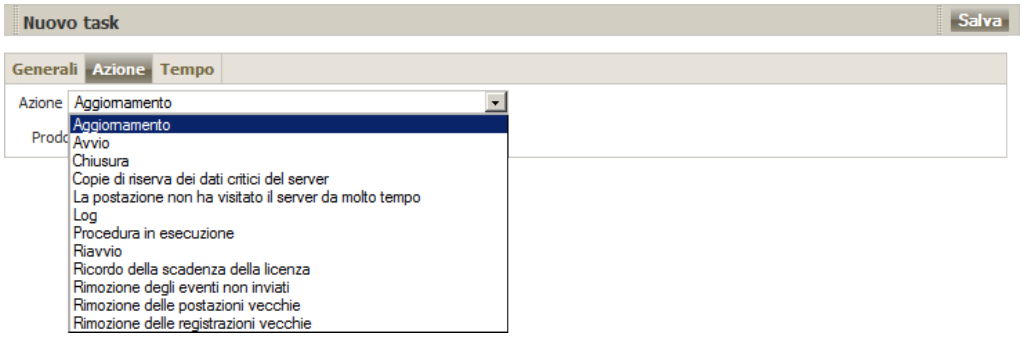


Figura 14. Scegliere il tipo di task

Nella scheda **Tempo** scegliere la periodicità e il tempo di avvio del task.

I task dei tipi **Chiusura** e **Riavvio** non hanno parametri.

Per impostare il tipo **Avvio**, nel campo **Percorso** immettere il percorso al file eseguibile del server e nel campo **Argomenti** immettere parametri dalla riga di comando all'avvio. Tramite il flag **Eseguire** in modo sincrono, definire il modo di esecuzione del task.

Per impostare il tipo **Log**, si deve immettere un messaggio da essere registrato nel log.

Per impostare i tipi **Rimozione delle postazioni vecchie** e **Rimozione delle registrazioni vecchie**, è necessario indicare un periodo dopo il quale le postazioni e le registrazioni sono riconosciute vecchie.

Per i task del tipo **La postazione non ha visitato il server da molto tempo**, è necessario indicare un periodo dopo il quale si considera che la postazione non abbia visitato il server da molto tempo.

I task del tipo **Copie di riserva dei dati critici del server** sono progettati per creare una copia di backup dei dati critici del server (quali database, file della chiave di licenza del server, chiave privata di cifratura). Si devono indicare il percorso alla directory in cui verranno salvati i dati (un percorso vuoto significa la directory predefinita) e il numero massimo di copie di backup (lo zero significa che questa limitazione è levata).

I task del tipo **Aggiornamento** sono progettati per gli aggiornamenti automatici del prodotto nel repository e hanno un singolo parametro: il nome del prodotto da aggiornare che si sceglie da un elenco a discesa.

4.2.5.2. Configurazione del calendario del gruppo Everyone

In Dr.Web ESS la protezione delle workstation può essere gestita tramite gruppi. Questa funzione consente di modificare impostazioni simultaneamente per tutte le postazioni che rientrano in un gruppo. Tutte le postazioni protette fanno parte del gruppo Everyone perciò tutte le workstation che si collegano alla rete antivirale ereditano automaticamente le impostazioni (compreso il calendario) di questo gruppo. Tutti i gruppi disponibili per la modifica si visualizzano nella finestra principale del Pannello di controllo. Per configurare il calendario del gruppo Everyone, è necessario selezionare questo gruppo dalla directory della rete antivirale e poi dal menu situato a sinistra selezionare la voce Orario (*figura 15*).

Figura 15. Calendario del gruppo Everyone

In questa finestra si possono modificare task esistenti e aggiungerne nuovi nel modo simile a quello che abbiamo descritto sopra (riguardante il calendario dell'Enterprise server).

Nel calendario del gruppo Everyone sono possibili quattro tipi di azione:

Dr.Web Enterprise Scanner per Windows — una scansione trasparente dal punto di vista degli utenti che cerca virus sulle workstation tramite Enterprise Scanner con la possibilità di configurare la scansione.

Dr.Web Scanner per Windows — la scansione sulle workstation viene eseguita dal prodotto Dr.Web Scanner per Windows, i parametri possibili sono argomenti dalla riga di comando per lo scanner.

Avvio — eseguire un'applicazione sulla workstation. I parametri possibili sono il percorso al file eseguibile e argomenti dalla riga di comando per l'applicazione da eseguire.

Log — inviare un messaggio al server. Il parametro è il messaggio da inviare (una stringa di testo).

4.3. Installazione degli Enterprise agent

Si consiglia vivamente di installare gli Enterprise agent solo dopo aver attuato tutte le raccomandazioni sopraindicate!

A questa fase è desiderabile (sebbene non obbligatorio) collegare alla rete locale tutti i computer che ci possono collegarsi.

4.3.1. Installazione degli Enterprise agent sulle postazioni protette

Gli agent possono essere installati sulle postazioni in tre modi:

- manualmente tramite l'installer di rete drwinst.exe (questo modo è adatto per la maggior parte di reti locali, ma il deployment della rete antivirale non è veloce in questo caso).

  Con questo metodo di installazione, possibile assicurare una protezione centralizzata ai computer con i sistemi operativi Windows XP Home Edition; Windows Vista Starter, Home Basic, Home Premium; Windows 7 Starter, Home Basic, Home Premium;

- su remoto utilizzando un browser e il Pannello di controllo (questo modo si usa spesso non solo al momento di deployment della rete antivirale, ma anche in seguito per amministrare Dr.Web ESS);
- utilizzando le possibilità di Active Directory.

I primi due metodi sono descritti più avanti.

Per installare il software tramite questi metodi, è necessario condividere sul server la directory `%DrWeb_ES%\Installer` (di default, nel SO Windows è la directory *C:\Program Files\DrWeb Enterprise Server\Installer*, il suo nome di rete predefinito è `DRWESI$`) che contiene due file: `drwcsd.pub` e `drwinst.exe`. Questa cartella e questi file vengono generati automaticamente durante l'installazione dell'Enterprise server.

4.3.1.1. Installazione manuale degli Enterprise agent tramite l'installer di rete

L'amministratore della rete antivirale deve connettersi manualmente (o mediante il programma di amministrazione remota) a ciascuna postazione protetta utilizzando i permessi dell'amministratore locale, deve collegare la sopraindicata cartella condivisa come unità di rete e avviare il programma `drwinst.exe`. Se necessario, potete utilizzare alcune delle chiavi di avvio per questo programma di installazione. In particolare, è utile il seguente parametro dalla riga di comando:

`-interactive` — avvio della procedura guidata di installazione dell'Enterprise agent. All'inizio, la procedura guidata chiede di confermare che sul computer non è installato un altro software antivirale. Quindi si deve scegliere una delle varianti di installazione dell'Enterprise agent — installazione rapida, personalizzata o amministrativa. A differenza dell'installazione rapida, l'installazione personalizzata consente di selezionare i componenti del

software antivirale da installare, mentre nella variante amministrativa si possono scegliere il nome o l'indirizzo IP del server antivirale e la posizione della chiave pubblica degli Enterprise agent, si possono impostare la password di accesso al server e la modalità di compressione e di cifratura dei dati trasmessi tra il server e l'agent.

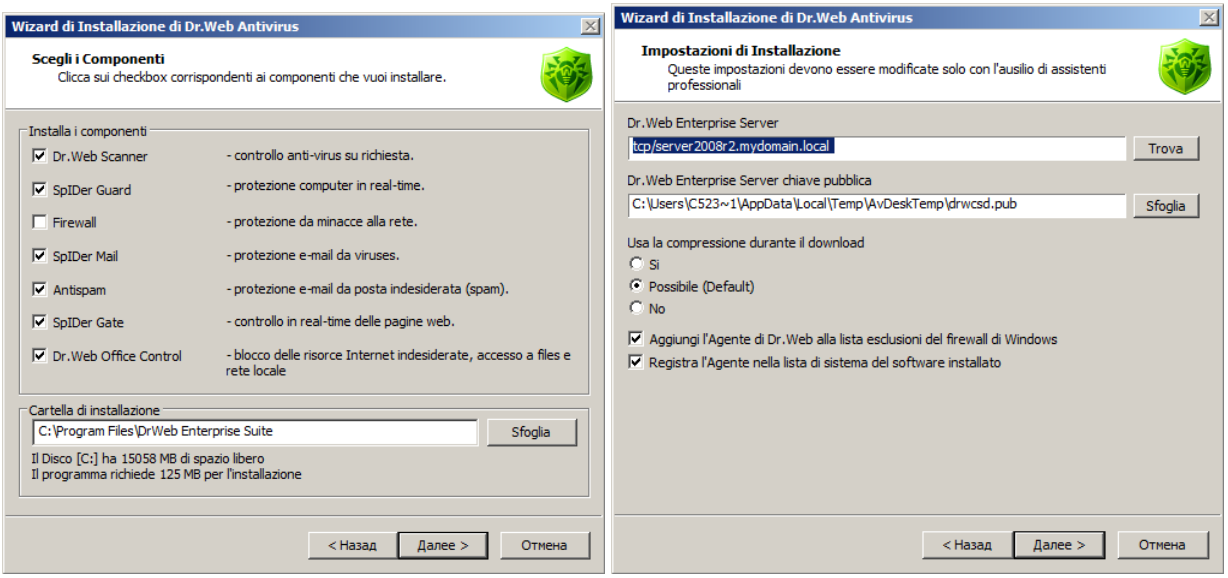


Figura 16. Interfaccia della procedura guidata di installazione dell'Enterprise agent

Qualche minuto dopo la fine dell'installazione preparatoria, l'Enterprise agent verrà installato sulla postazione. Questo processo potrebbe richiedere alcuni minuti a seconda del carico della rete e delle prestazioni del computer. In seguito, appare un avviso della necessità di riavviare il computer. Dopo il riavvio della postazione, l'Enterprise agent funzionerà in maniera regolare.

4.3.1.2. Installazione degli Enterprise agent attraverso la rete

Per l'installazione remota degli Enterprise agent, è necessario installare Dr.Web Browser-Plugin.

