AVG 8.5 Internet Security Edition

Manuale per l'utente

Revisione documento 85.1 (26.1.2009)

Sommario

1. Introduzione

Il presente manule per l'utente fornisce una documentazione completa per **AVG 8.5 Internet Security** .

Congratulazioni per l'acquisto di AVG 8.5 Internet Security .

AVG 8.5 Internet Security È la gamma di prodotti AVG premiati progettata per fornire maggiore tranquillità e una protezione completa del PC. Analogamente a tutti i prodotti AVG, **AVG 8.5 Internet Security** è stato intermante riprogettato per fornire una protezione completa accreditata e interamente rinnovata di AVG in maniera efficace e intuitiva.

Il nuovo prodotto **AVG 8.5 Internet Security** offre un'interfaccia semplificata combinata con scansioni più aggressive e rapide. Sono state automatizzate più funzioni di protezione per offrire maggiore comodità e sono state incluse nuove opzioni intelligenti per l'utente per adattare le funzionalità della nostra protezione alle tue abitudini. Nessun utilizzo compromettente per la protezione.

AVG è stato progettato e sviluppato per proteggere le attività di rete e del computer. Godetevi la sensazione di protezione totale da parte di AVG.

2. Requisiti per l'installazione di AVG

2.1. Sistemi operativi supportati

AVG 8.5 Internet Security consente di proteggere i computer che eseguono i seguenti sistemi operativi:

- Windows 2000 Professional SP4 + Update Rollup 1
- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (x86 e x64, tutte le edizioni)

(e possibilmente Service Pack superiori per sistemi operativi specifici)

2.2. Requisiti hardware minimi

Di seguito sono riportati i requisiti hardware minimi per **AVG 8.5 Internet Security** :

- Intel Pentium CPU, 1,2 GHz
- 70 MB di spazio libero su disco rigido (per l'installazione)
- 256 MB di memoria RAM

3. Opzioni di installazione di AVG

È possibile installare AVG dal file di installazione disponibile nel CD di installazione oppure è possibile scaricare il file di installazione più recente dal sito Web di AVG (www.avg.com).

Prima di avviare l'installazione di AVG, è consigliabile visitare il sito Web di AVG per controllare che non sia disponibile un nuovo file di installazione. In questo modo è possibile essere certi di installare la versione disponibile di AVG 8.5 Internet Security più recente.

Si consiglia di provare il nuovo strumento Gestore download di AVG che consentirà di selezionare il file di installazione appropriato.

Durante il processo di installazione verrà chiesto il numero di licenza/vendita. Prima di avviare l'installazione, assicurarsi che sia disponibile. Il numero di vendita si trova nel pacchetto del CD. Se la copia di AVG è stata acquistata via Web, il numero di licenza è stato fornito tramite e-mail.

4. Gestore download di AVG

AVG Download Manager è uno strumento semplice che consente di selezionare il file di installazione corretto per il prodotto AVG. In base ai dati immessi, il gestore download selezionerà il prodotto, il tipo di licenza, i componenti e la lingua specifici. Infine, **AVG Download Manager** procederà al download e all'avvio del processo di installazione appropriato.

Viene fornita di seguito una breve descrizione dei vari passaggi da eseguire in **AVG Download Manager**:

4.1. Selezione lingua

In questo primo passaggio di **AVG Download Manager** selezionare la lingua di installazione dal menu a discesa. Tenere presente che la selezione della lingua si applica solo al processo di installazione; dopo l'installazione, sarà possibile modificare la lingua direttamente dalle impostazioni del programma. Selezionare quindi il pulsante ***Avanti*** per continuare.

4.2. Controllo connettività

Nel passaggio successivo, **AVG Download Manager** tenterà di stabilire una connessione Internet per individuare gli aggiornamenti. Non sarà possibile procedere con il processo di download finché **AVG Download Manager** non avrà completato il

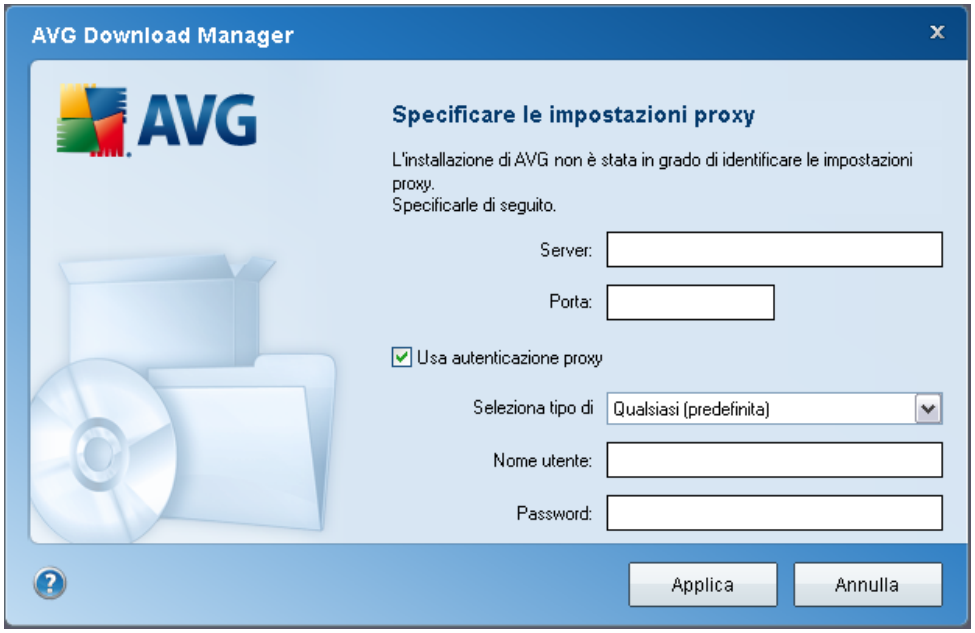
controllo della connettività.

- Se il controllo non rileva alcuna connettività, assicurarsi di essere connessi a Internet. Quindi fare clic sul pulsante ***Riprova***

- Se si utilizza una connessione a Internet tramite proxy, fare clic sul pulsante ***Impostazioni proxy*** per specificare le informazioni proxy:

- Se il controllo ha esito positivo, selezionare il pulsante ***Avanti*** per continuare.

4.3. Impostazioni proxy



Se **AVG Download Manager** non è stato in grado di identificare le impostazioni proxy, è necessario specificarle manualmente. Immettere i seguenti dati:

- ***Server***: immettere un nome o indirizzo IP valido per il server proxy
- ***Porta***: immettere il relativo numero di porta
- ***Usa autenticazione proxy***: se il server proxy richiede l'autenticazione, selezionare questa casella di controllo.
- ***Seleziona tipo di autenticazione***: dal menu a discesa selezionare il tipo di autenticazione. Si consiglia di mantenere il valore predefinito (*il server proxy trasmetterà automaticamente i propri requisiti*). Tuttavia, gli utenti esperti possono anche scegliere l'opzione Di base (*richiesta da alcuni server*) o NTLM (*richiesta da tutti i server ISA*). Quindi, immettere ***nome utente*** e ***password*** (opzionale) validi.

Confermare le impostazioni selezionando il pulsante ***Applica*** per accedere al passaggio successivo di **AVG Download Manager**.

4.4. Selezione del tipo di licenza

In questo passaggio viene richiesto di scegliere il tipo di licenza del prodotto che si desidera scaricare. La descrizione fornita consente di selezionare il prodotto più

adatto alle specifiche esigenze:

- ***Versione completa***: ossia ***AVG Anti-Virus***, ***AVG Anti-Virus plus Firewall*** o ***AVG Internet Security***
- ***Versione Trial***: fornisce la possibilità di utilizzare tutte le funzioni del prodotto completo AVG per il periodo di tempo limitato di 30 giorni
- ***Versione gratuita***: fornisce la protezione agli utenti privati gratuitamente, tuttavia le funzionalità dell'applicazione sono limitate. Inoltre, la versione gratuita include solo alcune delle funzioni disponibili nel prodotto a pagamento.

4.5. Download dei file di installazione

A questo punto sono state fornite tutte le informazioni necessarie a **AVG Download Manager** per avviare il download del pacchetto di installazione e avviare il processo di installazione. Accedere quindi al Processo di installazione di AVG.

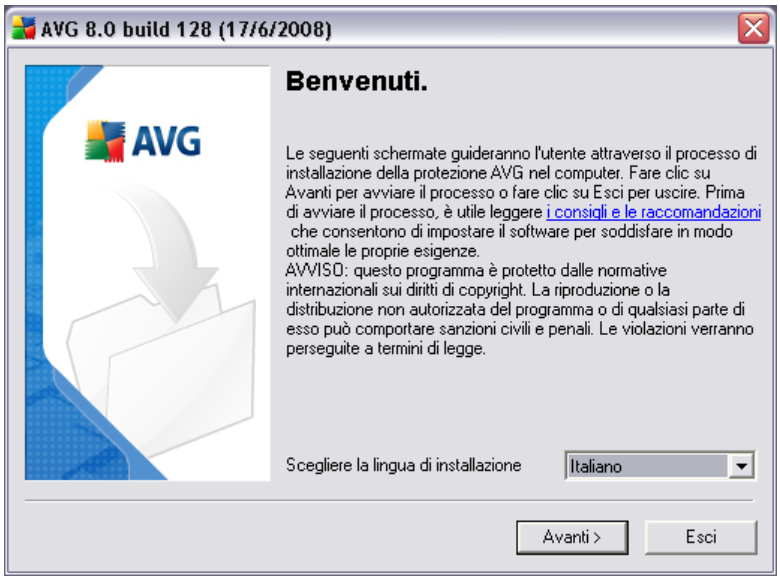
5. Processo di installazione di AVG

Per installare AVG nel computer, è necessario disporre del file di installazione più recente. È possibile utilizzare il file di installazione nel CD in dotazione con il prodotto; tuttavia questo file potrebbe non essere aggiornato.

Pertanto, è consigliabile procurarsi il file di installazione più recente in linea. È possibile scaricare il file dal sito Web AVG (all'indirizzo www.avg.com) nella sezione ***Download.*** In alternativa, è possibile utilizzare il nuovo strumento **AVG Download Manager** che consente di creare e scaricare il pacchetto di installazione desiderato, quindi avviare il processo di installazione.

L'installazione consiste in una sequenza di finestre di dialogo contenenti una breve descrizione delle operazioni da eseguire ad ogni passaggio. Di seguito viene fornita una descrizione di ciascuna finestra di dialogo:

5.1. Avvio dell'installazione

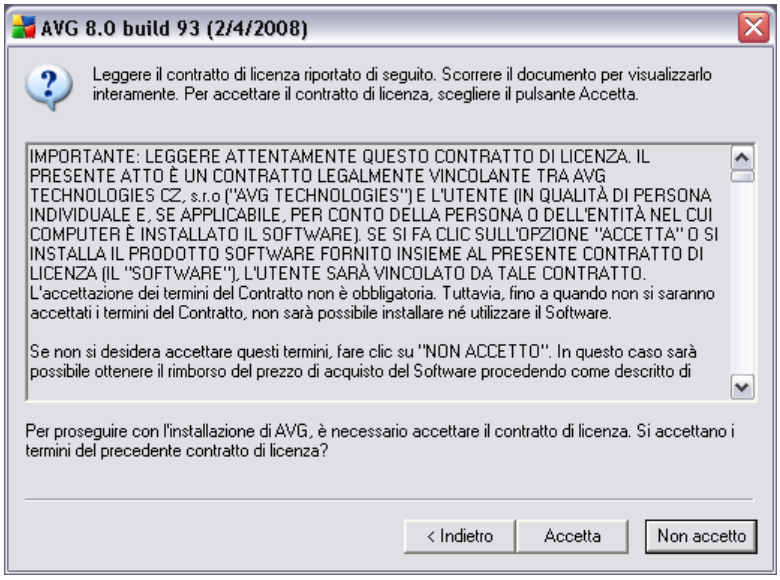


Il processo di installazione inizia con la finestra ***Benvenuti nel programma di installazione di AVG*** . Da qui è possibile selezionare la lingua utilizzata per il processo di installazione. Nella parte inferiore della finestra di dialogo, individuare la voce ***Scegliere la lingua di installazione*** e selezionare la lingua desiderata dal menu a discesa. Quindi selezionare il pulsante ***Avanti*** per confermare e procedere alla finestra di dialogo successiva.

Attenzione: *in questa fase si sceglie solo la lingua per il processo di installazione.*

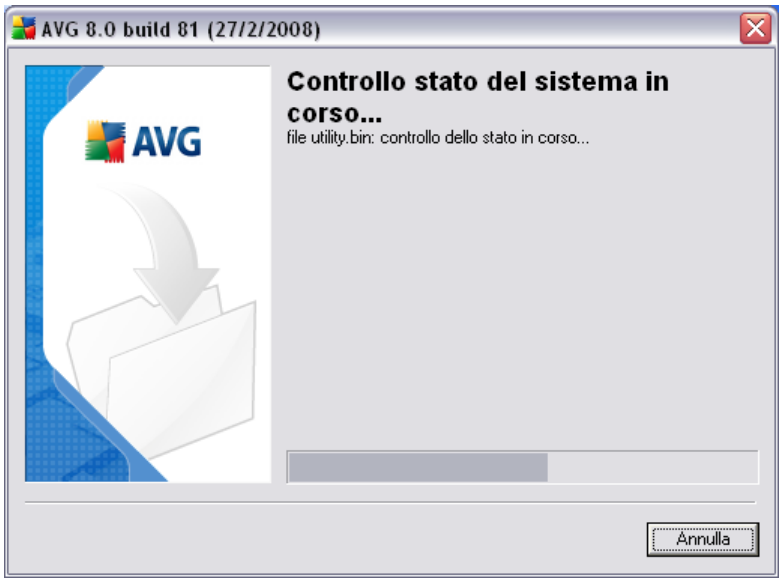
Non si sta selezionando la lingua per l'applicazione AVG poiché sarà specificata successivamente durante il processo di installazione.