Per installare su remoto gli Enterprise agent, l'amministratore della rete antivirale deve avviare il Pannello di controllo, poi deve connettersi all'Enterprise server (v. punti 4.2.1 e 4.2.2) e andare alla sezione **Amministrazione**, in cui è necessario selezionare la voce **Installazione per la rete**.

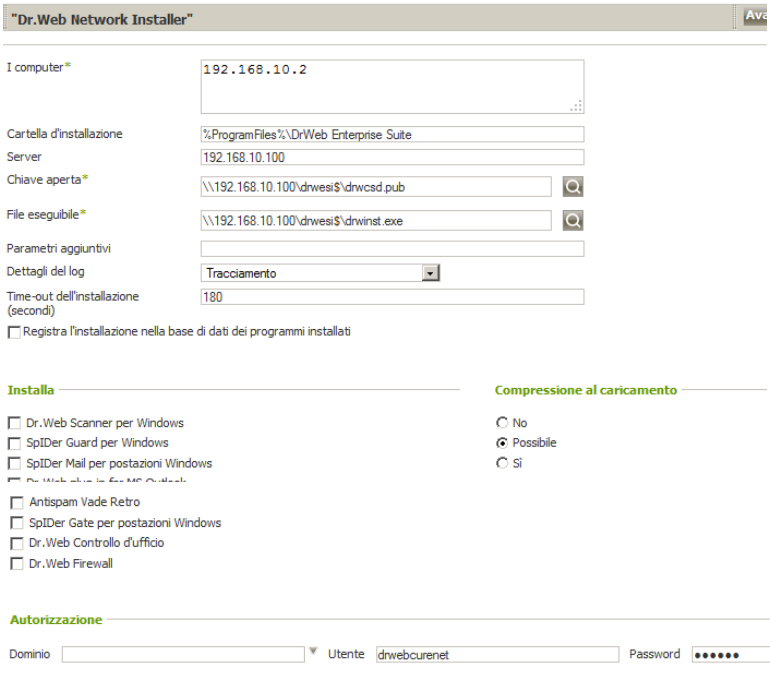


Figura 17. Installazione degli Enterprise agent attraverso la rete. Parametri dell'installazione

Nel modulo **Dr.Web Network Installer** che si è aperto, specificare i parametri desiderati dell'installazione remota.

In particolare, nel campo **I computer** è necessario elencare i nomi, gli indirizzi IP o gli intervalli di indirizzi IP dei computer su cui si vuole eseguire l'installazione. Nel campo **Server** è necessario immettere il nome o l'indirizzo IP dell'Enterprise server a cui aderiranno gli Enterprise agent una volta installati. Nei campi **Chiave pubblica** e **File eseguibile** è necessario indicare il percorso alla chiave pubblica `drwcsd.pub` e il percorso al file eseguibile dell'installer di rete dell'Enterprise agent. Nel gruppo di impostazioni **Installa** è necessario selezionare i componenti del software antivirale da installare. A questo punto, tenete presente che non potete selezionare componenti non supportati dalla licenza di uso Dr.Web acquistata. Nel gruppo di impostazioni **Autorizzazione** è necessario selezionare il dominio a cui appartengono i calcolatori su cui si installeranno gli Enterprise agent e inoltre è necessario immettere le credenziali dell'utente che ha poteri dell'amministratore locale su questi calcolatori. Nel gruppo di impostazioni **Compressione** è necessario scegliere la modalità di compressione dei dati trasmessi tra l'installer di rete e l'Enterprise server. Dopo che sono stati specificati i parametri dell'installazione degli Enterprise agent, cliccare sul pulsante **Avanti**.

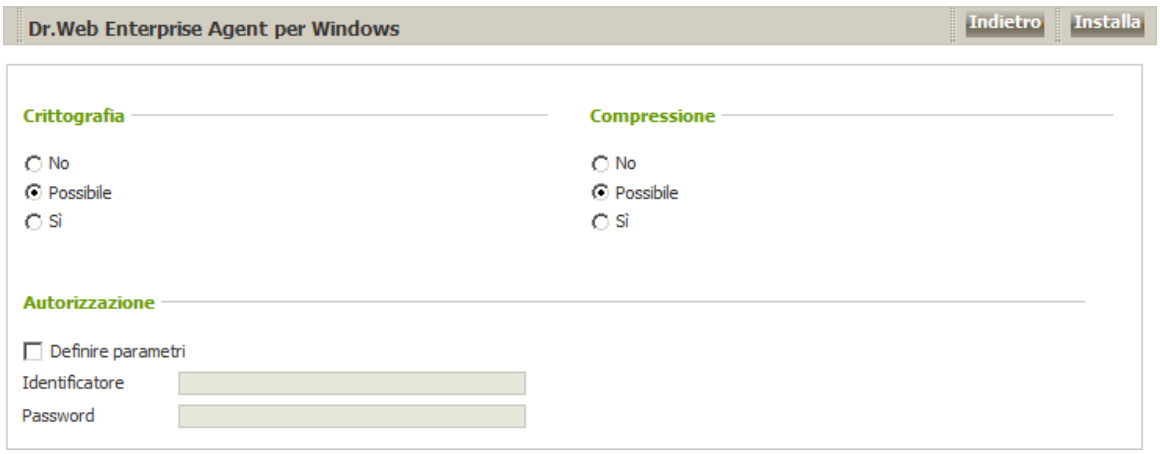


Figura 18. Installazione degli Enterprise agent tramite la rete. Parametri degli Enterprise agent

Nel modulo comparso, si possono impostare le credenziali per l'autorizzazione dell'Enterprise agent sull'Enterprise server, nonché la modalità di cifratura e di compressione dei dati trasmessi tra l'agent antivirale e il server antivirale. Selezionate le opzioni desiderate e cliccare su **Installa**.

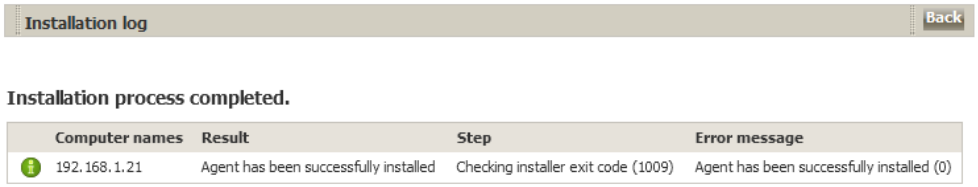


Figura 19. Log dell'installazione remota degli Enterprise agent

Nella finestra Log dell'installazione si visualizza il progresso e il risultato dell'installazione degli Enterprise agent sui computer selezionati.

In seguito, selezionare dal menu a sinistra la voce Postazioni non confermate, quindi segnare le postazioni su cui è stata eseguita l'installazione e fare clic sull'icona  o  .

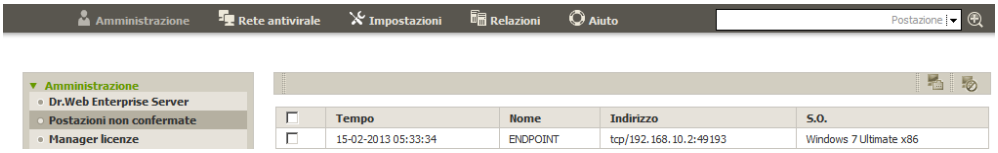


Figura 20. Selezionare postazioni su cui è stata eseguita l'installazione

Se viene cliccata l'icona  , si apre una finestra in cui si può scegliere il gruppo primario.

Figura 21. Scelta del gruppo primario

Attenzione! *Durante l'installazione, i prodotti antivirus trovati sui computer vengono eliminati automaticamente. Una lista dei prodotti antivirus che possono essere eliminati in maniera automatica è riportata nella documentazione.*

4.3.1.3. Installazione dell'agent tramite il servizio Active Directory

Se nella Vostra rete locale si usa il servizio Active Directory, potete installare l'agent antivirale sulle postazioni su remoto tramite questo servizio. In questa descrizione facciamo un esempio di configurazione per Windows Server 2008 R2. Nelle altre versioni dei SO Microsoft Windows Server, la procedura potrebbe essere diversa.

Procedura dell'installazione:

1. Scaricare dal sito http://www.drweb.com l'installer dell'agent antivirale per le reti con Active Directory (di seguito installer di Dr.Web Enterprise Agent) (`drweb-esuite-agent-6xx-xxxxxxxx-activedirectory.msi`, dove le cifre `6xx-xxxxxxxx` dipendono dal numero della versione corrente di Dr.Web ESS e possono cambiare).
2. Avviare l'installer in modalità grafica:

   ```
   msiexec /a <percorso all'installer>\drweb-esuite-agent-5xx-xxxxxxxx- activedirectory.msi
   ```

3. Si apre la finestra del benvenuto di Dr.Web Enterprise Agent. Cliccare su **Avanti**.

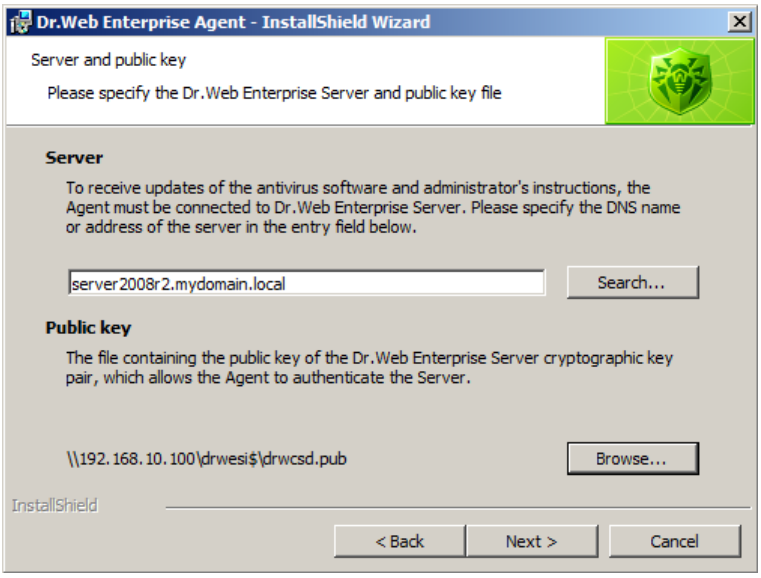


Figura 22. Server e chiave pubblica

4. Nella finestra **Server e chiave pubblica**, nel campo **Server** inserire il nome DNS (il nome del server e il dominio a cui appartiene il server) o l'indirizzo IP dell'Enterprise server a cui si connetteranno gli Enterprise agent da installare. Nel campo **Chiave pubblica**, è necessario indicare il percorso alla chiave pubblica dell'Enterprise server specificato nel campo **Server** utilizzando la funzione di ricerca disponibile attraverso il pulsante **Sfoglia**. Cliccare su **Avanti.**
5. Creare sul server una cartella in cui si registrerà l'immagine dell'Enterprise agent. Per esempio, sarà la cartella `C:\DrWebESAgent` situata sul server `WIN2008`. Condividere questa cartella per renderla accessibile attraverso la rete a tutti i computer nel dominio. Nel nostro esempio, la risorsa condivisa può avere il nome: `\\WIN\DrWebESAgent`.