5.2. Contratto di licenza



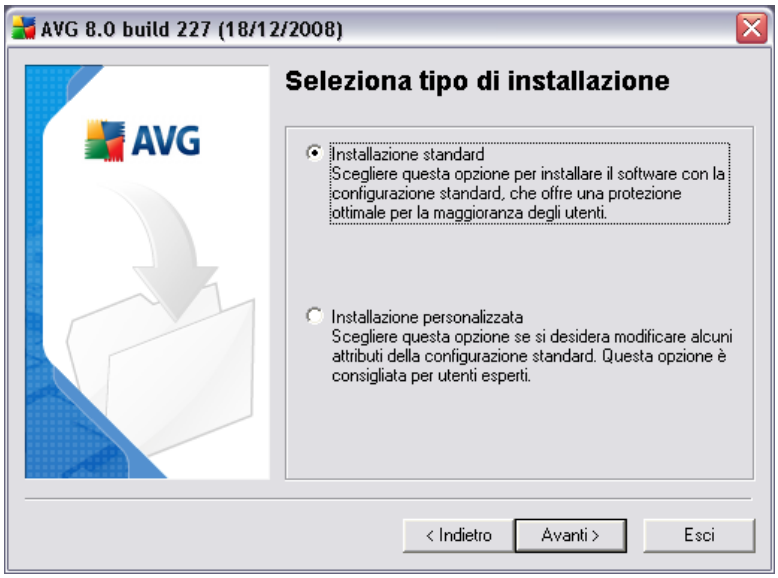
Nella finestra di dialogo ***Contratto di licenza*** è disponibile l'intero contenuto del contratto di licenza di AVG. Leggere attentamente il contratto e, se si accettano tutti i termini, confermare l'approvazione facendo clic sul pulsante ***Accetto***. Se non si accettano i termini del contratto di licenza, premere il pulsante ***Non accetto*** e il processo di installazione verrà interrotto immediatamente.

5.3. Controllo stato del sistema in corso



Una volta accettati i termini del contratto di licenza, si verrà reindirizzati alla finestra di dialogo ***Controllo stato del sistema in corso***. Non è necessario alcun intervento dell'utente; viene eseguito un controllo del sistema prima di avviare l'installazione di AVG. Attendere il completamento del programma, quindi passare alla finestra di dialogo successiva.

5.4. Seleziona tipo di installazione



La finestra di dialogo ***Seleziona tipo di installazione*** consente di scegliere tra due opzioni di installazione: installazione ***standard*** e ***personalizzata***.

Alla maggior parte degli utenti, si consiglia di mantenere l'***installazione standard*** che consente di installare AVG in modalità completamente automatica con le impostazioni predefinite dal produttore del software. La configurazione fornisce la massima protezione combinata con l'utilizzo ottimale delle risorse. In futuro, se ci fosse necessità di modifcare la configurazione, sarà possibile farlo direttamente nell'applicazione AVG.

L'installazione personalizzata dovrebbe essere utilizzata solo da utenti esperti che hanno valide ragioni per installare AVG senza le impostazioni standard. Ad esempio, per soddisfare specifici requisiti di sistema.

5.5. Attiva la licenza AVG

Nella finestra di dialogo ***Attiva AVG*** è necessario immettere i dati di registrazione. Digitare il nome (nel campo ***Nome utente***) e il nome dell'organizzazione (nel campo ***Nome azienda***).

Immettere quindi il numero di licenza/vendita nel campo di testo ***Numero di licenza/vendita***. Il numero di vendita si trova nel pacchetto del CD nella confezione di AVG. Il numero di licenza sarà contenuto nel messaggio e-mail di conferma inviato

dopo l'acquisto in linea di AVG. È necessario digitare il numero esattamente come viene indicato. Se il numero di licenza è disponibile nel formato digitale (contenuto nel messaggio e-mail), si consiglia di utilizzare il metodo copia/incolla per inserirlo.

Premere il pulsante ***Avanti*** per continuare con il processo di installazione.

Se nel passaggio precedente è stata selezionata l'installazione standard, verrà visualizzata la finestra di dialogo ***Riepilogo installazione*** . Se è stata selezionata l'installazione personalizzata, si proseguirà con la finestra di dialogo ***Cartella di destinazione***.

5.6. Installazione personalizzata - Cartella di destinazione

La finestra di dialogo ***Cartella di destinazione*** consente di specificare la posizione di installazione di AVG. Per impostazione predefinita, AVG viene installato nella cartella dei programmi che si trova nell'unità C:. Se si desidera modificare questa posizione, utilizzare il pulsante ***Sfoglia*** per visualizzare la struttura dell'unità e selezionare la cartella corrispondente. Premere il pulsante ***Avanti*** per confermare.

5.7. Installazione personalizzata - Selezione dei componenti

Nella finestra di dialogo ***Selezione componenti*** viene visualizzata una panoramica di tutti i componenti di AVG che possono essere installati. Se le impostazioni predefinite non sono adeguate alle proprie esigenze, è possibile rimuovere/aggiungere componenti specifici.

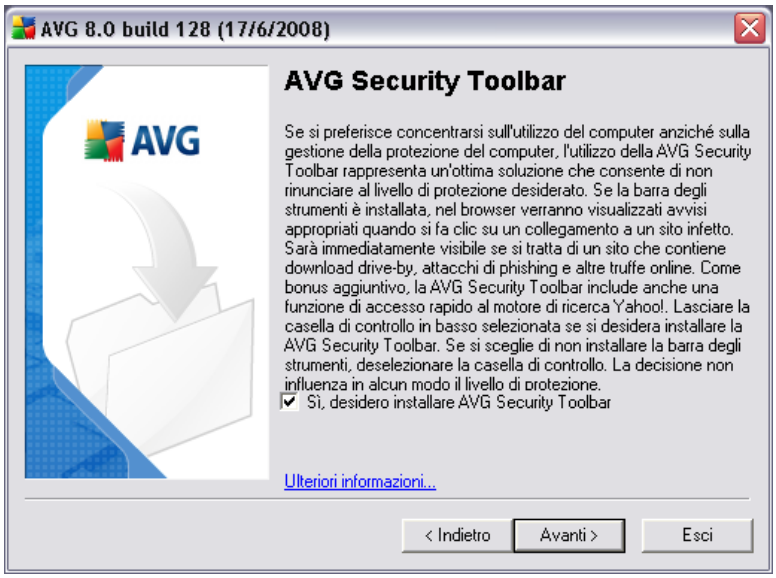
Tuttavia, è possibile eseguire la selezione solo dai componenti inclusi nell'edizione di AVG che è stata acquistata. Solo tali componenti verranno visualizzati come installabili nella finestra di dialogo Selezione componenti.

All'interno dell'elenco dei componenti da installare, è possibile definire in quali lingue installare AVG. Selezionare la voce ***Lingue aggiuntive installate*** quindi selezionare le lingue desiderate dal menu corrispondente.

Fare clic sulla voce ***Scansione E-mail*** e decidere quale plug-in dovrà essere installato per garantire la protezione della posta elettronica. Per impostazione predefinita, verrà installato il ***Plug-in di Microsoft Outlook***. Un'altra opzione specifica è il ***Plug-in di The Bat!*** Se si utilizza un altro client e-mail (*MS Exchange, Qualcomm Eudora e così via*), scegliere l'opzione ***Scansione e-mail personale*** per proteggere le comunicazioni e-mail automaticamente, indipendentemente dal programma e-mail eseguito.

Continuare selezionando il pulsante ***Avanti***.

5.8. AVG Security Toolbar



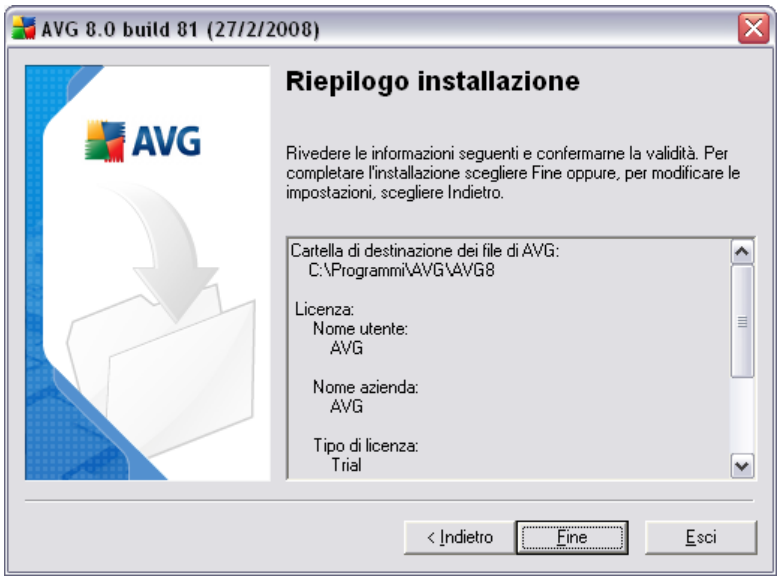
La finestra di dialogo ***AVG Security Toolbar*** consente di decidere se installare ***AVG Security Toolbar***. Se non vengono modificate le impostazioni predefinite, questo componente verrà installato automaticamente nel browser Internet in uso e funzionerà in combinazione con le tecnologie AVG 8.0 e AVG XPL per fornire la protezione in linea più completa durante la navigazione in Internet.

5.9. Windows Firewall

Il numero di licenza fornito in uno dei precedenti passaggi dell'installazione corrisponde all'edizione **AVG 8.5 Internet Security** che include AVG ***Firewall***. AVG ***Firewall*** non può essere eseguito in parallelo con un altro firewall installato. In questa finestra di dialogo, confermare che si desidera installare AVG ***Firewall*** e disattivare Windows Firewall.

Selezionare il pulsante ***Avanti*** per continuare.

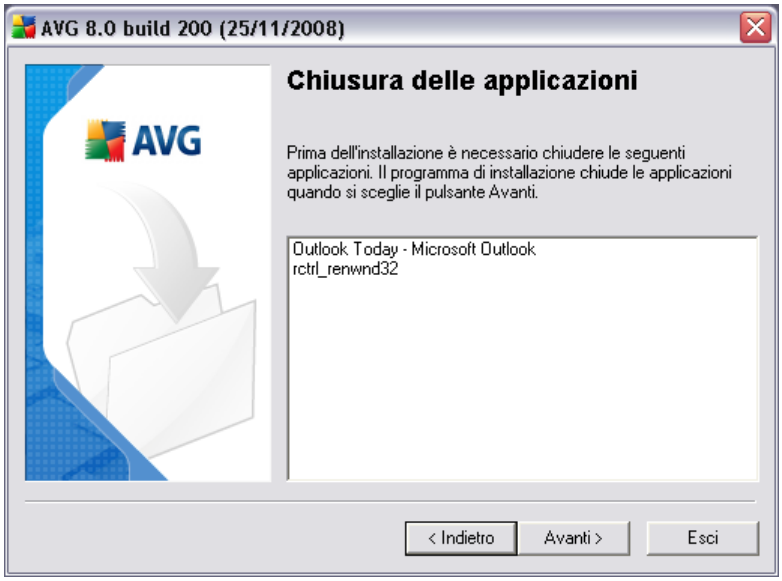
5.10.Riepilogo installazione



La finestra di dialogo ***Riepilogo installazione*** fornisce una panoramica di tutti i parametri del processo di installazione. Assicurarsi che tutte le informazioni siano corrette. In tal caso, premere il pulsante ***Fine*** per continuare. Altrimenti, è possibile utilizzare il pulsante ***Indietro*** per tornare alla rispettiva finestra di dialogo e correggere le informazioni.

5.11.Chiusura delle applicazioni

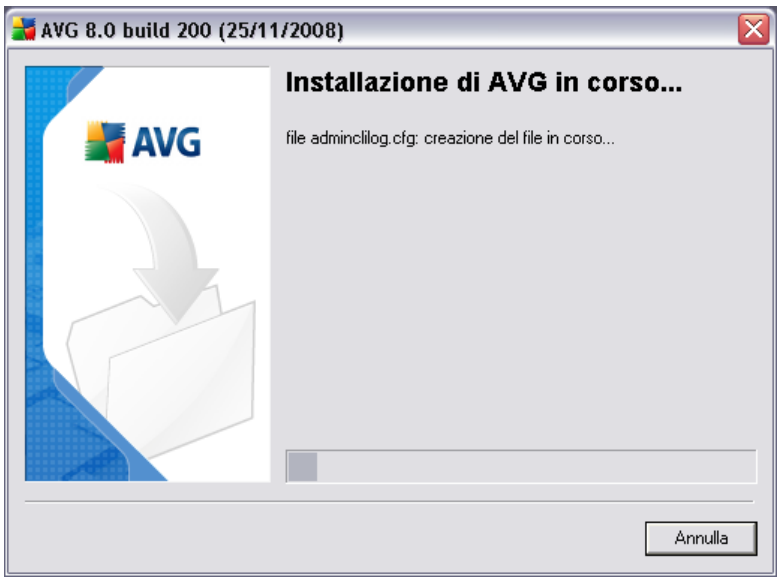
Prima dell'avvio del processo di installazione, potrebbe venire richiesto di chiudere alcune delle applicazioni in esecuzione che potrebbero entrare in conflitto con il processo di installazione di AVG. In tal caso, verrà visualizzata la seguente finestra di dialogo ***Chiusura delle applicazioni***. Questa finestra di dialogo è solo informativa e non richiede alcun intervento. Se si accetta che i programmi elencati vengano chiusi automaticamente, selezionare ***Avanti*** per continuare:



Nota: *accertarsi di aver salvato tutti i dati prima di confermare che si desidera chiudere le applicazioni in esecuzione.*

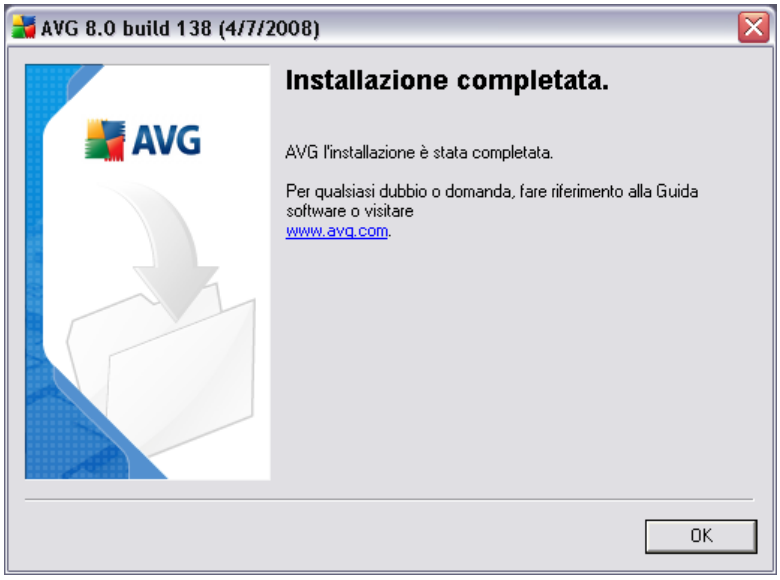
5.12.Installazione

Nella finestra di dialogo ***Installazione di AVG*** viene visualizzato l'avanzamento del processo di installazione. Non è necessario alcun intervento da parte dell'utente:



Al termine del completamento dell'installazione, verrà visualizzata la finestra di dialogo ***Installazione completata***.

5.13.Installazione completata



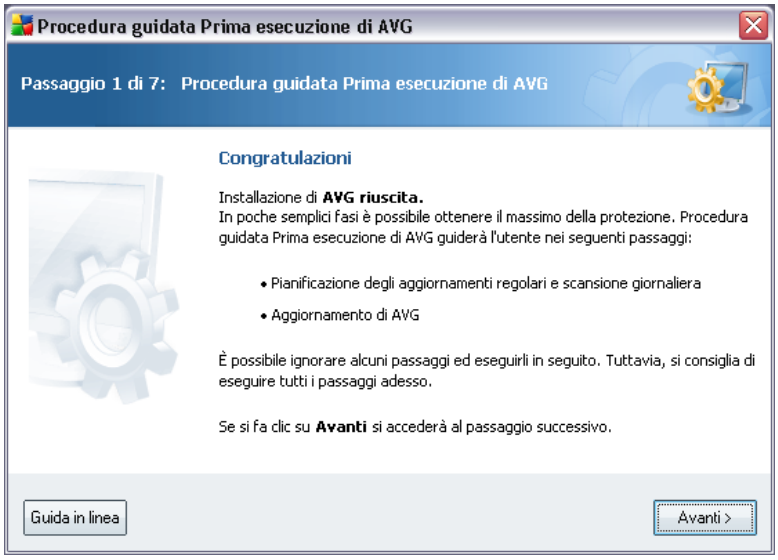
L'installazione di ***è completata!*** è l'ultimo passaggio del processo di installazione di AVG. Adesso AVG è installato nel computer e funziona correttamente. Il programma viene eseguito in background in modalità completamente automatica.

Dopo l'installazione verrà avviata automaticamente la ***Configurazione guidata di base di AVG*** e in pochi passaggi sarà possibile eseguire la **AVG 8.5 Internet Security** configurazione di base. Nonostante la configurazione di AVG sia accessibile in qualunque momento durante l'esecuzione di AVG, si consiglia di utilizzare questa opzione e di impostare la configurazione di base con l'aiuto della procedura guidata.

6. Procedura guidata Prima esecuzione di AVG

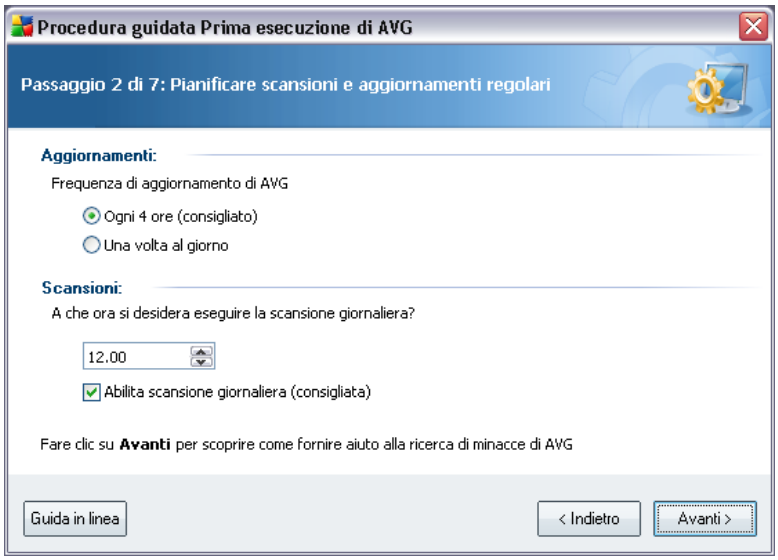
Quando si installa per la prima volta AVG nel computer, viene visualizzata la finestra popup ***Configurazione guidata di base di AVG*** per aiutare l'utente con le impostazioni iniziali di **AVG 8.5 Internet Security** . Anche se è possibile impostare in seguito tutti i parametri indicati, è consigliabile eseguire la procedura guidata per assicurare la protezione del computer' in modo semplice e immediato. Seguire i passaggi descritti in ogni finestra di dialogo della procedura guidata :

6.1. Presentazione della Procedura guidata Prima esecuzione di AVG



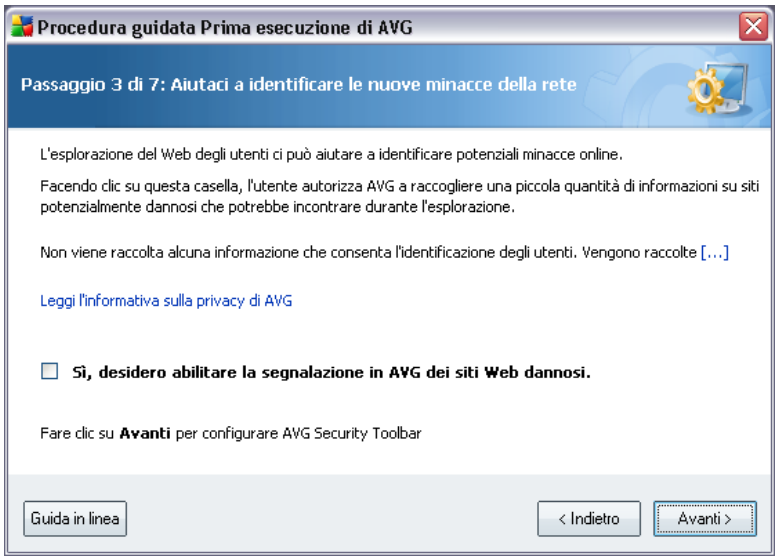
La finestra di benvenuto ***Presentazione della Procedura guidata Prima esecuzione di AVG*** riepiloga brevemente lo stato di AVG nel computer e suggerisce i passaggi da eseguire per ottenere la protezione completa. Fare clic sul pulsante ***Avanti*** per continuare.

6.2. Pianificazione di scansioni e aggiornamenti regolari



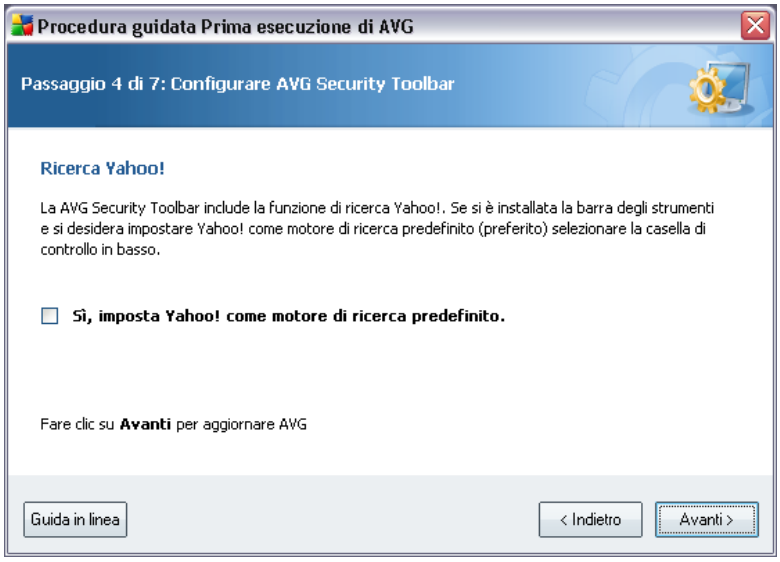
Nella finestra di dialogo ***Pianificazione di scansioni e aggiornamenti regolari*** impostare l'intervallo per il controllo dell'accessibilità di nuovi file di aggiornamento e definire l'ora in cui dovrà essere avviata la scansione pianificata. È consigliabile mantenere i valori predefiniti. Premere il pulsante ***Avanti*** per continuare.

6.3. Aiutaci a identificare le nuove minacce della rete



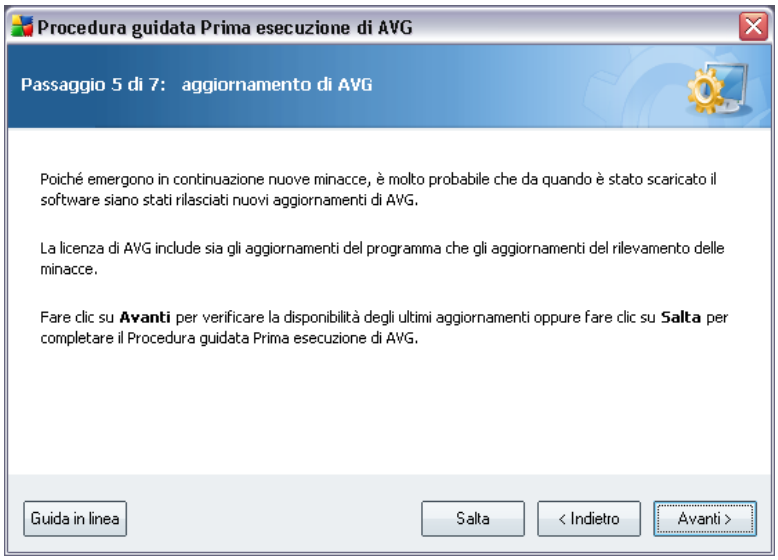
Nella finestra di dialogo ***Aiutaci a identificare le nuove minacce*** scegliere se attivare l'opzione di segnalazione di exploit e siti dannosi individuati dagli utenti mediante le funzionalità ***AVG Surf-Shield / AVG Search-Shield*** del componente ***LinkScanner*** per consentire la raccolta di informazioni nel database in merito ad attività dannose svolte sul Web. È consigliabile mantenere il valore predefinito con la segnalazione attivata. Premere il pulsante ***Avanti*** per continuare.

6.4. Configurazione di AVG Security Toolbar



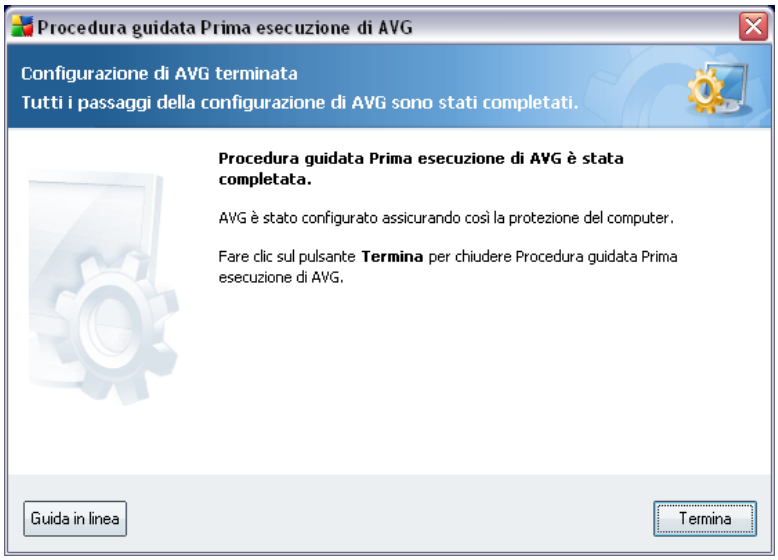
Nella finestra di dialogo ***Configurazione di AVG Security Toolbar*** è possibile selezionare la casella di controllo per impostare Yahoo! come motore di ricerca predefinito.

6.5. Aggiornamento della protezione AVG



Nella finestra di dialogo ***Aggiornamento della protezione AVG*** vengono automaticamente controllati e scaricati gli aggiornamenti di AVG più recenti. Fare clic sul pulsante ***Avanti*** per scaricare i file di aggiornamento più recenti ed eseguire l'aggiornamento.

6.6. Configurazione di AVG completata



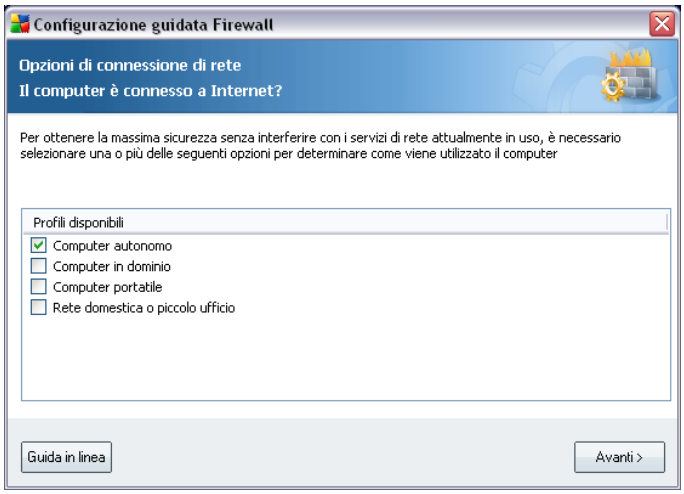
AVG 8.5 Internet Security è stato configurato. Premere il pulsante ***Fine*** per iniziare a lavorare con AVG.

7. Configurazione guidata del firewall

La Configurazione guidata del firewall viene avviata automaticamente subito dopo l'installazione di **AVG 8.5 Internet Security** . Anche se è possibile configurare in seguito i parametri del componente, è consigliabile eseguire la configurazione guidata' per assicurarsi che il componente ***Firewall*** funzioni correttamente.

Configurazione guidata del firewall può essere richiamato anche direttamente dall'interfaccia di Firewall premendo il pulsante ***Configurazione guidata*** .

7.1. Opzioni di connessione di rete



In questa finestra di dialogo della ***Configurazione guidata del firewall*** viene chiesta la modalità di connessione del computer a Internet. Ad esempio, un notebook che si connette a Internet da molti luoghi diversi (*aeroporti, camere d'albergo e così via*) richiede regole di protezione più rigide rispetto a un computer in un dominio (*rete aziendale e così via)*). In base al tipo di connessione selezionata le regole predefinite di ***Firewall*** verranno definite con un diverso livello di protezione.

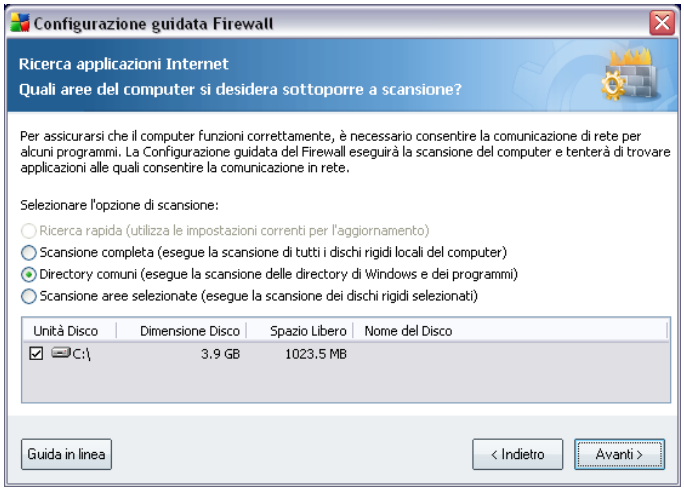
Sono disponibili tre opzioni:

- ***Computer autonomo***
- ***Computer in dominio*** (rete aziendale)
- ***Computer portatile*** (normalmente un notebook)

- ***Rete domestica o di piccoli uffici***

In questa finestra di dialogo scegliere i tipi di connessione che meglio si adattano al normale utilizzo del computer. È possibile selezionare più opzioni che corrispondono all'utilizzo corrente del computer. Confermare la selezione facendo clic sul pulsante ***Avanti***, quindi procedere alla finestra di dialogo successiva.