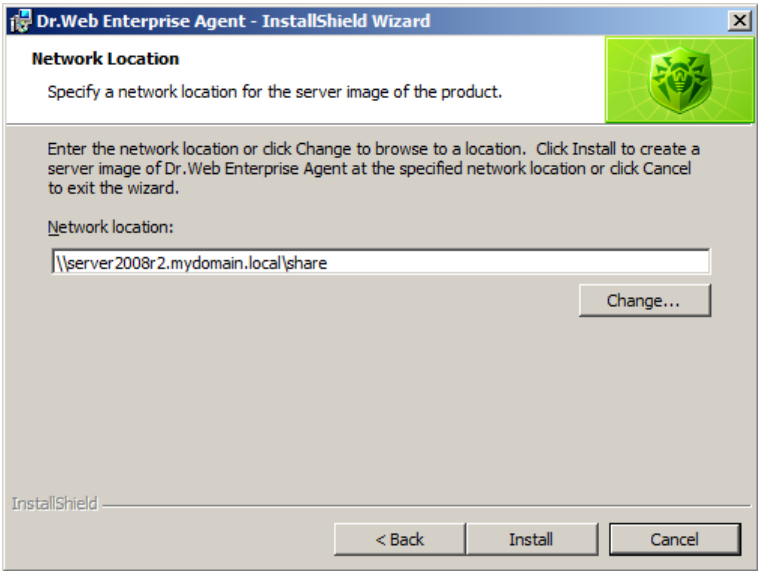


Figura 23. Cartella condivisa

6. Nella finestra **Cartella condivisa** dell'installer di Dr.Web Enterprise Agent, è necessario indicare la cartella condivisa creata nel punto 5. Si può trovarla tramite la funzione di ricerca cliccando sul pulsante **Cambia**. Quindi cliccare su **Installa**.
7. L'installer di Dr.Web Enterprise Agent comunica di aver completato la procedura di installazione. Cliccare su Fine.

8. Cliccare su **Start — Amministrazione — Active Directory — Utenti e computer**.

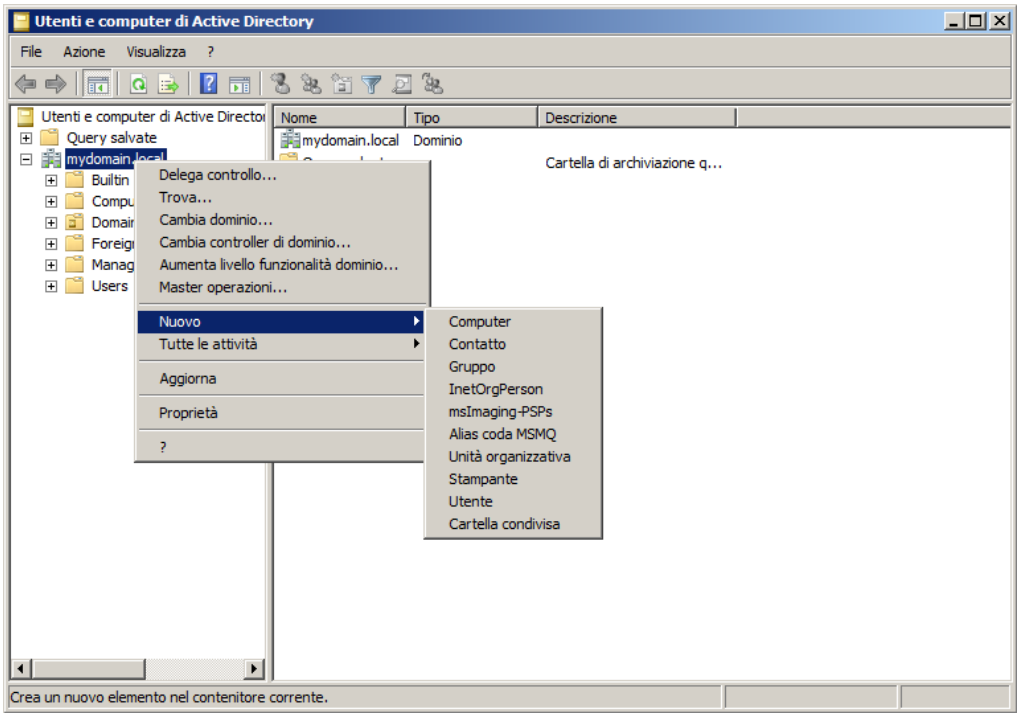


Figura 24. Creare un'unità organizzativa

9. Nel dominio dei computer su cui si vuole eseguire l'installazione degli Enterprise agent, creare una nuova **Unità organizzativa** con il nome, per esempio, **ESS**. A questo scopo, dal menu contestuale del dominio selezionare **Nuovo — Unità organizzativa**.
10. Nella finestra apparsa **Nuovo oggetto — Unità organizzativa**, digitare il nome della nuova unità organizzativa (per esempio, ES) e cliccare su **OK**. Includere nell'unità organizzativa creata i computer su cui si vuole installare l'Agent.
11. Aprire la finestra di modifica dei criteri di gruppo: cliccare su **Start — Amministrazione — Gestione Criteri di gruppo** (in Windows 2000/2003 Server: dal menu contestuale dell'unità creata ESS selezionare la voce **Proprietà**. Nella finestra delle proprietà, passare alla scheda **Criteri di gruppo**).

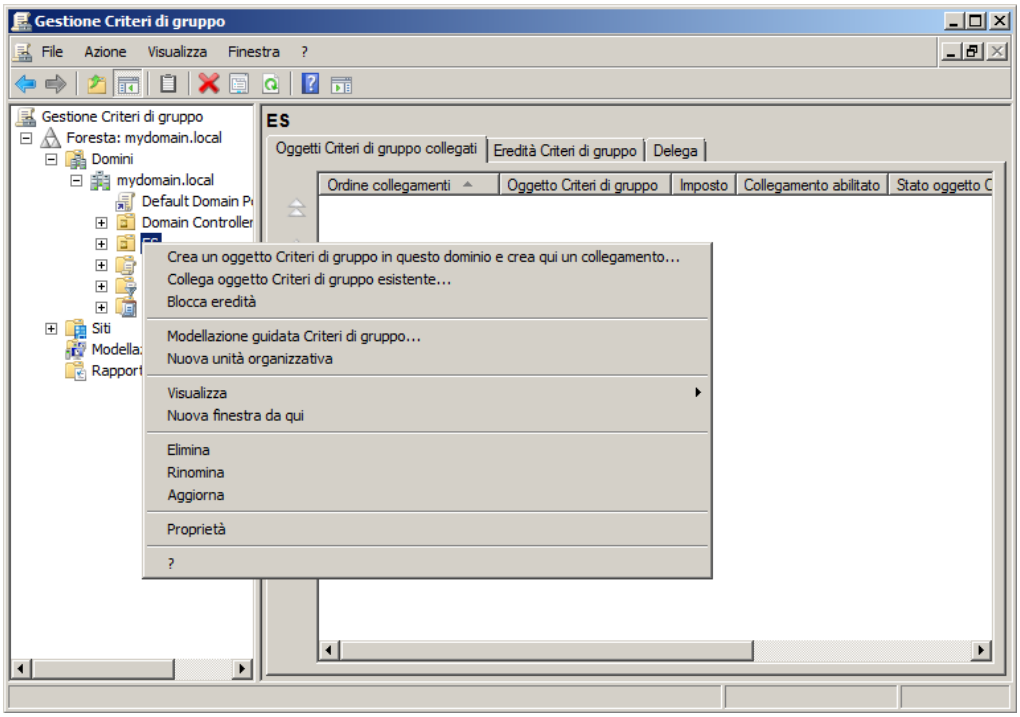


Figura 25. Gestione Criteri di gruppo

12. Dal menu contestuale dell'unità organizzativa creata nel punto 10 sopra, selezionare la voce **Crea un oggetto Criteri di gruppo in questo dominio e crea qui un collegamento**. Nella finestra **Nuovo oggetto Criteri di gruppo**, è necessario digitare il nome del nuovo oggetto Criteri di gruppo (per esempio, `Criteri di gruppo ES`) (in Windows 2000/2003 Server: cliccare sul pulsante **Aggiungi** e creare un elemento dell'elenco con il nome Criteri di gruppo **ESS**) e poi fare clic su **OK**.
13. Dal menu contestuale dei Criteri di gruppo creati, selezionare la voce **Modifica**.

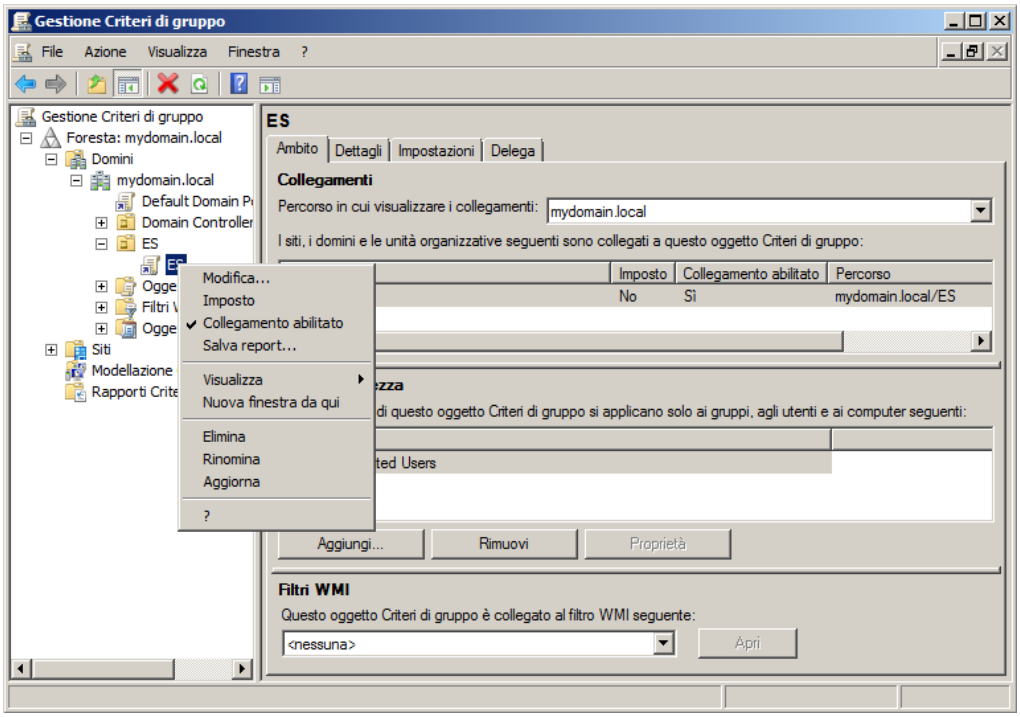


Figura 26. Modificare i criteri di gruppo creati

14. Nella finestra **Editor Gestione Criteri di gruppo**, è possibile configurare i Criteri di gruppo creati nel punto 12. Per fare questo, dall'elenco gerarchico è necessario selezionare l'elemento **Configurazione computer — Criteri — Impostazioni del software — Installazione software** (in Windows 2000/2003 Server: **Configurazione computer — Impostazioni del software — Installazione software**), e dal menu contestuale di questo elemento selezionare la voce **Nuovo — Pacchetto**.

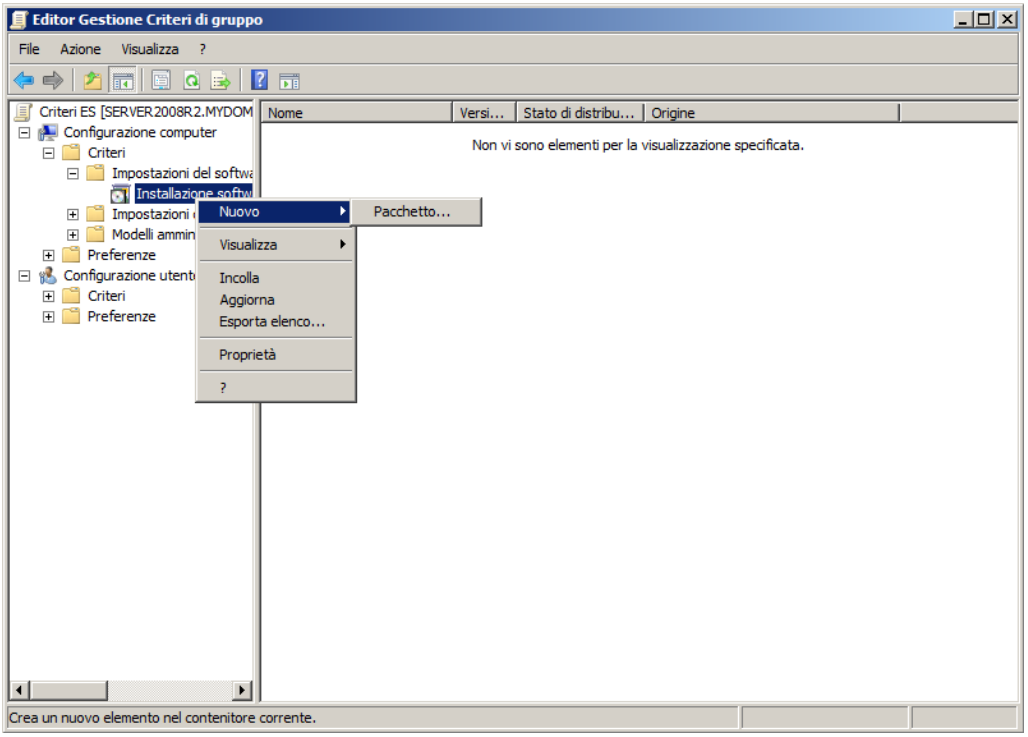


Figura 27. Editor Gestione Criteri di gruppo

15. Nella finestra apparsa **Apri**, nella barra degli indirizzi (il campo in alto della finestra), è necessario immettere l'indirizzo della cartella condivisa creata nel punto 5 e premere il tasto **INVIO**. Nella tabella della parte principale della finestra, è necessario selezionare la stringa `drweb-esuite-agent-600-200905310-activedirectory` e poi fare clic sul pulsante **Apri**. In seguito, si apre la finestra **Distribuire software**, dove è necessario scegliere **assegnato** e cliccare su **OK**.

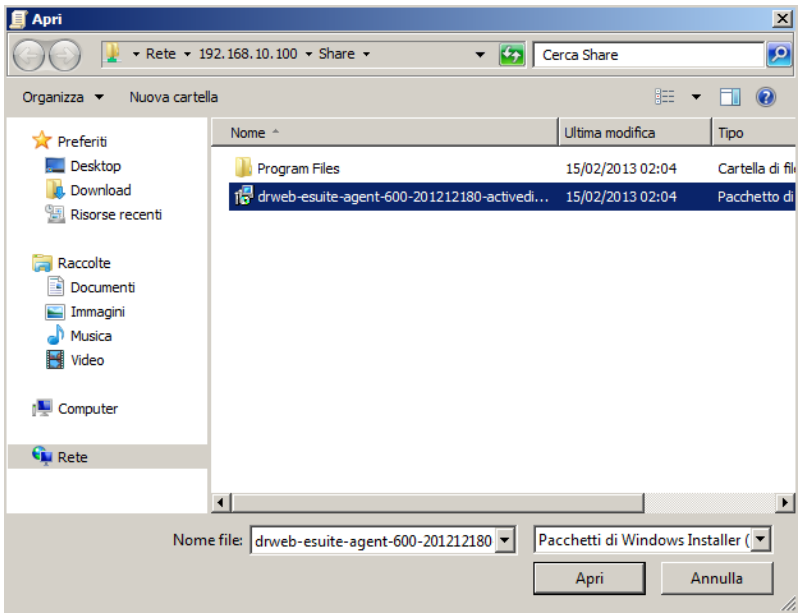


Figura 28. Indicare il posto dove è memorizzato Dr.Web Enterprise Agent

16. Nella finestra **Editor Gestione Criteri di gruppo** appare la stringa `Dr.Web Enterprise Agent`. Dal menu contestuale di questa stringa selezionare la voce **Proprietà**. Si apre la finestra **Proprietà: Dr.Web Enterprise Agent**. Passare alla scheda **Distribuzione** e fare clic sul pulsante **Avanzate**.

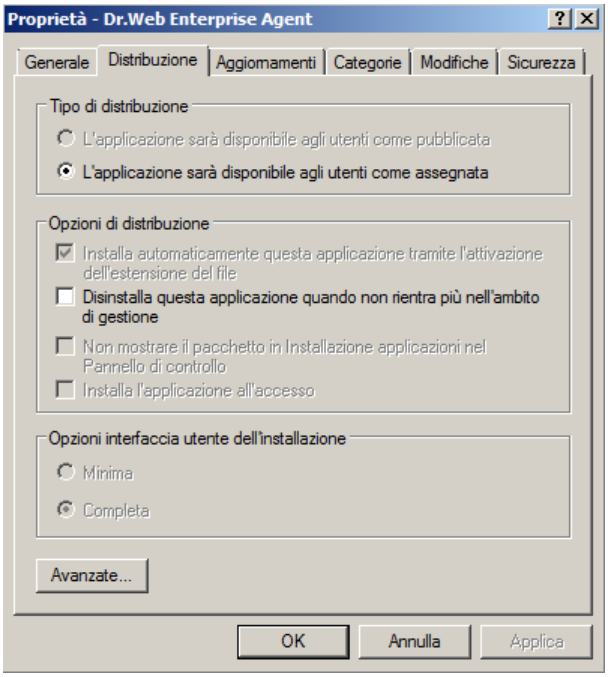


Figura 29. Proprietà dei Criteri di gruppo di Dr.Web Enterprise Agent

17. Nella finestra **Impostazioni avanzate di distribuzione**, spuntare il flag **Non usare le impostazioni di lingua per la distribuzione**. Cliccare su **OK** due volte e chiudere tutte le finestre aperte.

L'Enterprise agent si installerà in modo automatico sui computer selezionati quando alla prossima volta si registreranno nel dominio.

4.3.2. Connettere gli agent al server

Le impostazioni predefinite del server antivirale prevedono una conferma manuale delle postazioni nuove che devono connettersi al server. Ciò significa che il server non connette automaticamente le postazioni nuove, ma le aggiunge all'elenco di postazioni non confermate. Per consentire la connessione di una nuova postazione, andare alla sezione **Amministrazione** del Pannello di controllo e selezionare la voce **Postazioni non confermate**. Si apre un elenco delle postazioni con l'agent installato che ancora non sono state confermate sul server.

Scegliere dall'elenco le postazioni per cui si vuole consentire l'accesso all'Enterprise server, dopo di che cliccare sul pulsante **Consenti l'accesso e designa come primario il gruppo** nell'angolo superiore destro della finestra. Nella finestra apparsa, impostare il gruppo primario (per esempio, il gruppo `Everyone`).

4.4. Creare e utilizzare gruppi di postazioni

4.4.1. Gruppi. Gruppi predefiniti, creare gruppi nuovi. Rimuovere gruppi

Ai fini di facilitare l'amministrazione delle postazioni nella rete antivirale, il software Dr.Web fornisce una funzione di gestione dei gruppi.

Raggruppando le postazioni è possibile configurare tutte le postazioni del gruppo con un singolo comando ed eseguire determinati task contemporaneamente su tutte le postazioni del gruppo. I gruppi si possono usare per organizzare (strutturare) l'elenco delle postazioni.