7.2. Scansione di applicazioni Internet



Per impostare la configurazione iniziale di ***Firewall*** è necessario eseguire la scansione del computer e definire tutte le applicazioni e i servizi di sistema che dovranno comunicare in rete. È necessario creare regole iniziali di ***Firewall*** per tutte queste applicazioni e tutti questi servizi.

Nota: *la procedura guidata consente di rilevare tutte le applicazioni generalmente note che stabiliscono comunicazioni in rete e definire le regole per tali applicazioni. Non è tuttavia in grado di rilevare tutte le applicazioni di questo tipo.*

Nella finestra di dialogo ***Ricerca applicazioni Internet*** è necessario scegliere se si desidera eseguire:

- ***Ricerca rapida***: questa opzione è attiva solo se il componente ***Firewall*** è stato precedentemente configurato. Potranno essere rilevate solo le applicazioni attualmente salvate nella configurazione di ***Firewall*** esistente. A queste verrà quindi applicata una configurazione predefinita (ovvero consigliata dal produttore). Non verranno rilevate applicazioni nuove. Questa opzione è consigliata se le regole di ***Firewall*** sono già state definite e si desidera evitare di ripetere l'intero processo di scansione.

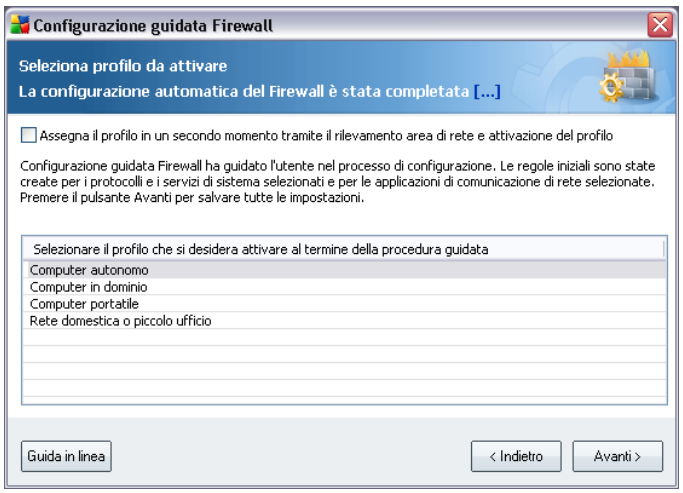
- ***Scansione completa***: esegue la scansione di tutti i dischi rigidi locali del computer
- ***Directory comuni***: (*impostazione predefinita*) esegue la scansione esclusivamente delle directory dei programmi e di Windows, l'intervallo di scansione è significativamente più breve
- ***Scansione di aree selezionate***: specifica le unità disco rigido selezionate da sottoporre a scansione

7.3. Seleziona profilo da attivare

Nella finestra di dialogo ***Seleziona profilo da attivare*** sono visualizzate informazioni relative alla configurazione del ***Firewall*** impostata nelle finestre di dialogo precedenti.

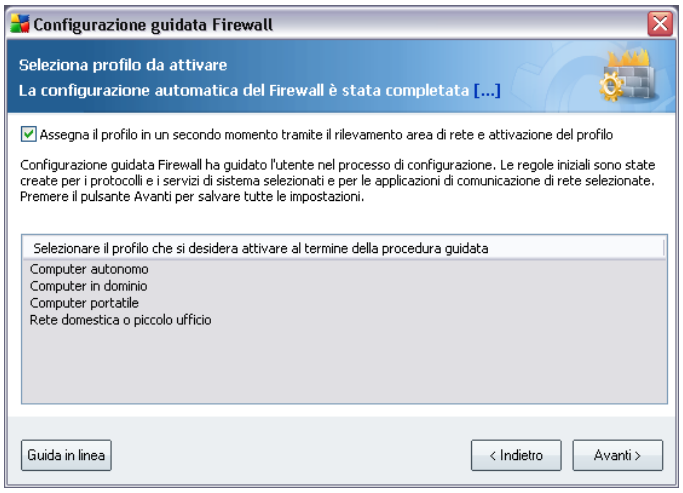
Prima di chiudere la ***Configurazione guidata del firewall***, è necessario selezionare il profilo da utilizzare per il computer. È possibile scegliere tra tre opzioni (Computer autonomo, Computer in dominio e Computer portatile) in base ai parametri di connessione specificati nella prima finestra di dialogo (***Opzioni di connessione di rete***) della procedura guidata. In seguito sarà possibile passare da un profilo predefinito ***Firewall*** all'altro in base allo stato corrente del computer.

È sufficiente selezionare il profilo desiderato dall'elenco e attivarlo facendo clic sul pulsante ***Avanti***:



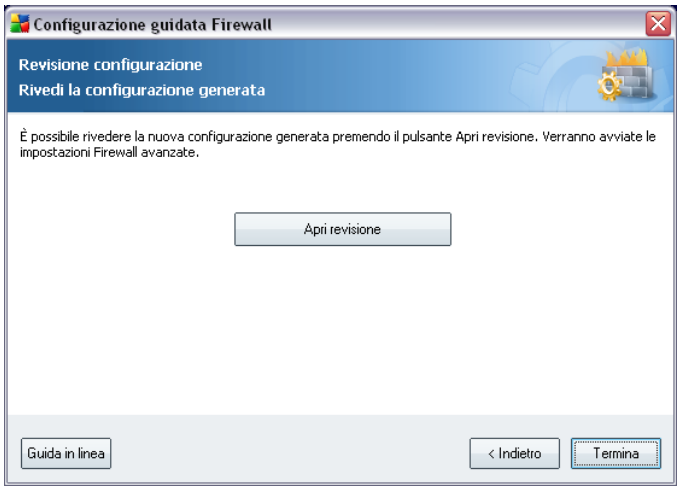
Se non si desidera impostare i profili manualmente, è possibile attivare la funzione di rilevamento automatico del profilo. In tal caso, il ***Firewall*** selezionerà

automaticamente il profilo più appropriato in base alla posizione e alla modalità di connessione del computer alla rete. La selezione automatica dei profili garantisce la massima protezione. Per scegliere questa opzione, selezionare la voce ***Assegna il profilo in un secondo momento tramite il rilevamento area di rete e attivazione del profilo*** nella parte superiore della finestra di dialogo:



In questo modo l'elenco dei profili viene disattivato. Selezionare quindi il pulsante ***Avanti*** per accedere alla successiva finestra di dialogo della procedura guidata.

7.4. Revisione della configurazione



La finestra ***Revisione della configurazione*** chiude la ***Configurazione guidata del***

firewall. Fare clic sul pulsante ***Fine*** per finalizzare le impostazioni iniziali del ***Firewall***. Se si desidera visualizzare una panoramica dei parametri di impostazione o continuare con la configurazione dettagliata del componente ***Firewall***, premere il pulsante ***Apri revisione*** per passare all'interfaccia di modifica ***Impostazioni del firewall***.

8. Dopo l'installazione

8.1. Registrazione del prodotto

Una volta completata l'installazione di **AVG 8.5 Internet Security** , registrare il prodotto on line dal sito Web di AVG, nella pagina ***Registrazione*** (*seguire le istruzioni fornite direttamente nella pagina*). Dopo la registrazione sarà possibile ottenere l'accesso completo all'account utente AVG, alla newsletter di aggiornamento AVG e ad altri servizi offerti esclusivamente agli utenti registrati.

8.2. Accesso all'interfaccia utente

È possibile accedere a ***Interfaccia utente di AVG*** in diversi modi:

- fare doppio clic sull'icona di AVG sulla barra delle applicazioni
- fare doppio clic sull'icona di AVG sul desktop
- dal menu ***Start/Tutti i programmi/AVG 8.0/Interfaccia utente di AVG***

8.3. Scansione dell'intero computer

Esiste il rischio potenziale che un virus sia stato trasmesso al computer dell'utente prima dell'installazione di **AVG 8.5 Internet Security** . Per questo motivo è necessario eseguire ***Scansione intero computer*** per assicurarsi che non siano presenti infezioni sul PC.

Per istruzioni sull'esecuzione di ***Scansione intero computer*** consultare il capitolo ***Scansione AVG***.

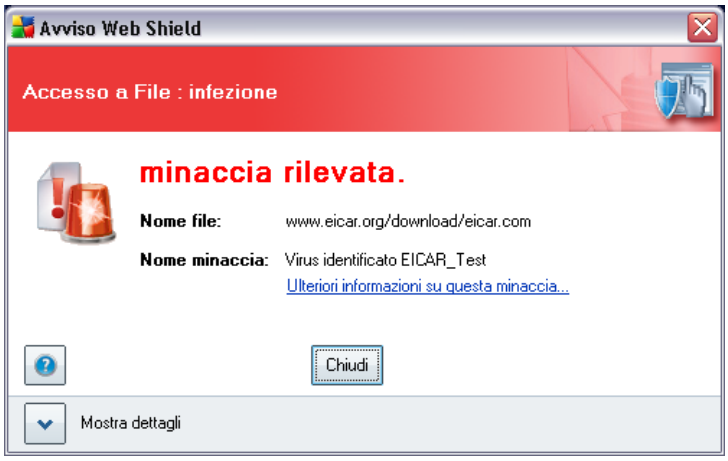
8.4. Controllo Eicar

Per assicurarsi della corretta installazione di **AVG 8.5 Internet Security** , è possibile eseguire il Controllo EICAR.

Il Controllo EICAR è un metodo standard e assolutamente sicuro per verificare il funzionamento del sistema antivirus. La sua esecuzione è sicura perché non si tratta di un vero virus e non include frammenti del codice di qualche virus. La maggior parte dei prodotti reagisce a questo controllo come se fosse un virus *anche se normalmente lo segnalano con un nome ovvio come "EICAR-AV-Test"*. È possibile scaricare il virus EICAR dal sito Web di EICAR all'indirizzowww.eicar.com dove si troveranno anche

tutte le informazioni necessarie sul controllo ECAR.

Provare a scaricare il file ***eicar.com*** e salvarlo sul disco locale. Subito dopo aver confermato il download del file di controllo, il componente ***Web Shield*** visualizzerà un avviso. Questo avviso di ***Web Shield*** segnala che AVG è stato installato correttamente nel computer.



Se AVG non identifica il file di controllo EICAR come un virus, è necessario controllare nuovamente la configurazione del programma.

8.5. Configurazione predefinita di AVG

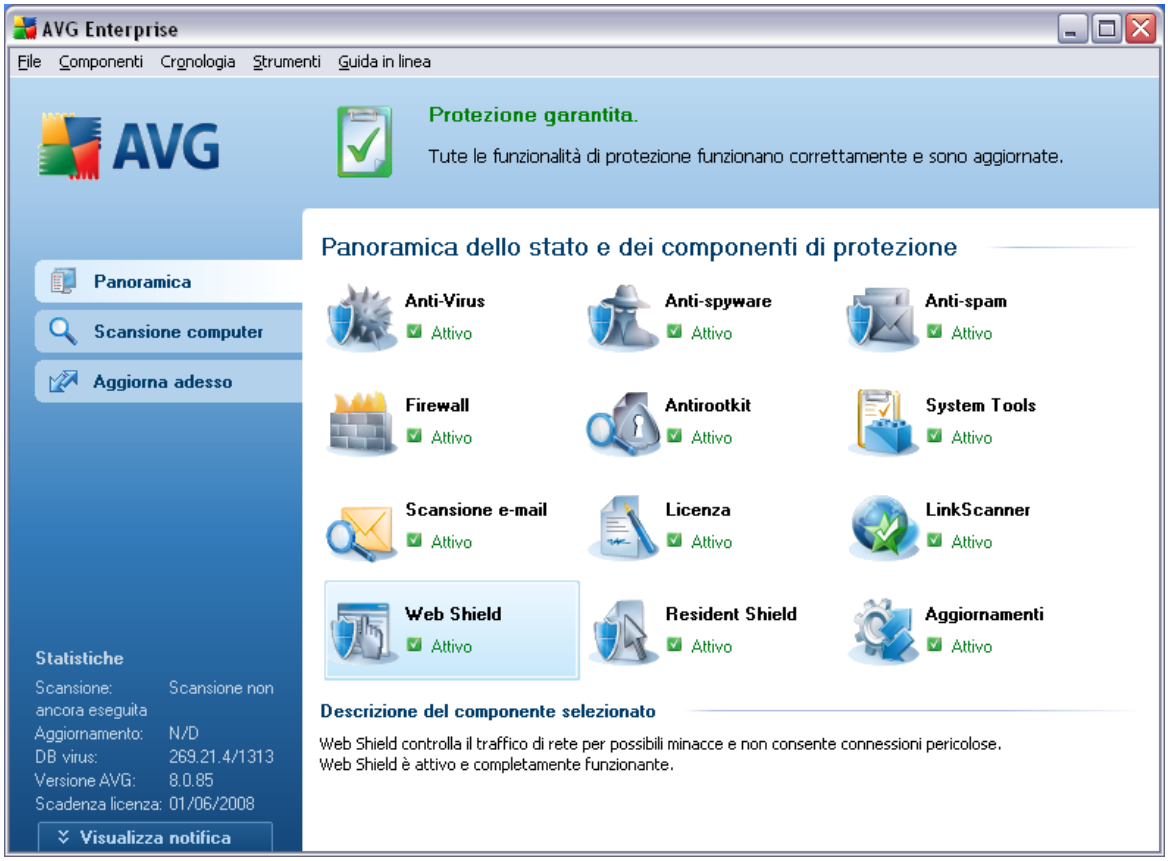
La configurazione predefinita (*ovvero la modalità di impostazione dell'applicazione dopo l'installazione*) di **AVG 8.5 Internet Security** è impostata dal fornitore di software in modo tale che tutti i componenti e le funzioni offrano un'ottimizzazione massima di prestazioni.

A meno che non ci sia una ragione valida, si consiglia di non modificare la configurazione di AVG. Le modifiche alle impostazioni dovrebbero essere eseguite solo da un utente esperto.