All'installazione del software Dr.Web, si creano i cosiddetti gruppi predefiniti.

Il gruppo predefinito Everyone comprende tutte le postazioni della rete antivirale.

I gruppi Online e Offline cambiano automaticamente nel corso del funzionamento del server; il primo gruppo include tutte le postazioni connesse (che rispondono alle query inviate dal server), mentre il secondo gruppo racchiude tutte le postazioni non connesse.

Gli altri gruppi predefiniti includono le postazioni che girano sotto determinati sistemi operativi o utilizzano protocolli di rete speciali. I gruppi predefiniti non possono essere modificati manualmente.

È possibile creare gruppi personalizzati per raggruppare le postazioni.

Per creare un gruppo nuovo:

1. Nella sezione **Rete antivirale** del Pannello di controllo cliccare sul pulsante **Aggiungi postazione o gruppo — Crea gruppo**. Appare il modulo **Gruppo nuovo**.
2. Il campo di input **Identificatore** si compila automaticamente. Se necessario, può essere modificato. L'identificatore non può contenere spazi.
3. Digitare il nome del gruppo nuovo nel campo **Nome**.
4. Per i gruppi nidificati, nel campo **Gruppo padre**, è necessario selezionare dall'elenco a discesa un gruppo da designare come padre da cui il gruppo nuovo eredita la configurazione se non vengono definite impostazioni individuali. Per un gruppo radice (che non ha padre), lasciare vuoto questo campo; il gruppo verrà aggiunto alla radice dell'elenco gerarchico. In tale caso, il gruppo nuovo eredita le impostazioni del gruppo predefinito Everyone.
5. Inserire qualche commento nel campo **Descrizione**.
6. Cliccare su **Salva**.

Inoltre, è possibile rimuovere i gruppi creati (non è invece possibile rimuovere i gruppi predefiniti). A questo scopo, selezionare il gruppo desiderato, dopo di che cliccare sul pulsante **Rimuovi gli oggetti segnati** e confermare l'azione nella finestra di avviso che avverte che non sarà possibile ripristinare un gruppo una volta rimosso.

4.4.2. Aggiunzione delle postazioni al gruppo. Rimozione delle postazioni dal gruppo

Esistono più modi di come si possono aggiungere postazioni ai gruppi personalizzati:

1. Modificando le impostazioni della postazione.
2. Trascinando la postazione nell'elenco gerarchico (drag'n'drop).

Per modificare la lista dei gruppi di cui la postazione fa parte nelle sue impostazioni:

1. Selezionare la voce **Rete antivirale** dal menu principale del Pannello di controllo, poi nella finestra che si è aperta, nell'elenco gerarchico cliccare sul nome della postazione desiderata.
2. Aprire le impostazioni della postazione in uno dei seguiti modi:
   - Dal menu di amministrazione (il pannello a sinistra) selezionare la voce **Proprietà**.
   - Cliccare su **Generali** — **Modifica** sulla barra degli strumenti.

3. Nel pannello **Proprietà della postazione** che si è aperto, andare alla scheda **Gruppi**.

   Nell'elenco **Appartiene a**, sono enumerati i gruppi in cui la postazione è già inclusa. L'elenco **Gruppi conosciuti** riporta tutti gli altri gruppi personalizzati.

4. Per aggiungere la postazione a un gruppo personalizzato, cliccare sul nome del gruppo nella lista **Gruppi conosciuti**. La postazione verrà aggiunta a questo gruppo che verrà spostato nella lista **Appartiene a**.
5. Per rimuovere la postazione da un gruppo personalizzato, cliccare sul nome del gruppo nella lista **Appartiene a**. La postazione verrà rimossa da questo gruppo che verrà spostato nella lista **Gruppi conosciuti**.

Nota! *Non è possibile rimuovere postazioni dai gruppi predefiniti.*

6. Per salvare le modifiche apportate, cliccare su **Salva**.

Inoltre, nelle impostazioni della postazione, si può definire il gruppo primario per la postazione (per dettagli, v. Impostazioni ereditate. Gruppi primari).

Per modificare la lista dei gruppi, nei quali rientra una postazione, tramite l'elenco gerarchico:

1. Selezionare la voce **Rete antivirale** dal menu principale del Pannello di controllo e aprire l'elenco gerarchico di gruppi e postazioni.
2. Per aggiungere una postazione a un gruppo personalizzato, tenere premuto il tasto **CTRL** e trascinare la postazione con il mouse al gruppo desiderato (drag'n'drop).
3. Per spostare una postazione da un gruppo personalizzato a un altro, trascinare la postazione con il mouse (drag'n'drop) dal gruppo personalizzato da cui si vuole rimuoverla al gruppo a cui si vuole aggiungerla.

Nota! *Se la postazione viene trascinata da un gruppo predefinito a un gruppo personalizzato, la postazione verrà aggiunta al gruppo personalizzato e non verrà rimossa dal gruppo predefinito. Il metodo drag'n'drop non funziona se si usa il web browser Windows Internet Explorer 7.*

4.4.3. Configurare gruppi. Utilizzare gruppi per configurare postazioni. Definire permessi degli utenti

Una postazione può:

1. ereditare le impostazioni dal gruppo primario;
2. essere configurata in modo individuale.

Quando si crea un gruppo nuovo, eredita le impostazioni dal suo gruppo padre o dal gruppo Everyone se non è impostato un gruppo padre.

Quando si crea una postazione, eredita le impostazioni dal suo gruppo primario.

Quando si leggono o si modificano le impostazioni ereditate di una postazione, nella finestra corrispondente si specifica che un'impostazione è ereditata dal gruppo primario.

È possibile creare varie configurazioni per diversi **gruppi** e **postazioni**.

Per definire impostazioni individuali di una postazione, modificare la parte corrispondente delle impostazioni. In tale caso, si visualizza che un'impostazione è stata definita in modo individuale per questa postazione.

Se per una postazione sono stati impostati parametri individuali, i parametri del gruppo primario e qualsiasi modifica degli stessi non saranno effettivi per la postazione.

La configurazione che una postazione ha ereditato dal gruppo primario può essere ripristinata. Per fare questo, cliccare sul pulsante **Rimuovi queste impostazioni** sulla barra degli strumenti del Pannello di controllo, nella sezione delle impostazioni corrispondenti o nella sezione delle proprietà della postazione.

Per definire le impostazioni di un gruppo (che saranno le impostazioni predefinite per le postazioni in questo gruppo), nella sezione **Rete antivirale** del Pannello di controllo selezionare il gruppo da configurare e cliccare sul pulsante **Modifica**. Nella parte destra della finestra si apre il modulo **Proprietà del gruppo <nome gruppo>**.

Le impostazioni di un gruppo includono parametri dei moduli antivirali, del calendario e dei diritti degli utenti.

Sia per un singolo gruppo, che per più gruppi selezionati, si possono lanciare, visualizzare e fermare task di scansione. Inoltre, si possono visualizzare le statistiche (infezioni, virus, avvio/terminazione, errori di scansione e di installazione) e le statistiche riassuntive di tutte le postazioni in uno o in più gruppi.

4.4.4. Impostazioni ereditate. Gruppi primari

Quando alla rete antivirale aderisce una postazione nuova, prende (eredita) le impostazioni da uno dei gruppi di cui fa parte (cioè, dal gruppo primario). Se i parametri di un gruppo primario vengono modificati, cambiano rispettivamente anche i parametri delle postazioni che appartengono a questo gruppo primario. Per una postazione nuova, è possibile scegliere quale gruppo verrà designato come primario riguardo a questa postazione. Di default, è il gruppo Everyone. Se viene impostato come primario un altro gruppo e questo gruppo non ha impostazioni individuali, la postazione nuova eredita le impostazioni del gruppo Everyone.

Per designare come primario un gruppo diverso da `Everyone`, selezionare il gruppo desiderato e cliccare sul pulsante **Imposta questo gruppo come primario**.

È possibile assegnare un gruppo primario a tutte le postazioni racchiuse in questo gruppo. Per fare questo, selezionare il gruppo desiderato e cliccare sul pulsante **Imposta questo gruppo come primario**.

Di default, la struttura della rete antivirale mostra l'appartenenza delle postazioni solo ai gruppi primari. Se si desidera che nella directory della rete venga mostrata l'appartenenza delle postazioni a tutti i gruppi di cui fanno parte, cliccare sul pulsante **Impostazioni della vista albero** e spuntare il flag **Appartenenza a tutti i gruppi**.

4.4.5. Configurare diritti degli utenti

Le postazioni ereditano diritti dal gruppo primario. Tuttavia, potete modificare non solo i diritti dell'intero gruppo, ma anche di una singola postazione.

Per impostare diritti dell'utente di una postazione, selezionarla dall'albero delle postazioni e dal menu di gestione (pannello a sinistra) selezionare la voce **Permessi**. Si apre la finestra di configurazione dei diritti. Per memorizzare le modifiche, cliccare sul pulsante **Salva**.

4.4.6. Propagazione delle impostazioni

I parametri dei moduli antivirali, dei calendari, dei diritti degli utenti di un gruppo o di una postazione possono essere copiati (propagati) verso uno o più gruppi o postazioni.

Per fare questo, nel modulo di configurazione del componente antivirale, del calendario o dei diritti della postazione, cliccare sul pulsante **Propaga queste impostazioni verso un altro oggetto**. Si apre la finestra della directory della rete in cui è necessario selezionare i gruppi e le postazioni verso i quali si vogliono propagare le impostazioni. Per accettare le modifiche apportate, cliccare sul pulsante **Salva**.

4.5. Collegare gli Enterprise server principali e subordinati

Talvolta nella rete locale un Enterprise server non basta perché il carico è troppo alto, quindi è necessario installare uno o più Enterprise server addizionali, tra cui si divide il carico. Oppure l'azienda possiede alcune sottoreti separate una dall'altra.

In tali casi, è possibile usare più Enterprise server e connetterli uno agli altri. Se la rete antivirale include più server, è possibile decidere a quale server verrà collegato ciascun agent. In questo paragrafo della guida vediamo il tipo più comune di collegamento di due Enterprise server, di cui uno è principale (riceve aggiornamenti del software antivirale dal Sistema globale d'aggiornamento e li trasmette al server subordinato, inoltre riceve statistiche dal server subordinato) e il secondo è subordinato (riceve aggiornamenti del software antivirale dal server principale e invia statistiche al server principale).

Per collegare due Enterprise server con una relazione del genere «principale-subordinato», è necessario eseguire le seguenti azioni:

1. Collegarsi tramite il Pannello di controllo a entrambi gli Enterprise server e assicurarsi che funzionano in modo normale.
2. Assicurarsi che per ciascun Enterprise server della rete locale si usa una chiave `enterprise.key` diversa (la chiave `agent.key` può essere anche uguale).
3. Collegarsi tramite il Pannello di controllo a ciascun Enterprise server e assegnare ad essi nomi distinguenti che aiutano ad evitare errori durante il collegamento e la gestione. I nomi possono essere assegnati nel Pannello di controllo, sezione **Amministrazione — Configurazione Dr.Web Enterprise Server**, scheda **Generali**, campo **Nome**, dopo di che si deve cliccare su **Salva**. Nel nostro esempio, chiamiamo il server principale `MAIN` e il server addizionale (subordinato) `AUXILIARY`. Portata a termine quest'azione, è necessario riavviare gli Enterprise server.

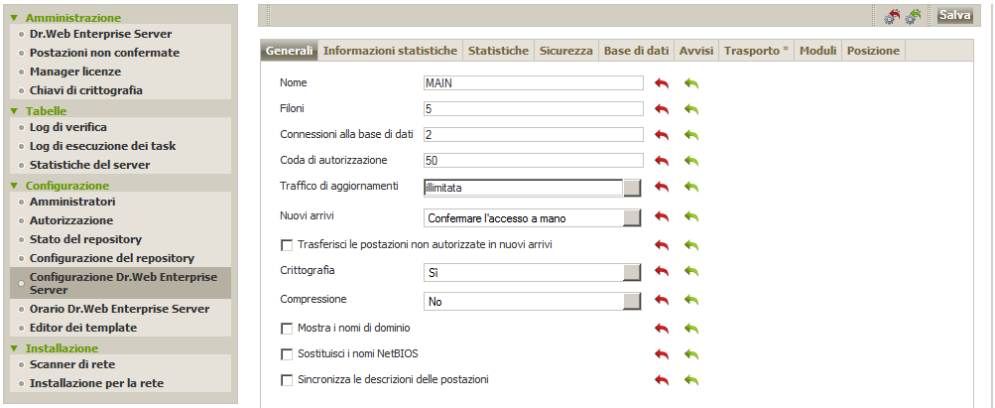


Figura 30. Assegnare nomi ai server

4. Su entrambi gli Enterprise server abilitare il protocollo di server. Questo si può fare nel Pannello di Controllo, sezione **Amministrazione — Configurazione Dr.Web Enterprise Server**, scheda **Moduli**, dove selezionare l'opzione **Protocollo "Dr.Web Enterprise Server"** e poi cliccare su **Salva**. Portata a termine quest'azione, è necessario riavviare gli Enterprise server.

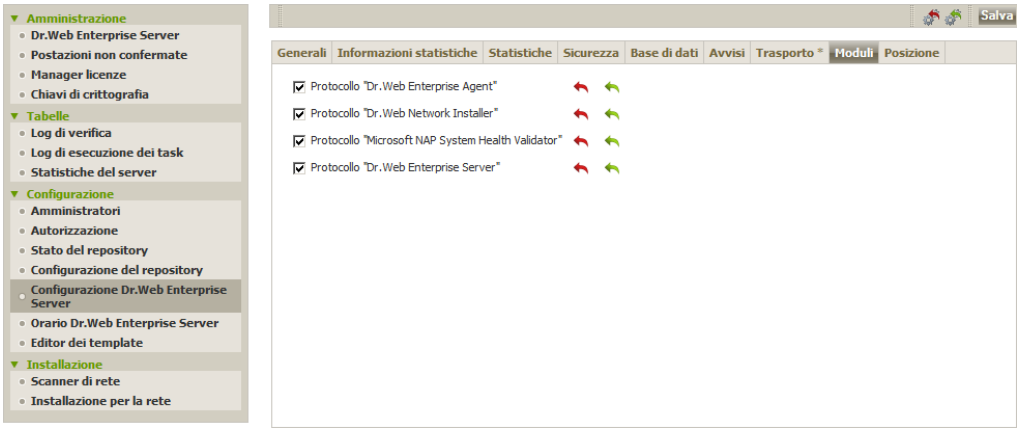


Figura 31. Abilitare il protocollo del server

***Nota!** . Potete eseguire insieme le impostazioni degli Enterprise server descritte nei punti 3 e 4 per diminuire il numero di riavvii necessari degli Enterprise server.*

5. Collegarsi tramite il Pannello di controllo al server subordinato (`AUXILIARY`) e aggiungere il server principale (`MAIN`). Per fare questo, entrare nella sezione **Amministrazione — Relazioni**. Nella finestra apparsa, cliccare sul pulsante **Crea relazione**. Appare il modulo **Nuova relazione**. Selezionare come **Tipo** l'opzione **Principale**. Nel campo **Nome** digitare il nome del server principale (`MAIN`). A destra del campo **Chiave**, cliccare sul pulsante **Sfoglia** e trovare la chiave `drwcsd.pub` appartenente al server principale. Nel campo **Password**, digitare qualsiasi password che comunque va ricordata. Nel campo **Indirizzo**, inserire l'indirizzo del server principale. Nel campo **Indirizzo della console di amministrazione**, inserire l'indirizzo del computer su cui è avviato il Pannello di controllo. Nel campo **Parametri di connessione**, selezionare l'opzione **Sempre connesso**. Cliccare sul pulsante **Salva**.

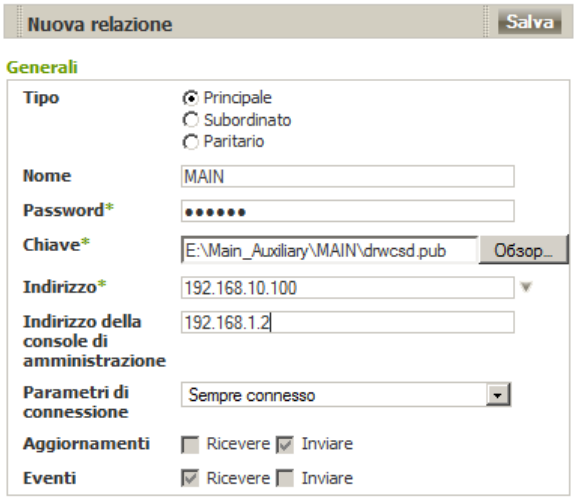


Figura 32. Connessione del server principale

6. Collegarsi tramite il Pannello di controllo al server principale (`MAIN`) e aggiungere il server subordinato (`AUXILIARY`). Per fare questo, entrare nella sezione **Amministrazione — Relazioni**. Nella finestra apparsa, cliccare sul pulsante **Crea relazione**. Nella finestra **Nuova relazione**, selezionare come **Tipo** l'opzione **Subordinato**. Nel campo **Nome** digitare il nome del server subordinato (`AUXILIARY`). Nel campo **Password**, digitare la stessa password che è stata inserita nel punto 5 sopra. A destra del campo **Chiave**, cliccare sul pulsante **Sfoglia** e trovare la chiave `drwcsd.pub` appartenente al server subordinato. Nel campo **Indirizzo della console di amministrazione**, inserire l'indirizzo del computer su cui è avviato il Pannello di controllo. Nel campo **Parametri di connessione**, selezionare l'opzione **Sempre connesso**. Cliccare sul pulsante **Salva**.

Figura 33. Connessione del server subordinato

Come risultato, deve apparire una notifica di quello che la relazione è stata creata con successo.

7. Nell'albero che si trova nella parte centrale della finestra del Pannello di controllo, il server subordinato (`AUXILIARY`) deve comparire nei gruppi **Online** e **Subordinati**.

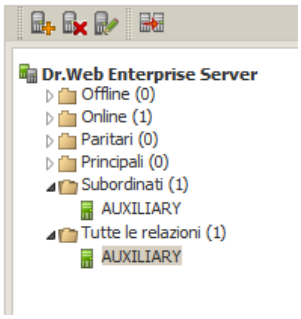


Figura 34. Il server subordinato si è connesso

8. Collegarsi tramite il Pannello di controllo al server subordinato (`AUXILIARY`) e assicurarsi che anche il server principale (`MAIN`) è connesso al server subordinato (`AUXILIARY`), cioè si trova nei gruppi **Online** e **Principali**.

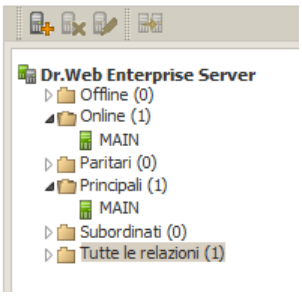


Figura 35. Il server principale si è connesso

Attenzione! *Non è possibile collegare due Enterprise server utilizzando la stessa chiave di licenza (*`enterprise.key`*). Non è possibile collegare più Enterprise server con un'uguale coppia di parametri: password e chiave di cifratura pubblica* `drwcsd.pub`.

4.6. Utilizzo del database esterno

La rete antivirale spesso esige più capacità di quante sono disponibili nel database interno dell'Enterprise server.

Più avanti descriviamo particolarità dell'installazione di Microsoft SQL Server 2008 Express Edition SP1 e vediamo la procedura di migrazione dal database interno dell'Enterprise server al database esterno gestito da questo DBMS.

4.6.1. Installare Microsoft SQL Server 2008 R2 Express e configurare il driver ODBC

Microsoft SQL Server 2008 R2 Express oggi è il DBMS più accessibile. Dalle soluzioni gratuite, questa è la più adatta per l'utilizzo insieme all'Enterprise server.

Per scaricare la versione attuale di Microsoft SQL Server R2 2008 Express e i componenti necessari per utilizzare questo DBMS, passare a questo link:

http://www.microsoft.com/sqlserver/2008/ru/ru/express.aspx.

Questo DBMS è compatibile con Microsoft Windows XP SP2/Vista/2003 SP2/2008.