È possibile apportare alcune modifiche minori alle impostazioni dei componenti di AVG direttamente dall'interfaccia utente del componente specifico. Se è necessario cambiare la configurazione di AVG per adeguare meglio l'applicazione alle proprie esigenze, accedere a ***Impostazioni AVG avanzate***: selezionare la voce di menu di sistema ***Strumenti/Impostazioni avanzate*** e modificare la configurazione di AVG nelal finestra di dialogo ***Impostazioni AVG avanzate*** visualizzata.

9. Interfaccia utente di AVG

AVG 8.5 Internet Security apertura con la finesta principale:



La finestra principale è suddivisa in diverse sezioni:

- ***Menu di sistema*** *(riga di sistema superiore nella finestra)* è l'esplorazione standard che consente di accedere a tutti i componenti, i servizi e le funzionalità di AVG - dettagli >>
- ***Informazioni sullo stato di protezione*** *(sezione superiore della finestra)* fornisce informazioni sullo stato corrente del programma AVG - dettagli >>
- ***Collegamenti veloci*** *(sezione a sinistra della finestra)* consentono di accedere rapidamente alle attività più importanti e più utilizzate di AVG - dettagli >>

- ***Panoramica dei componenti*** *(sezione centrale della finestra)* offre una panoramica di tutti i componenti AVG installati - dettagli >>

- ***Statistiche*** *(pulsante a sinistra nella finestra)* offre tutti i dati statistici relativi al funzionamento del programma - dettagli >>

- ***Icona sulla barra delle applicazioni*** *(angolo inferiore destro del monitor, sulla barra delle applicazioni)* indica lo stato corrente di AVG - dettagli >>

9.1. Menu di sistema

Menu di sistema è l'esplorazione standard utilizzata in tutte le applicazioni Windows. Si trova orizzontalmente nella parte superiore della finestra principale **AVG 8.5 Internet Security** . Utilizzare il menu di sistema per accedere a componenti, funzioni e servizi specifici di AVG.

Il menu di sistema è suddiviso in cinque sezioni principali:

9.1.1. File

- ***Esci***: consente di chiudere l'interfaccia utente di **AVG 8.5 Internet Security** . Tuttavia, l'applicazione AVG continuerà a essere eseguita in background e il computer sarà comunque protetto.

9.1.2. Componenti

Nella voce ***Componenti*** del menu di sistema sono inclusi i collegamenti a tutti i componenti di AVG installati che consentono di aprire la finestra di dialogo predefinita nell'interfaccia utente:

- ***Panoramica sistema***: consente di passare alla finestra di dialogo dell'interfaccia utente predefinita contenente una panoramica di tutti i componenti installati e dello stato relativo

- ***Anti-Virus***: consente di aprire la pagina predefinita del componente ***Anti-Virus***

- ***Anti-Rootkit*** : consente di aprire la pagina predefinita del componente ***Anti-Rootkit***

- ***Anti-Spyware***: consente di aprire la pagina predefinita del componente ***Anti-Spyware***

- ***Firewall*** : consente di aprire la pagina predefinita del componente ***Firewall***

- ***Utilità di sistema***: consente di aprire la pagina predefinita del componente ***System Tools***
- ***Anti-Spam***: consente di aprire la pagina predefinita del componente ***Anti-Spam***
- ***Scansione E-mail***: consente di aprire la pagina predefinita del componente ***Scansione E-mail***
- ***Licenza***: consente di aprire la pagina predefinita del componente ***Licenza***
- ***LinkScanner:*** consente di aprire la pagina predefinita del componente ***LinkScanner***
- ***Web Shield***: consente di aprire la pagina predefinita del componente ***Web Shield***
- ***Resident Shield***: consente di aprire la pagina predefinita del componente ***Resident Shield***
- ***Aggiornamenti***: consente di aprire la pagina predefinita del componente ***Aggiornamenti***

9.1.3. Cronologia

- ***Risultati scansione***: consente di visualizzare l'interfaccia di controllo di AVG, in particolare la finestra di dialogo ***Panoramica dei risultati***.
- ***Rilevamenti Resident Shield*** : consente di aprire una finestra di dialogo con una panoramica delle minacce rilevate da ***Resident Shield***
- ***Rilevamento scansione e-mail*** : consente di aprire una finestra di dialogo con una panoramica dei messaggi di posta elettronica rilevati come pericolosi dal componente ***Scansione e-mail***.
- ***Rilevamenti di Web Shield***: consente di aprire una finestra di dialogo con una panoramica delle minacce rilevate da ***Web Shield***
- ***Quarantena virus***: consente di aprire l'interfaccia della finestra di quarantena (***Quarantena virus***) in cui AVG sposta tutte le infezioni rilevate che per qualche motivo non è possibile eliminare automaticamente. All'interno della quarantena i file infetti sono isolati e la protezione del computer è garantita. Allo stesso tempo, i file infetti vengono archiviati per una possibile riparazione futura.

- ***Log della Cronologia eventi***: consente di aprire l'interfaccia della Cronologia eventi con una panoramica di tutte le azioni**AVG 8.5 Internet Security** registrate.

- ***Firewall***: consente di aprire l'interfaccia di impostazione del Firewall sulla scheda ***Log*** con una panoramica dettagliata di tutte le azioni del componente Firewall

9.1.4. Strumenti

- ***Scansione computer***: consente di passare all'interfaccia di scansione di AVG e di avviare una scansione dell'intero computer.

- ***Scansione cartella selezionata***: consente di passare all'interfaccia di scansione di AVG e di definire i file e le cartelle da sottoporre a scansione nella struttura del computer.

- ***Scansione file***: consente di eseguire un controllo su richiesta di un singolo file selezionato dalla struttura del disco.

- ***Aggiorna***: consente di avviare automaticamente il processo di aggiornamento di **AVG 8.5 Internet Security**

- ***Aggiorna da directory***: consente di eseguire il processo di aggiornamento dai file di aggiornamento che si trovano in una cartella specifica sul disco locale. Tuttavia, questa opzione è consigliabile solo in caso di emergenza, come situazioni in cui non si ottiene la connessione a Internet (*ad esempio, il computer è stato infettato e si è disconnesso da Internet, il computer è connesso a una rete senza accesso a Internet e così via*). Nella finestra appena aperta selezionare la cartella in cui è stato precedentemente posizionato il file di aggiornamento e avviare il processo di aggiornamento.

- ***Impostazioni avanzate***: consente di aprire la finestra di dialogo ***Impostazioni avanzate di AVG*** dove è possibile modificare la configurazione di **AVG 8.5 Internet Security** . In genere è consigliabile mantenere le impostazioni predefinite dell'applicazione definite dal fornitore di software.

- ***Impostazioni Firewall***: consente di aprire una finestra di dialogo autonoma per la configurazione avanzata del componente ***Firewall***.

9.1.5. Guida in linea

- ***Sommario***: consente di aprire i file della Guida di AVG

- ***Utilizza Guida in linea***: consente di aprire il sito Web di AVG alla pagina del

centro di assistenza clienti

- ***Web AVG personale***: consente di aprire la pagina iniziale di AVG (all'indirizzo www.avg.com)
- ***Informazioni sui virus e sulle minacce***: consente di aprire l'***Enciclopedia dei virus*** in rete in cui è possibile trovare informazioni dettagliate sul virus identificato
- ***Riattiva***: consente di aprire la finestra di dialogo ***Attiva AVG*** con i dati immessi nella finestra di dialogo ***Personalizza AVG*** del processo di installazione. In questa finestra di dialogo è possibile immettere il numero di licenza per sostituire il numero di vendita (*il numero con cui è stata eseguita l'installazione di AVG*) o il numero di licenza in uso (*ad esempio, durante l'aggiornamento a un nuovo prodotto AVG*).
- ***Registra ora***: consente di connettersi al sito Web di registrazione all'indirizzo www.avg.com. Immettere i dati di registrazione; solo i clienti che registrano il proprio prodotto AVG possono ricevere assistenza tecnica gratuita.
- ***Informazioni su AVG***: consente di aprire la finestra di dialogo ***Informazioni*** che include cinque schede in cui sono disponibili dati sul nome del programma, la versione del database dei virus e del programma, informazioni sul sistema, il contratto di licenza e le informazioni di contatto di ***AVG Technologies CZ***.

9.2. Informazioni sullo stato di protezione

La sezione ***Informazioni sullo stato di protezione*** si trova nella parte superiore della finestra principale di AVG. All'interno di questa sezione sono contenute le informazioni sullo stato di protezione corrente di **AVG 8.5 Internet Security** . Vedere la panoramica delle icone possibilmente colorate in questa sezione e il relativo significato:

 L'icona verde indica che AVG è completamente operativo. Il computer è totalmente protetto, aggiornato e tutti i componenti installati funzionano correttamente.

 L'icona arancione indica la configurazione non corretta di uno o più componenti invitando a prestare attenzione alle relative proprietà/impostazioni.

Non sono presenti problemi gravi in AVG e probabilmente è stato già deciso di disattivare alcuni componenti per qualche ragione. La protezione di AVG è ancora attiva. Tuttavia, prestare attenzione alle proprietà del componente in cui si sono verificati problemi. Il nome verrà fornito nella sezione ***Informazioni sullo stato di protezione*** .

Questa icona viene inoltre visualizzata se, per qualche motivo, l'utente ha deciso di ignorare lo stato di errore di un componente (l'opzione "***Ignora stato del componente***" è disponibile nel menu contestuale che viene aperto facendo clic con il pulsante destro del mouse sull'icona del componente pertinente nella panoramica dei componenti della finestra principale di AVG). Potrebbe essere necessario utilizzare "***Ignora stato del componente***" in situazioni particolari, tuttavia si consiglia di disattivare questa opzione nel più breve tempo possibile.

 L'icona rossa indica che lo stato di AVG è critico. Uno o più componenti non funzionano correttamente e AVG non è in grado di proteggere il computer. Intervenire immediatamente per risolvere il problema segnalato. Se non si è in grado di correggere l'errore, contattare il team di assistenza tecnica di AVG.

Si consiglia di prestare attenzione alla sezione ***Informazioni sullo stato di protezione*** e, nel caso in cui fosse segnalato un problema, procedere cercando di risolverlo immediatamente. In caso contrario, il computer è a rischio.

Nota: *le informazioni sullo stato di AVG sono sempre disponibili anche dall'icona sulla barra delle applicazioni.*

9.3. Collegamenti veloci

Collegamenti rapidi *(nella sezione a sinistra di Interfaccia utente di AVG)* consentono di accedere immediatamente alle funzionalità più importanti e più utilizzate di AVG:

- ***Panoramica***: utilizzare questo collegamento per passare da una qualsiasi interfaccia di AVG visualizzata a quella predefinita contenente una panoramica di tutti i componenti installati: vedere il capitolo ***Panoramica dei componenti >>***

- ***Scansione computer***: utilizzare questo collegamento per aprire l'interfaccia di scansione di AVG che consente di eseguire direttamente controlli, scansioni pianificate oppure modificare i parametri: vedere il capitolo ***Controlli AVG >>***

- ***Aggiorna subito***: questo collegamento consente di aprire un'interfaccia di aggiornamento e di avviare immediatamente il processo di aggiornamento di AVG: vedere il capitolo ***Aggiornamenti di AVG>>***

Questi collegamenti sono accessibili in qualsiasi momento dall'interfaccia utente. Una volta che si utilizza un collegamento rapido per eseguire un processo specifico, l'interfaccia utente grafica visualizzerà una nuova finestra di dialogo anche se i collegamenti rimarranno comunque disponibili. Inoltre, il processo in esecuzione viene visualizzato con un'ulteriore rappresentazione grafica: *vedere l'immagine 2*.

9.4. Panoramica dei componenti

La sezione ***Panoramica dei componenti*** si trova nella parte centrale di Interfaccia utente di AVG. La sezione è suddivisa in due parti:

- Panoramica di tutti i componenti installati costituita da un pannello con l'icona del componente e le informazioni sullo stato attivo o inattivo del componente stesso
- Descrizione di un componente selezionato

Nella sezione **AVG 8.5 Internet Security** the ***Panoramica dei componenti*** sono contenute le informazioni sui componenti seguenti:

- ***Anti-Virus*** assicura che il computer sia protetto da virus che tentano di accedere al computer - dettagli >>
- ***Anti-Spyware*** esegue la scansione in background delle applicazioni mentre queste vengono eseguite - dettagli >>
- ***Anti-Spam*** controlla tutti i messaggi di posta elettronica in entrata e contrassegna quelli indesiderati come SPAM - dettagli >>
- ***Anti-Rootkit*** rileva i programmi e le tecnologie che tentano di camuffare il malware - dettagli >>
- ***System Tools*** offre un riepilogo dettagliato dell'ambiente AVG - dettagli >>
- ***Firewall*** controlla il modo in cui il computer scambia dati con altri computer in Internet o nella rete locale - dettagli >>
- ***Scansione e-mail*** controlla la posta in entrata e in uscita per rilevare virus - dettagli >>
- ***Licenza*** fornisce l'intero contenuto del contratto di licenza - dettagli >>
- ***LinkScanner*** consente di verificare i risultati della ricerca visualizzati nel browser Internet dettagli >>
- ***Web Shield*** esegue la scansione di tutti i dati scaricati da un browser Web - dettagli >>
- ***Resident Shield*** viene eseguito in background ed esegue la scansione dei file mentre vengono copiati, aperti o salvati - dettagli >>

- ***Aggiornamenti*** controlla tutti gli aggiornamenti AVG - dettagli >>

Fare clic sull'icona di un componente per evidenziarlo all'interno della panoramica dei componenti. Contemporaneamente, viene visualizzata la descrizione delle funzionalità di base del componente nella parte inferiore dell'interfaccia utente. Fare doppio clic sull'icona per aprire l'interfaccia dei componenti con un elenco dei dati statistici di base.

Fare clic con il pulsante destro del mouse sull'icona di un componente per visualizzare un menu contestuale: oltre ad aprire l'interfaccia grafica del componente, è possibile selezionare l'opzione ***Ignora stato del componente***. Selezionare questa opzione per confermare che si è al corrente dello stato di errore del componente, tuttavia si desidera mantenere AVG nella condizione corrente e non si desidera ricevere notifiche tramite la visualizzazione in grigio dell'icona presente nella barra delle applicazioni.

9.5. Statistiche

La sezione ***Statistiche*** si trova nella parte inferiore a sinistra di Interfaccia utente di AVG. In essa è contenuto l'elenco delle informazioni in relazione al funzionamento del programma:

- ***Ultima scansione***: indica la data dell'ultima esecuzione della scansione
- ***Ultimo aggiornamento***: indica la data di avvio dell'ultimo aggiornamento
- ***Virus DB***: contiene informazioni sulla versione correntemente installata del database di virus
- ***Versione di AVG***: contiene informazioni sulla versione AVG installata *(il formato del numero è 8.0.xx, dove 8.0 indica la versione della linea del prodotto e xx indica il numero di build)*
- ***Scadenza licenza:***: indica la data della scadenza della licenza di AVG

9.6. Icona della barra delle applicazioni

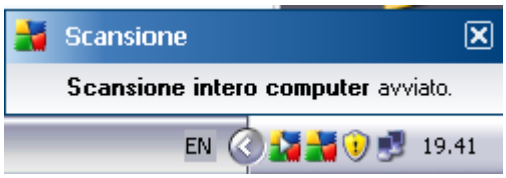
L'icona sulla barra delle applicazioni (*sulla barra delle applicazioni di Windows*) indica lo stato corrente di **AVG 8.5 Internet Security** . È possibile visualizzarla in qualsiasi momento sulla barra delle applicazioni indipendentemente dall'apertura o meno della finestra principale di AVG.

Se è completamente colorata , l'***icona della barra delle applicazioni*** indica che tutti i componenti di AVG sono attivi e funzionano correttamente. Inoltre, l'icona AVG della barra delle applicazioni può venire visualizzata completamente colorata se AVG

si trova in stato di errore ma l'utente è consapevole di questa situazione e ha deliberatamente attivato l'opzione ***Ignora stato del componente***.

Un'icona di colore grigio con un punto esclamativo indica un problema (componente inattivo, stato di errore e così via). Fare doppio clic sull'***icona sulla barra delle applicazioni*** per aprire la finestra principale e modificare un componente.

L'icona presente nella barra delle applicazioni informa inoltre l'utente circa attività AVG correnti ed eventuali modifiche dello stato del programma (*ad esempio avvio automatico di una scansione o un aggiornamento pianificato, variazione del profilo del firewall, modifica dello stato di un componente, occorrenza di uno stato di errore e così via*) tramite una finestra a comparsa che si apre sopra l'icona stessa:



L'***icona sulla barra delle applicazioni*** può anche essere utilizzata come collegamento rapido per accedere alla finestra principale di AVG in qualsiasi momento. Fare doppio clic sull'icona. Se si fa clic con il pulsante destro del mouse sull'***icona presente nella barra delle applicazioni***, viene aperto un menu di scelta rapida contenente le opzioni seguenti:

- ***Apri interfaccia utente di AVG***: fare clic sull'opzione per aprire Interfaccia utente di AVG
- ***Aggiornamento***: viene avviato un aggiornamento immediato
- ***Esci***: fare clic sull'opzione per chiudere AVG *(viene chiusa solo l'interfaccia utente, l'esecuzione di AVG prosegue in background garantendo la completa protezione del computer).*

10. Componenti di AVG

10.1.Anti-Virus

10.1.1.Anti-Virus Principi

Il motore di scansione del software antivirus esegue la scansione di tutti i file e delle operazioni sui file (apertura/chiusura di file e così via) per i virus noti. Tutti i virus rilevati verranno bloccati per essere poi ripuliti o messi in quarantena. La maggior parte dei software antivirus utilizza anche la scansione euristica che consente di rilevare le caratteristiche tipiche di virus, le cosiddette firme virali. In questo modo la scansione antivirus è in grado di rilevare un nuovo virus sconosciuto, se il nuovo virus contiene alcune caratteristiche tipiche dei virus esistenti.

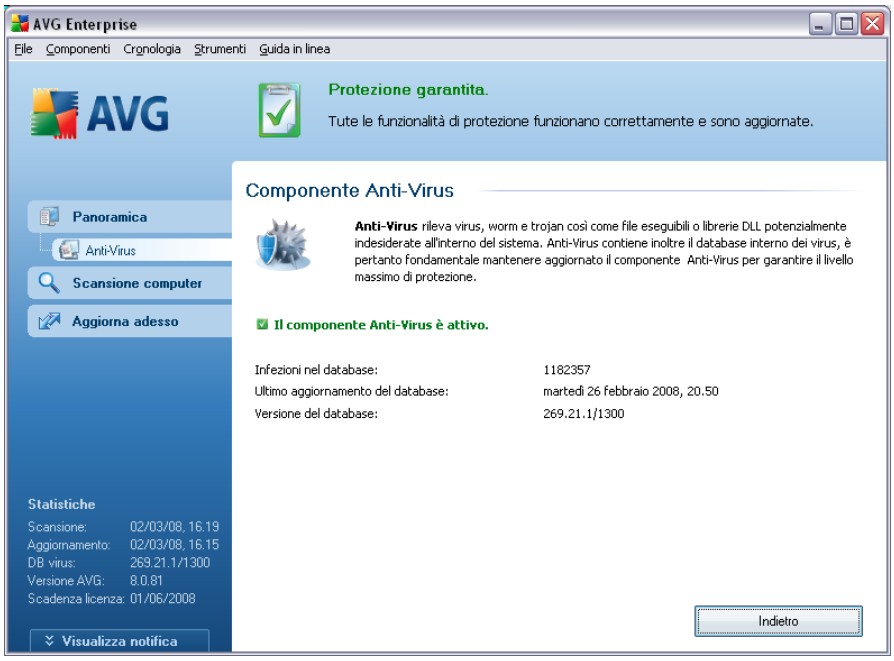
La funzione principale della protezione antivirus è impedire l'esecuzione di virus noti sul computer.

Se una sola tecnologia potrebbe avere esito negativo nel rilevamento o nell'identificazione di un virus, il componente ***Anti-Virus*** combina diverse tecnologie per assicurare che il computer sia protetto da virus:

- Scansione: ricerca di stringhe di caratteri specifiche di un determinato virus.
- Analisi euristica: emulazione dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale
- Rilevamento generale: rilevamento di istruzioni caratteristiche del virus o del gruppo di virus specifico

Inoltre AVG è in grado di analizzare e rilevare le applicazioni eseguibili o le librerie DLL che potrebbero essere potenzialmente indesiderate nel sistema. Queste minacce vengono denominate Programmi potenzialmente indesiderati (vari tipi di spyware, adware e così via). Inoltre, AVG esegue la scansione del Registro di sistema alla ricerca di voci sospette e file Internet temporanei e cookie e consente di trattare tutti gli elementi potenzialmente dannosi allo stesso modo delle altre infezioni.

10.1.2.Interfaccia Anti-Virus



L'interfaccia del componente ***Anti-Virus*** fornisce alcune informazioni di base relative alla funzionalità del componente, ovvero le informazioni sullo stato corrente del componente (*Il componente Anti-Virus è attivo.*) e una breve panoramica delle statistiche di ***Anti-Virus*** :

- ***Definizioni infezioni***: indica il numero dei virus definiti nella versione aggiornata del database di virus
- ***Ultimo aggiornamento del database***: specifica quando e a che ora è stato eseguito l'utlimo aggiornamento del database di virus
- ***Versione del database***: indica il numero della versione più recente del database di virus. Il numero aumenta dopo ogni aggiornamento di base dei virus

È presente un solo pulsante operativo nell'interfaccia di questo componente (***Indietro***): premere il pulsante per tornare all'interfaccia utente di AVG predefinita (panoramica dei componenti).

Nota: *il fornitore di software ha impostato tutti i componenti AVG per fornire prestazioni ottimali. A meno che non ci sia una ragione valida, si consiglia di non modificare la configurazione di AVG. Tutte le eventuali modifiche alle impostazioni*

*dovrebbero essere eseguite da un utente esperto. Se è necessario modificare la configurazione di AVG, selezionare la voce di menu di sistema **Strumenti / Impostazioni avanzate** e modificare la configurazione di AVG nella finestra di dialogo Impostazioni AVG avanzate visualizzata.*

10.2.Anti-Spyware

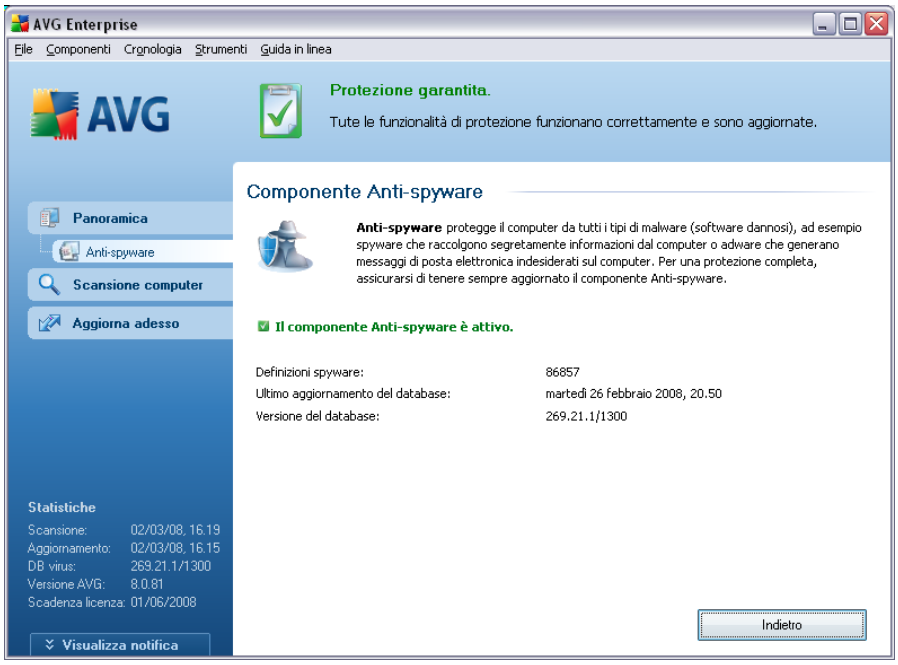
10.2.1.Anti-Spyware Principi

In genere, per spyware si intende un particolare tipo di malware, ovvero un software che raccoglie informazioni dal computer senza informarne l'utente e senza richiederne l'autorizzazione. Alcune applicazioni spyware possono anche essere installate intenzionalmente e spesso contengono annunci pubblicitari, finestre popup o altri tipi di software indesiderato.

Attualmente la fonte più comune di infezione sono i siti Web con contenuto potenzialmente pericoloso. Anche altri metodi di trasmissione, quali ad esempio i messaggi di e-mail o le trasmissioni tramite worm e virus, sono molto diffusi. La protezione più importante consiste nell'utilizzo di un programma di scansione in background sempre attivo, ***Anti-Spyware***, che funziona come una protezione permanente ed esegue la scansione in background delle applicazioni mentre queste vengono eseguite.

Esiste anche il rischio potenziale che il malware sia stato trasmesso al computer dell'utente prima dell'installazione di AVG oppure che si sia dimenticato di aggiornare **AVG 8.5 Internet Security** con il database e gli aggiornamenti del programma. Per questo motivo AVG consente di eseguire una scansione completa del computer alla ricerca di malware/spyware mediante la funzione di scansione. Consente inoltre di rilevare malware inattivo e innocuo, ovvero che è stato scaricato ma non ancora attivato.

10.2.2.Interfaccia Anti-Virus



L'interfaccia del componente ***Anti-Spyware*** fornisce una breve panoramica della funzionalità del componente, ovvero le informazioni sullo stato corrente (*Il componente Anti-Spyware è attivo.*) e alcune statistiche di ***Anti-Spyware*** :

- ***Definizioni spyware***: indica il numero di campioni di spyware definiti nella versione più recente del database di spyware
- ***Ultimo aggiornamento del database***: specifica quando e a che ora è stato eseguito l'utlimo aggiornamento del database di spyware
- ***Versione del database***: indica il numero della versione più recente del database di spyware. Il numero aumenta dopo ogni aggiornamento di base dei virus

È presente un solo pulsante operativo nell'interfaccia di questo componente (***Indietro***): premere il pulsante per tornare all'interfaccia utente di AVG predefinita (panoramica dei componenti).

Nota: il *fornitore di software ha impostato tutti i componenti AVG per fornire prestazioni ottimali. A meno che non ci sia una ragione valida, si consiglia di non modificare la configurazione di AVG. Tutte le eventuali modifiche alle impostazioni dovrebbero essere eseguite da un utente esperto. Se è necessario modificare la*

*configurazione di AVG, selezionare la voce di menu di sistema **Strumenti / Impostazioni avanzate** e modificare la configurazione di AVG nella finestra di dialogo Impostazioni AVG avanzate visualizzata.*

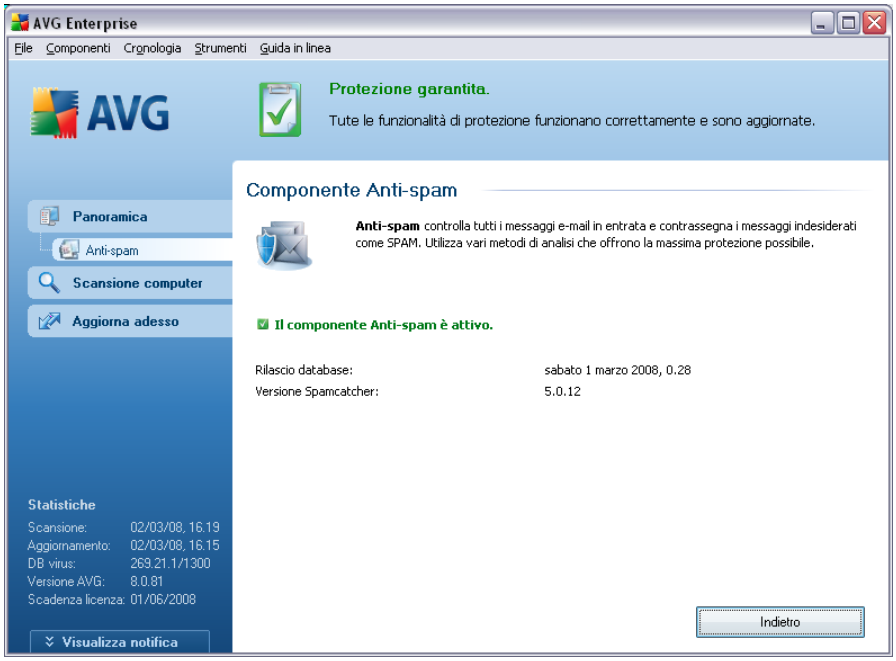
10.3.Anti-Spam

10.3.1.Principi Anti-Spam

Il termine "spam" indica messaggi di posta indesiderati, per lo più pubblicità di prodotti o servizi, inviati in massa e simultaneamente a un enorme numero di indirizzi di posta elettronica, che intasano le cassette postali dei destinatari. Lo spam non rientra nella categoria dei legittimi messaggi di posta elettronica commerciale per i quali i consumatori hanno fornito il loro consenso. Lo spam non è solo fastidioso ma può includere spesso anche truffe, virus o contenuti offensivi.