Sotto supponiamo che l'SQL Server e l'Enterprise server si trovino su diversi computer della rete locale e che siano connessi attraverso il protocollo TCP/IP.

Quando si installa Microsoft SQL Server 2008 R2 Express, fare attenzione ai seguenti dettagli.

Nella **Configurazione del motore di database** selezionare l'opzione **Modalità mista (autenticazione di SQL Server e autenticazione di Windows)**. Immettere qualsiasi password per l'account predefinito amministratore di sistema SQL Server. Si deve ricordare questa password.

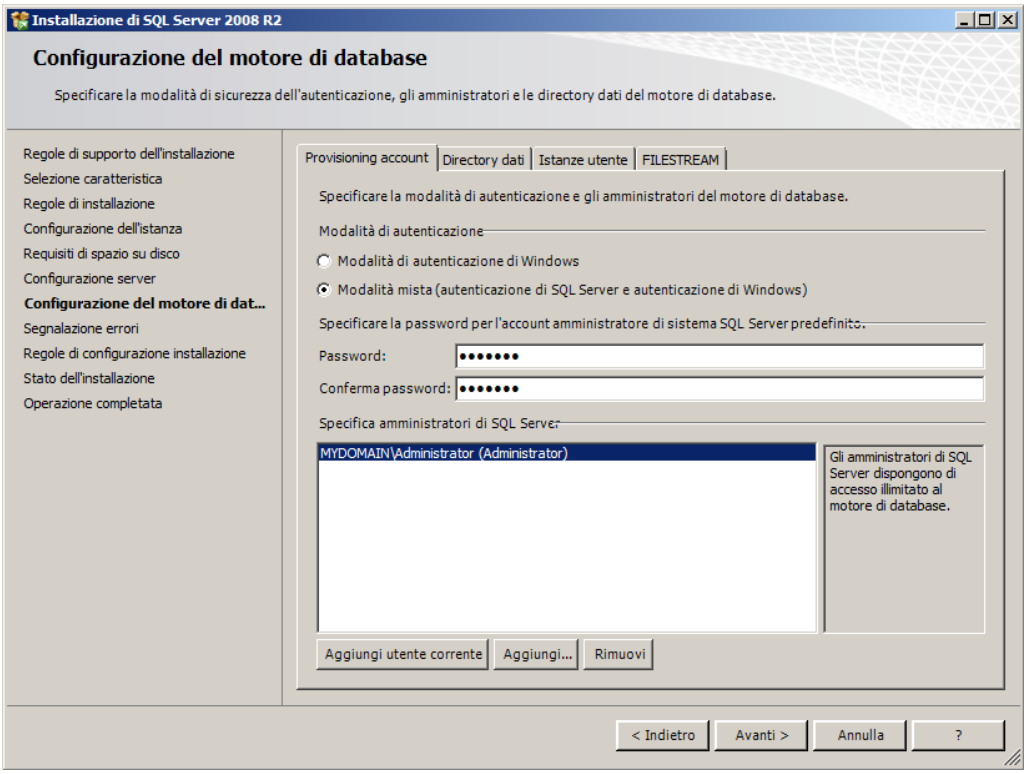


Figura 36. Autenticazione in modalità mista

Una volta installato Microsoft SQL Server R2 2008 Express, è necessario aprire **SQL Server Configuration Manager** sul computer con il DBMS e abilitare il protocollo **TCP/IP**.

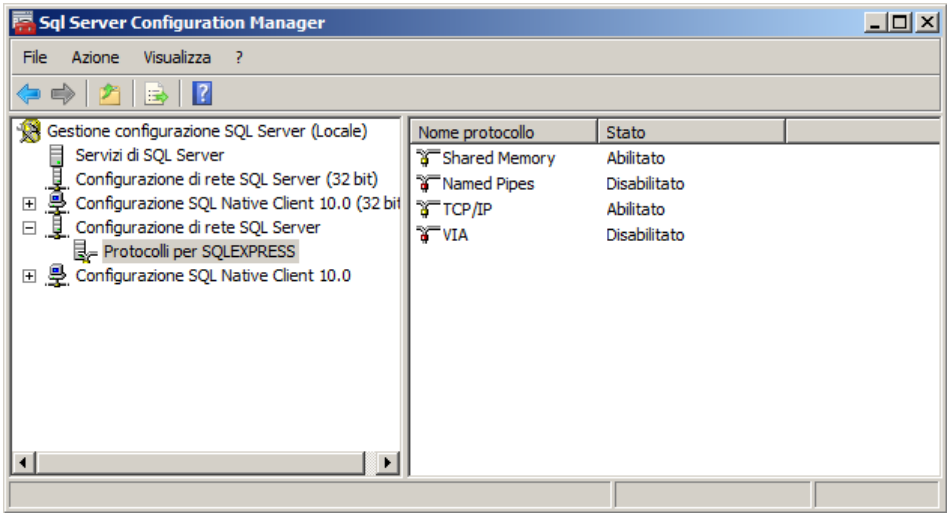


Figura 37. Abilitare il protocollo TCP/IP per SQL Server

Per continuare il lavoro, è necessario riavviare il servizio SQL Server.

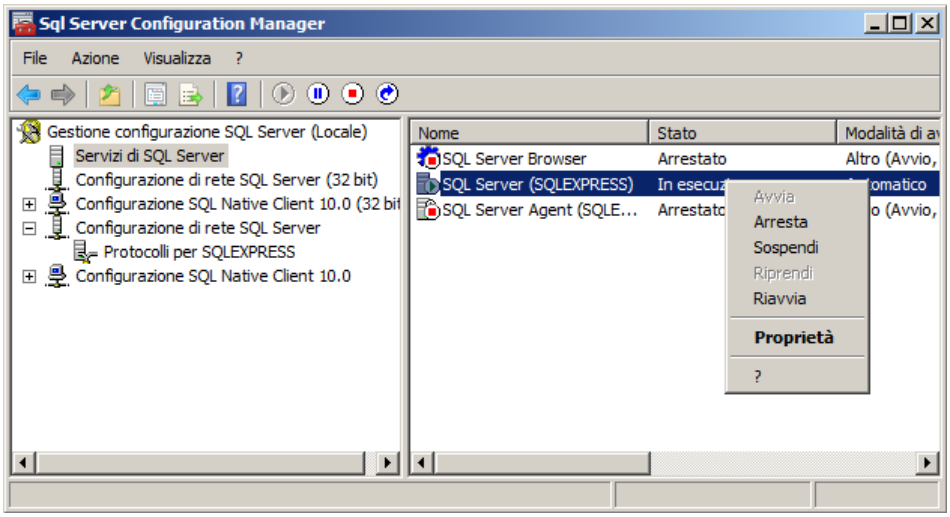


Figura 38. Riavviare il servizio SQL Server

Per configurare il driver ODBC, è necessario eseguire le seguenti azioni sul computer con l'Enterprise server installato (nel nostro esempio utilizziamo Windows Server 2008 R2):

1. Dal **Pannello di controllo di Windows** selezionare la voce **Amministrazione**, nella finestra comparsa fare doppio clic sull'icona **Origine dati (ODBC)**. Si apre la finestra **Amministratore origine dati ODBC**. Andare alla scheda **DSN di sistema**.
2. Cliccare sul pulsante **Aggiungi**. Si apre una finestra in cui è possibile scegliere il driver.
3. Scegliere dall'elenco la voce **SQL Server** e fare clic sul pulsante **Fine**. Si apre la prima finestra della procedura guidata che consente di configurare l'accesso al server dei database.
4. Specificare i parametri di accesso all'origine dati che coincidono con i parametri del server antivirale. Va notato che nel campo **Server** il nome del server, su cui è installato il DBMS, si sceglie automaticamente dal menu a discesa.

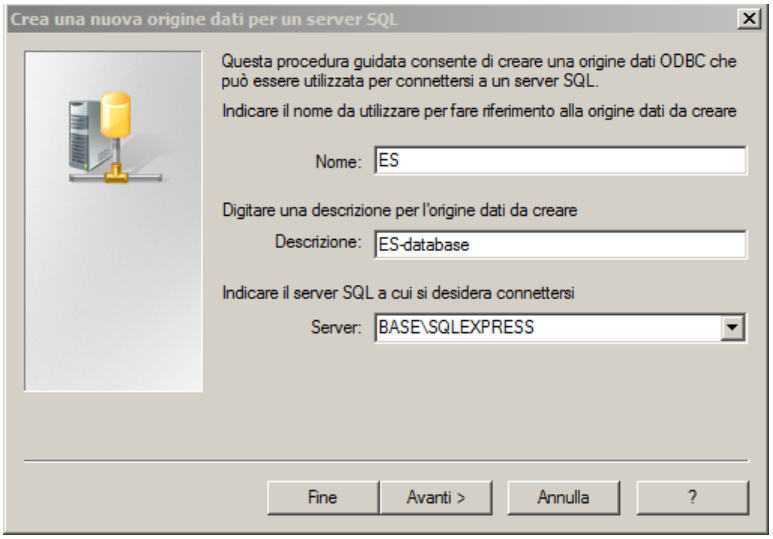


Figura 39. Creazione dell'origine dati per SQL Server

Cliccare su **Avanti**. Si apre la finestra successiva della procedura guidata.

5. In questa finestra, è necessario definire le impostazioni di accesso al database. Cliccare sul tasto Configurazione client. Si apre la finestra di scelta e di configurazione del protocollo di rete.
6. Scegliere la libreria di rete per il protocollo **TCP/IP**. Fare clic sul pulsante **OK**. La finestra si chiude. Si torna alla finestra di configurazione del driver.
7. Selezionare l'opzione **Autenticazione SQL Server tramite ID e password di accesso immessi dall'utente**. Nel campo **ID accesso**, digitare `sa`, nel campo **Password** inserire la stessa password amministratore DBMS che si è impostata all'installazione del DBMS. Cliccare due volte su **Avanti**.