Anti-Spam controlla tutti i messaggi di posta elettronica in entrata e contrassegna quelli indesiderati come SPAM. Per elaborare ogni messaggio e-mail vengono utilizzati diversi metodi di analisi che offrono il massimo livello di protezione possibile contro i messaggi e-mail indesiderati.

10.3.2.Interfaccia Anti-Spam



Nella finestra di dialogo del componente ***Anti-Spam*** sono contenuti un breve testo che descrive la funzionalità del componente, le informazioni sullo stato corrente (*Il componente Anti-Spam è attivo.*) e le statistiche seguenti:

- ***Rilascio database***: specifica quando e a che ora il database di spam è stato aggiornato e pubblicato
- ***Versione di Spamcatcher***: indica il numero della versione più recente del motore anti-spam

È presente un solo pulsante operativo nell'interfaccia di questo componente (***Indietro***): premere il pulsante per tornare all'interfaccia utente di AVG predefinita (panoramica dei componenti).

Nota: *il fornitore di software ha impostato tutti i componenti AVG per fornire prestazioni ottimali. A meno che non ci sia una ragione valida, si consiglia di non modificare la configurazione di AVG. Tutte le eventuali modifiche alle impostazioni dovrebbero essere eseguite da un utente esperto. Se è necessario modificare la configurazione di AVG, selezionare la voce di menu di sistema* ***Strumenti / Impostazioni avanzate*** *e modificare la configurazione di AVG nella finestra di dialogo Impostazioni AVG avanzate visualizzata.*

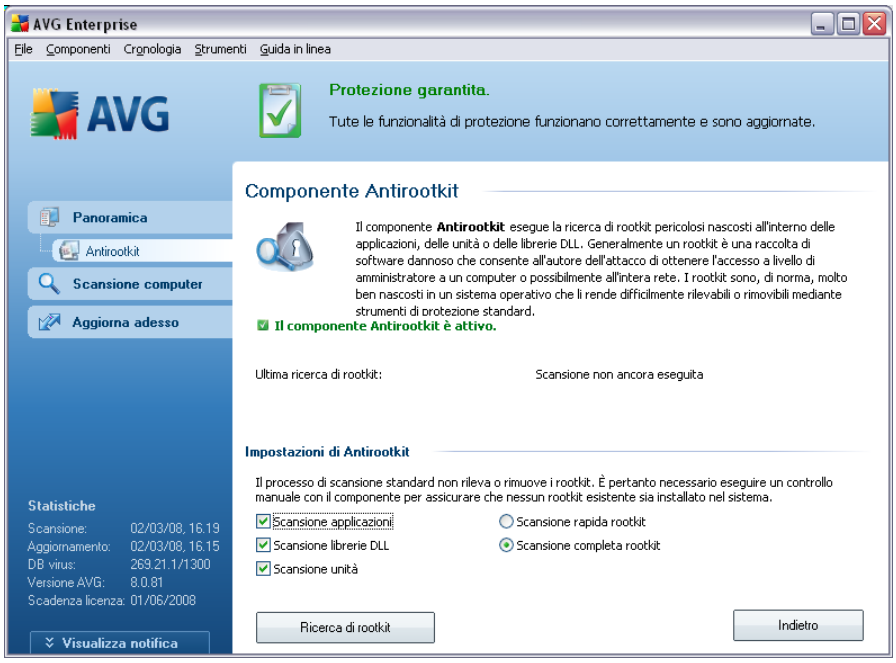
10.4.Anti-Rootkit

10.4.1.Principi Anti-Rootkit

Antirootkit è uno strumento specializzato per il rilevamento e la rimozione efficace di rootkit dannosi, quali programmi e tecnologie che possono camuffare la presenza di software dannoso sul computer.

Un rootkit è un programma progettato per assumere il controllo di base del sistema di un computer senza autorizzazione da parte dei proprietari di sistema e di gestori legittimi. L'accesso all'hardware è raramente necessario poiché un rootkit deve catturare il controllo del sistema operativo in esecuzione sull'hardware. In genere, i rootkit agiscono per nascondere la propria presenza sul sistema tramite sovversione o espedienti relativi ai meccanismi di protezione standard del sistema operativo. Si tratta spesso anche di trojan che ingannano gli utenti facendo loro credere che possono essere eseguiti in tutta sicurezza sui propri sistemi. Le tecniche utilizzate a questo scopo possono includere l'occultamento di processi in esecuzione da programmi di monitoraggio oppure di file o dati di sistema dal sistema operativo.

10.4.2.Interfaccia Anti-Rootkit



L'interfaccia utente di ***Anti-Rootkit*** fornisce una breve descrizione della funzionalità del componente informando sullo stato corrente del componente (*Il componente Anti-Rootkit è attivo.*) e indica l'ultimo avvio del controllo ***Anti-Rootkit***.

Nella parte inferiore della finestra di dialogo è contenuta la sezione ***Impostazioni Anti-Rootkit*** che consente di impostare alcune funzioni elementari della scansione per la presenza di rootkit. Selezionare innanzitutto le caselle di controllo corrispondenti per specificare gli oggetti da sottoporre a scansione:

- ***Scansione applicazioni***
- ***Scansione librerie DLL***
- ***Scansione unità***

Quindi, è possibile selezionare la modalità di scansione di rootkit:

- ***Scansione rapida rootkit***: esegue la scansione solo della cartella di sistema (*in genere c:\Windows*)
- ***Scansione completa rootkit***: esegue la scansione di tutti i dischi accessibili tranne A: e B:

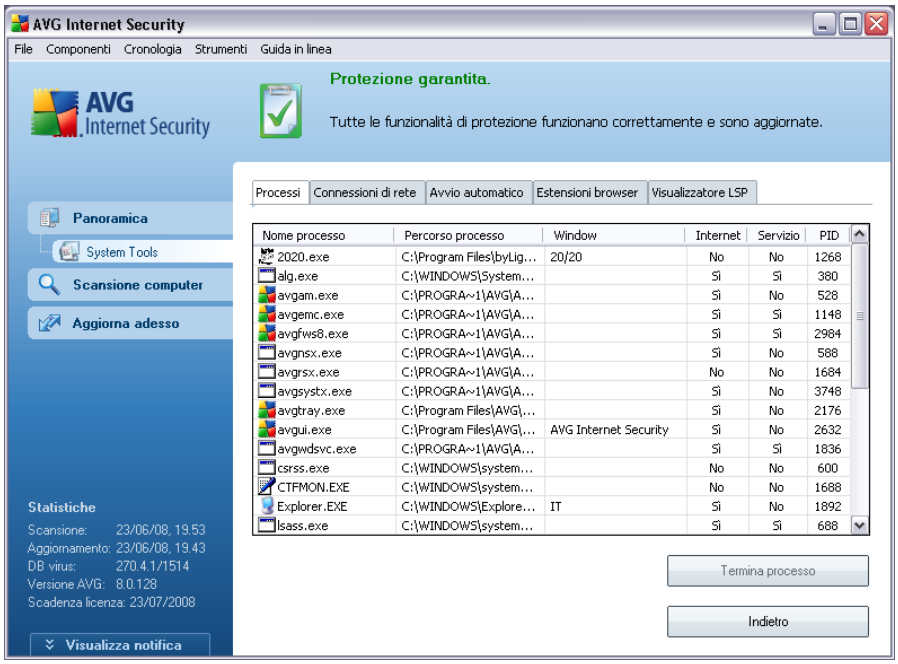
Pulsanti di controllo disponibili:

- ***Ricerca di rootkit***: poiché la scansione di rootkit non è una parte implicita di ***Scansione intero computer***, è possibile eseguire la scansione di rootkit direttamente dall'interfaccia ***Anti-Rootkit*** utilizzando questo pulsante
- ***Salva modifiche***: selezionare questo pulsante per salvare tutte le modifiche apportate in questa interfaccia e tornare all'***interfaccia utente di AVG*** predefinita (panoramica dei componenti)
- ***Annulla***: selezionare questo pulsante per tornare all'***interfaccia utente di AVG*** predefinita (panoramica dei componenti) senza salvare le modifiche apportate

10.5.System Tools

System Tools indica gli strumenti che offrono un riepilogo dettagliato dell'ambiente **AVG 8.5 Internet Security** . Il componente visualizza una panoramica dei processi in esecuzione, delle applicazioni avviate all'avvio del sistema operativo , delle connessioni di rete attive e così via. È anche possibile modificare panoramiche specifiche, ma questa operazione è consigliabile solo per gli utenti molto esperti.

10.5.1.Processi



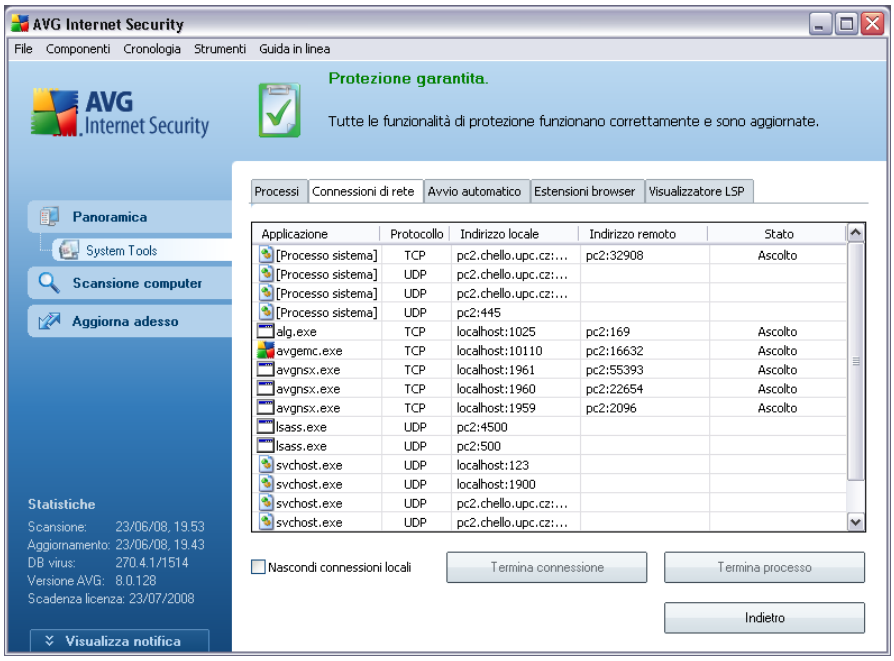
Nella finestra di dialogo ***Processi*** è incluso un elenco di processi (*ad esempio, applicazioni in esecuzione*) attualmente attivi sul computer. L'elenco è suddiviso in varie colonne:

- ***Nome processo***: nome del processo in esecuzione.
- ***Percorso***: percorso fisico del processo in esecuzione
- ***Finestra***: se applicabile, indica il nome della finestra dell'applicazione
- ***Internet***: indica se il processo in esecuzione è anche connesso a Internet (*Sì/No*).
- ***Servizio***: mostra se il processo in esecuzione è un servizio (*Sì/No*)
- ***PID***: il numero di identificazione del processo (Process Identification Number) è un numero interno di Windows univoco

È possibile selezionare una o più applicazioni e terminarle premendo il pulsante ***Termina processo.*** Il pulsante ***Indietro*** consente di tornare all'***interfaccia utente di AVG*** predefinita (panoramica dei componenti).

si consiglia di non terminare alcuna applicazione, se non si è assolutamente sicuri che rappresenta una reale minaccia!

10.5.2.Connessioni di rete



Nella finestra di dialogo ***Connessioni di rete*** è incluso un elenco di connessioni attualmente attive. L'elenco è suddiviso nelle seguenti colonne:

- ***Applicazione***: il nome dell'applicazione relativa alla connessione. Questa informazione è disponibile solo in Windows XP.
- ***Protocollo***: il tipo di protocollo di trasmissione utilizzato per la connessione:
  - TCP: protocollo utilizzato assieme al protocollo IP (Internet Protocol) per trasmettere le informazioni in Internet
  - UDP: protocollo alternativo al protocollo TCP.
- ***Indirizzo locale***: indirizzo IP del computer locale e il numero della porta utilizzata.
- ***Indirizzo remoto***: indirizzo IP del computer remoto e il numero della porta a cui viene eseguita la connessione. Se possibile, verrà cercato anche il nome host del computer remoto.
- ***Stato***: indica lo stato corrente più probabile (*Connesso, Il server deve essere*

chiuso, Ascolto, Chiusura attiva terminata, Chiusura passiva, Chiusura attiva).

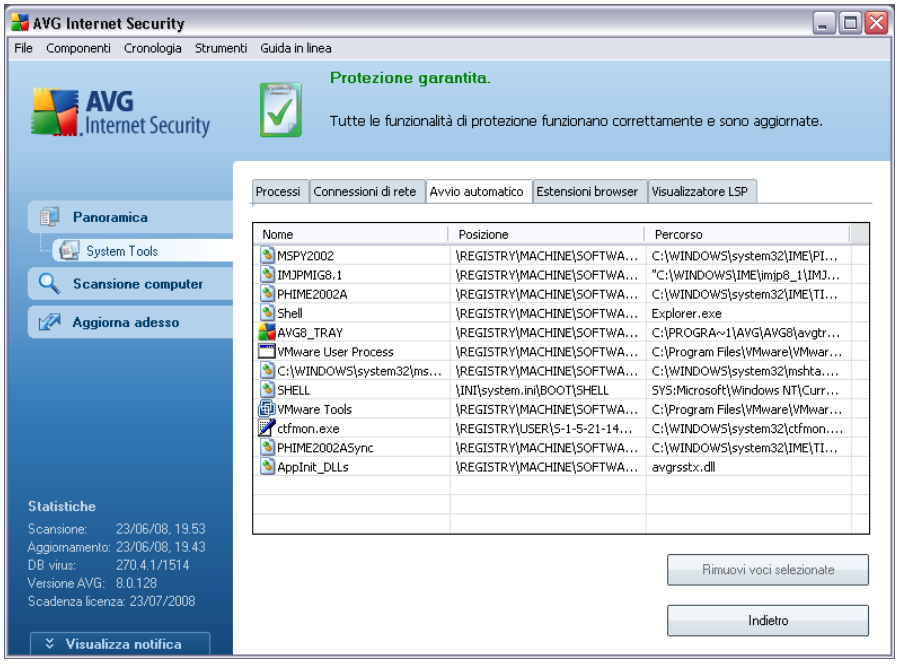
Per elencare solo connessioni esterne è sufficiente selezionare la casella di controllo ***Nascondi connessioni locali***.