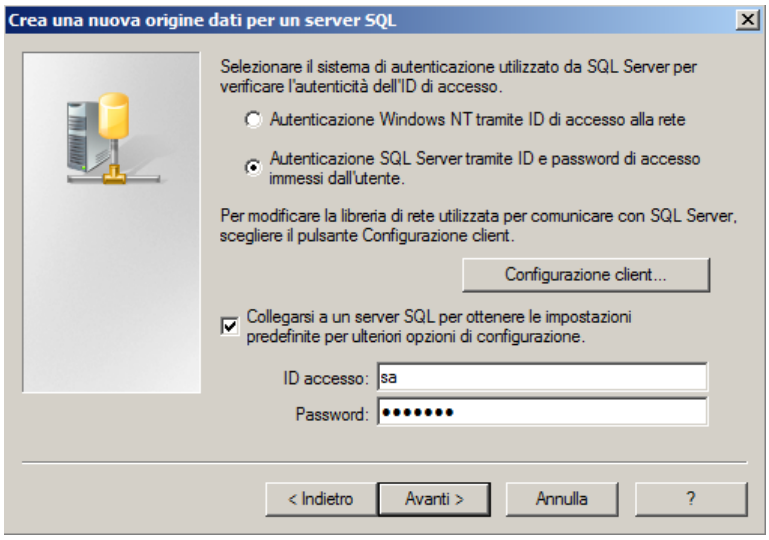


Figura 40. Autenticazione dell'utente

8. Nell'ultima finestra della procedura guidata selezionare la voce **Cambiare la lingua dei messaggi di sistema SQL server** e scegliere l'inglese. Fare clic sul pulsante **Fine** e poi su **OK**.

4.6.2. Migrare dal database interno al database esterno

Per migrare dal database interno dell'Enterprise server al database esterno, eseguire le seguenti azioni:

1. Arrestare il servizio Enterprise server tramite il **Pannello di controllo — Amministrazione — Dr.Web Enterprise Server**, cliccare sul pulsante **Arresta Dr.Web Enterprise Server**.
2. Esportare il database interno esistente. Per fare questo, eseguire il seguente comando sul computer, su cui è installato l'Enterprise server:

   ```
   "C:\Program Files\DrWeb Enterprise Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Enterprise Server" -var-root="C:\Program Files\DrWeb Enterprise Server\var" -verbosity=all exportdb C:\esbase.es
   ```

   Come risultato di quest'azione, il database interno verrà esportato nel file `C:\esbase.es`.
3. Lanciare il servizio Dr.Web Enterprise Server tramite la gestione dei servizi di Windows (**Pannello di controllo — Amministrazione — Servizi**). Collegarsi all'Enterprise server tramite il Pannello di controllo e configurare i parametri del server che permettono di utilizzare il database esterno: **Amministrazione — Configurazione Dr.Web Enterprise Server — Base di dati**, dopo di che fare clic sul pulsante **Salva**. Rifiutare la proposta di riavvio del server.

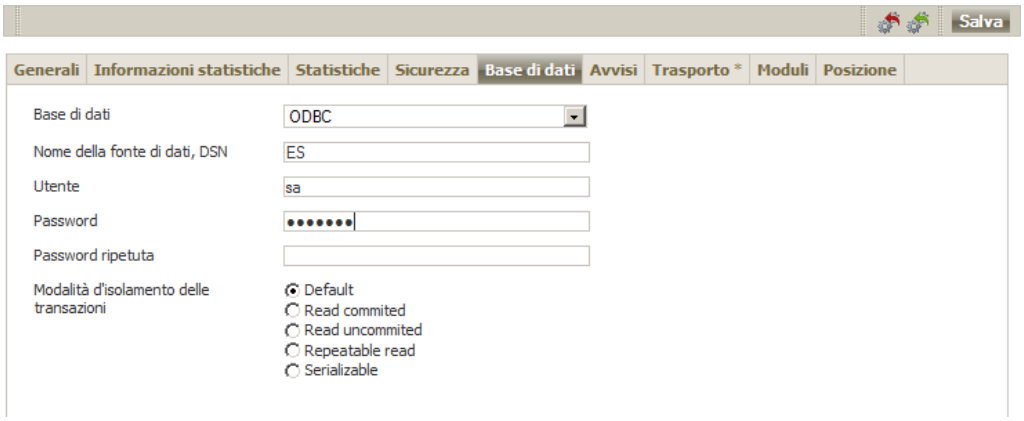


Figura 41. Configurare l'Enterprise server per consentire l'utilizzo del database esterno

4. Arrestare il servizio Enterprise server tramite il **Pannello di controllo — Amministrazione — Dr.Web Enterprise Server**, cliccare sul pulsante **Arresta Dr.Web Enterprise Server**.
5. Inizializzare il nuovo database dell'Enterprise server. Per fare questo, sul computer, sui cui è installato l'Enterprise server, riscrivere la chiave `agent.key` appartenente all'Enterprise server nella cartella radice C:\ del disco ed eseguire il seguente comando:

   ```
   "C:\Program Files\DrWeb Enterprise Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Enterprise Server" -var-root="C:\Program Files\DrWeb Enterprise Server\var" -verbosity=all initdb C:\agent.key - - root
   ```
6. Importare il database che si è esportato nel punto 2 nel database nuovo. Per fare questo, sul computer con l'Enterprise server, eseguire il seguente comando:

   ```
   "C:\Program Files\DrWeb Enterprise Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Enterprise Server" -var-root="C:\Program Files\DrWeb Enterprise Server\var" -verbosity=all importdb C:\esbase.es
   ```
7. Lanciare il servizio Dr.Web Enterprise Server tramite la gestione dei servizi di Windows (**Pannello di controllo — Amministrazione — Servizi**).

4.7. Installazione di NAP Validator

NAP Validator consente di utilizzare la tecnologia Microsoft Network Access Protection (NAP) per verificare se il software delle postazioni protette funziona in modo normale in conformità ai criteri impostati e consente di gestire l'accesso delle postazioni alle risorse della rete sulla base dei risultati di tale verifica.

NAP Validator si installa su un server che svolge il ruolo **Servizi di accesso e criteri di rete** (Windows Server 2008 o superiore), e sul server devono funzionare servizi di ruoli, quali **Server dei criteri di rete e Protocollo di identità host**. Client della tecnologia NAP possono essere computer Windows XP SP3 o superiore.

Per installare NAP Validator, eseguire le seguenti azioni:

1. Scaricare il software Dr.Web NAP Validator dal sito http://www.drweb.com. Il nome del file del software è scritto nel formato `drweb-esuite-napshv-6xx-xxxxxxxxx-windows-nt-yyy.msi`, dove `yyy` può essere x86 e x64. Si apre la finestra **InstallShield Wizard** che informa sul prodotto da installare. Fare clic sul pulsante **Next**.
2. Si apre una finestra con il testo del contratto di licenza. Dopo aver letto i termini del contratto di licenza, nel gruppo dei pulsanti di scelta indicare **I accept the terms in the license agreement** e fare clic sul pulsante **Next**.
3. Nella finestra comparsa, nei campi **Address** e **Port**, impostare rispettivamente l'indirizzo IP e la porta dell'Enterprise server. Fare clic sul pulsante **Next.**

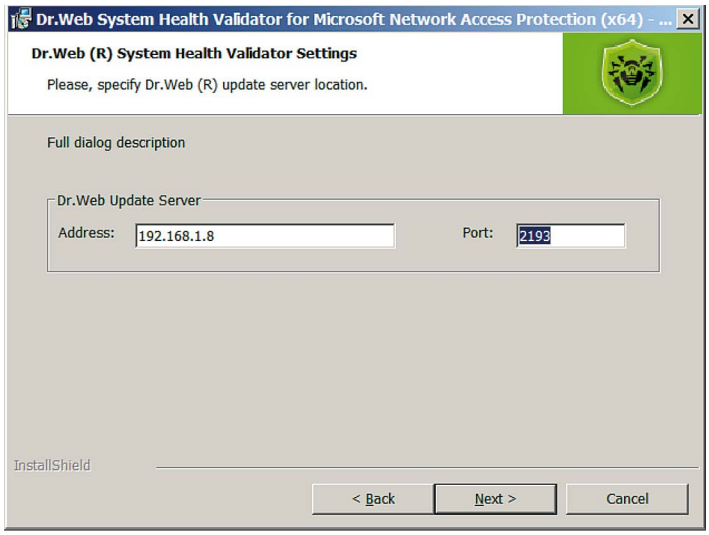


Figura 42. Interfaccia dell'installer di Dr.Web NAP Validator

4. Fare clic sul pulsante **Install**. Le azioni successive del programma di installazione non richiedono alcuna partecipazione da parte dell'utente. Una volta completata l'installazione, fare clic sul pulsante Finish.
5. Nel Pannello di controllo del server antivirale selezionare la voce **Dr.Web Enterprise Agent per Windows**, nel menu **Rete antivirale** selezionare l'opzione Microsoft Network Access Protection per abilitare il supporto della tecnologia Microsoft® Network Access Protection utilizzata per controllare lo stato delle postazioni.
6. Dopo che Dr.Web NAP Validator è stato installato sul computer su cui è installato NAP Server, è necessario aprire il componente di configurazione del server NAP tramite il comando nps.msc, selezionare dalla sezione **Policies** la sottovoce **Health Policies** e nella finestra comparsa aprire le proprietà degli elementi NAP DHCP Compliant. Nella finestra delle impostazioni è necessario spuntare il flag **Dr.Web System Health Validator**, e dall'elenco a discesa che contiene tipi di controlli selezionare la voce **Client passed all SHV checks**. Secondo quest'opzione, il funzionamento di una postazione verrà dichiarato normale se è conforme a tutti gli elementi del criterio impostato.

5. Ultimi commenti

È importante ricordare che una volta modificati i parametri del repository dell'Enterprise server, è necessario eseguire subito un aggiornamento valido di tutti i componenti del software antivirale affinché la rete antivirale possa funzionare correttamente.

Attenzione! *Una volta effettuato il deployment della rete antivirale sulla base di questa guida, si consiglia vivamente di studiare nel dettaglio il documento "Dr.Web Enterprise Security Suite. Versione 6.0. Manuale dell'amministratore".*

Questo documento può essere scaricato dal sito della società Doctor Web:

http://download.drweb.com/doc.

Russia, 125124, Mosca, via 3 Yamskogo Polya, tenuta 2, edificio 12A

Telefono: +7 (495) 789-45-87 (centralino)

Fax: +7 (495) 789-45-97

www.drweb.com I www.freedrweb.com I www.av-desk.com I www.drweb-curenet.com