Sono disponibili i seguenti pulsanti di controllo:

- ***Termina connessione***: consente di chiudere una o più connessioni selezionate nell'elenco.
- ***Termina processo***: consente di chiudere una o più applicazioni correlate alle connessioni selezionate nell'elenco (*il pulsante è disponibile solo sui sistemi che eseguono Windows XP*)
- ***Indietro***: consente di tornare all'***interfaccia utente di AVG*** predefinita (panoramica dei componenti).

a volte è possibile terminare solo le applicazioni il cui stato corrente è Connesso. Si consiglia di non terminare alcuna connessione, se non si è assolutamente sicuri che rappresenti una reale minaccia!

10.5.3.Avvio automatico

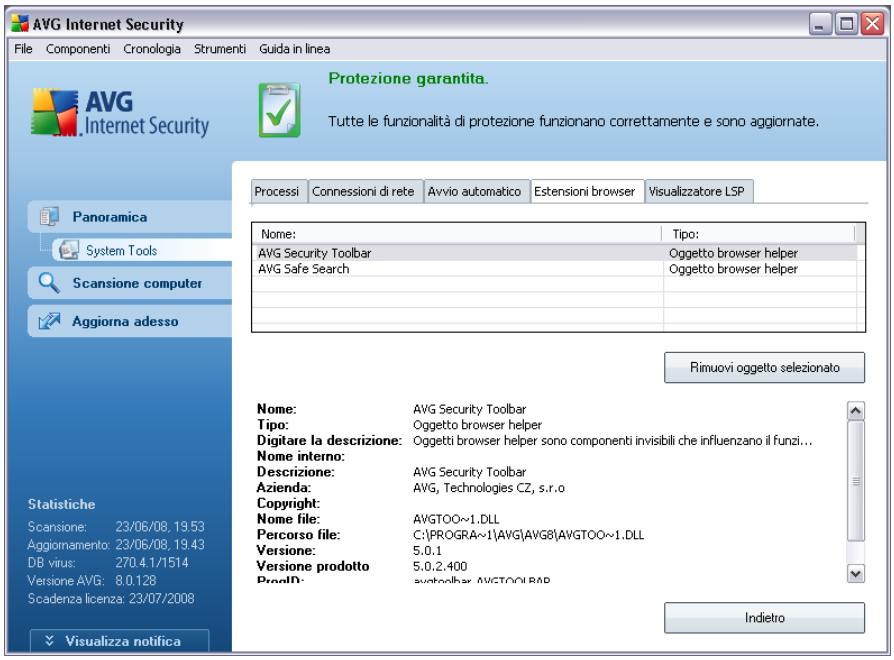


Nella finestra di dialogo ***Avvio automatico*** è visualizzato un elenco di tutte le applicazioni eseguite durante l'avvio del sistema Windows. Molto spesso diverse applicazioni malware si aggiungono automaticamente alle voci del Registro di sistema di avvio.

È possibile eliminare una o più voci selezionandole e facendo clic sul pulsante ***Rimuovi selezione.*** Il pulsante ***Indietro*** consente di tornare all'***interfaccia utente di AVG*** predefinita (panoramica dei componenti).

si consiglia di non eliminare alcuna applicazione dall'elenco, se non si è assolutamente sicuri che rappresenta una reale minaccia!

10.5.4.Estensioni browser



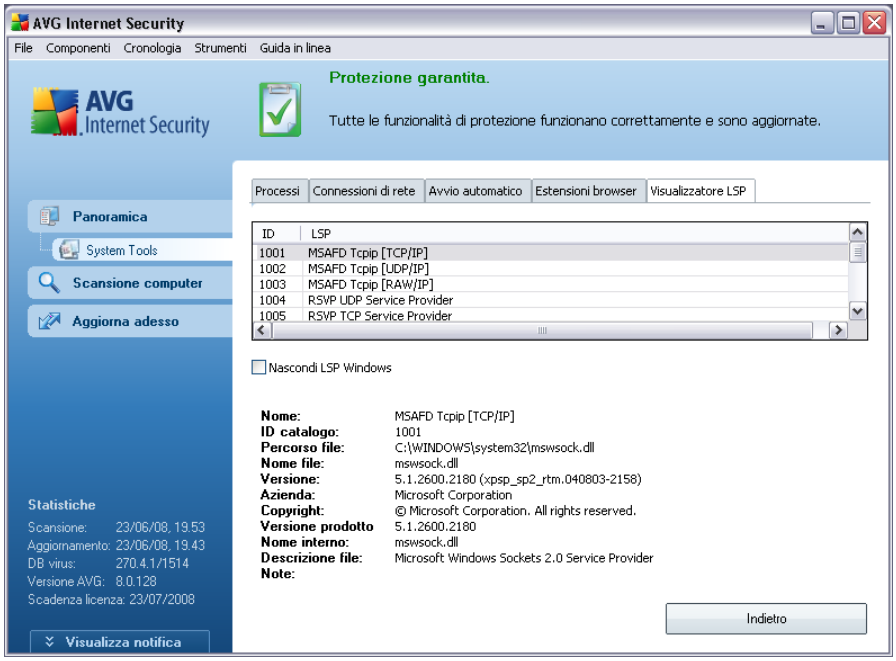
Nella finestra di dialogo ***Estensioni browser*** è presente l'elenco dei plug-in (*ovvero, applicazioni*) installati nel browser Web. L'elenco può includere normali plug-in dell'applicazione ma anche potenziali programmi malware. Fare clic su un oggetto presente nell'elenco per ottenere ulteriori informazioni (*visualizzate nella parte inferiore della finestra di dialogo*).

Se non si è assolutamente sicuri che un plug-in rappresenti una reale minaccia, si consiglia di non eliminarlo dall'elenco.

Il pulsante ***Indietro*** consente di tornare all'***interfaccia utente di AVG*** predefinita

(panoramica dei componenti).

10.5.5.Visualizzatore LSP



Nella finestra di dialogo ***Visualizzatore LSP*** viene visualizzato un elenco di LSP (Layered Service Providers, provider di servizi sottostante).

Un ***LSP*** (Layered Service Provider) è un driver di sistema collegato ai servizi di rete del sistema operativo Windows. È in grado di accedere a tutti i dati in entrata e in uscita dal computer e di modificare tali dati. Alcuni LSP sono necessari per consentire a Windows di connettere il computer dell'utente ad altri computer e a Internet. Tuttavia, alcune applicazioni malware possono anche installarsi come LSP e in tal modo potranno avere accesso a tutti i dati trasmessi dal computer. Pertanto, questa analisi potrà aiutare l'utente a verificare tutte le possibili minacce LSP.

In determinate circostanze è anche possibile correggere LSP danneggiati (*ad esempio quando il file è stato rimosso ma le voci del Registro di sistema sono rimaste intatte*). Quando viene rilevato un LSO riparabile, viene visualizzato un nuovo pulsante per la correzione del problema.

Per includere un LSP Windows nell'elenco, deselezionare la casella di controllo ***Nascondi LSP Windows.*** Il pulsante ***Indietro*** consente di tornare all'***interfaccia utente di AVG*** predefinita (panoramica dei componenti).

10.6.Firewall

10.6.1.Principi del firewall

Il firewall è un sistema che impone un criterio di controllo dell'accesso tra due o più reti, per bloccare o consentire il traffico. Il firewall contiene un insieme di regole che proteggono la rete interna da attacchi esterni (normalmente da Internet) e controlla tutte le comunicazioni su ogni singola porta di rete. La comunicazione viene valutata in base alle regole definite, quindi viene eventualmente consentita o impedita. Se il firewall rileva tentativi di intrusione, li blocca immediatamente e non consente all'intruso di accedere al PC.

Il firewall viene configurato per consentire o negare le comunicazioni interne/esterne (in entrambe le direzioni, entrata o uscita) tramite le porte definite e per le applicazioni software definite. Ad esempio, il firewall potrebbe essere configurato per consentire il solo flusso dei dati Web in entrata e in uscita tramite Microsoft Internet Explorer. Qualsiasi tentativo di trasmettere i dati Web tramite un altro browser viene quindi bloccato.

Il firewall consente di impedire l'invio non autorizzato delle informazioni di identificazione personale contenute nel computer. Controlla il modo in cui il computer scambia dati con altri computer in Internet o nella rete locale. All'interno di un'organizzazione il componente firewall protegge anche i singoli computer da attacchi lanciati da utenti interni ai computer nella rete.

Nota: *il componente AVG Firewall non è destinato alle piattaforme server.*

Funzionamento di AVG Firewall

In AVG il componente ***Firewall*** consente di controllare tutto il traffico su ogni porta di rete del computer. In base alle regole definite, il componente ***Firewall*** valuta le applicazioni in esecuzione sul computer che vogliono eseguire la connessione alla rete locale o a Internet, oppure le applicazioni che dall'esterno tentano di connettersi al PC dell'utente. Per ciascuna di queste applicazioni, il componente ***Firewall*** consente o impedisce la comunicazione sulle porte di rete. Per impostazione predefinita, se l'applicazione è sconosciuta (ovvero non dispone di regole ***Firewall*** definite), il componente ***Firewall*** chiederà se si desidera consentire o bloccare il tentativo di comunicazione.

Funzionalità di Firewall:

- Consente o blocca automaticamente tentativi di comunicazione di applicazioni note o chiede conferma
- Utilizza profili completi con regole predefinite, in base alle esigenze personali
- Mantiene un archivio di tutte le impostazioni e tutti i profili definiti
- Attiva profili automaticamente durante la connessione a varie reti o durante l'utilizzo di diverse schede di rete

10.6.2.Profili Firewall

Il componente ***Firewall*** consente di definire le regole di protezione specifiche a seconda che si tratti di un computer presente in un dominio, di un computer autonomo o perfino di un notebook. Ogni opzione richiede un livello diverso di protezione e i livelli sono coperti dai rispettivi profili. In breve, un profilo di ***Firewall*** è una configurazione specifica del componente ***Firewall*** ed è possibile utilizzare diverse di queste configurazioni predefinite.

Profili disponibili

- ***Permetti Tutto***: è un profilo di sistema del componente ***Firewall*** predefinito dal produttore ed è sempre presente. Se questo profilo è attivato, tutte le comunicazioni di rete sono consentite e non vengono applicate regole dei criteri di protezione, come se la protezione del componente ***Firewall*** fosse disattivata *(ossia tutte le applicazioni vengono contrassegnate come consentite ma i pacchetti continuano a essere controllati; per disattivare completamente i filtri è necessario disattivare il componente Firewall)*. Questo profilo di sistema non può essere duplicato o eliminato e le relative impostazioni non possono essere modificate.
- ***Blocca Tutto***: è un profilo di sistema del componente ***Firewall*** predefinito dal produttore ed è sempre presente. Quando il profilo è attivato, tutte le comunicazioni di rete sono bloccate e non è possibile accedere al computer da reti esterne né comunicare con l'esterno. Questo profilo di sistema non può essere duplicato o eliminato e le relative impostazioni non possono essere modificate.
- ***Profili personalizzati***: profili generati mediante la ***Configurazione guidata del firewall***. Mediante la procedura guidata è possibile generare un massimo di tre profili personalizzati:
    - *Computer autonomo*: adatto a computer desktop per ambienti domestici

direttamente connessi a Internet.

- *Computer in dominio*: adatto ai computer di una rete locale, ad esempio, reti scolastiche o aziendali. Si suppone che la rete sia protetta mediante misure di sicurezza aggiuntive in modo che il livello di protezione possa essere inferiore rispetto a un computer autonomo.

- *Rete domestica o di piccoli uffici*: adatto a computer appartenenti a una piccola rete (ad esempio, in casa o in un piccolo ufficio). Di norma si tratta solo di alcuni computer connessi senza amministratore "centrale".

- *Computer portatile*: adatto a notebook. Si suppone che, come computer portatile, esegua la connessione a Internet da luoghi sconosciuti e pertanto assolutamente non protetti (Internet café, camere di albergo, ecc.) e che sia impostato il livello di protezione più alto.

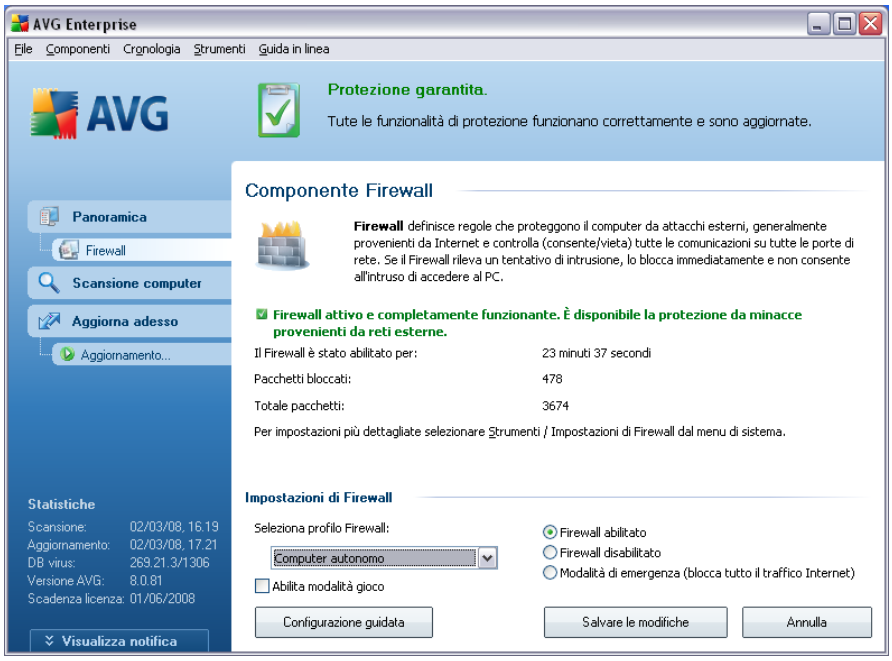
Attivazione profili

La funzionalità di attivazione dei profili consente di attivare automaticamente il componente ***Firewall*** in base al profilo definito quando si utilizza una determinata scheda di rete o quando viene eseguita la connessione a un determinato tipo di rete. Se non sono ancora stati assegnati profili a un'area di rete, alla successiva connessione a quest'area, il componente ***Firewall*** visualizzerà una finestra di dialogo in cui viene richiesta l'assegnazione di un profilo.

È possibile assegnare profili a tutte le aree o interfacce di rete locali e specificare ulteriori impostazioni nella finestra di dialogo ***Profili di aree e schede***, dove è possibile anche disabilitare la funzionalità se non si desidera utilizzarla (*quindi, per qualsiasi tipo di connessione, verrà utilizzato il profilo predefinito*).

Di norma, gli utenti che dispongono di un notebook e utilizzano vari tipi di connessione, riterranno molto utile questa funzionalità. Se si dispone di un computer desktop, e si utilizza sempre un solo tipo di connessione (*ad esempio, connessione via cavo a Internet*), non dovrebbero esserci problemi di attivazione dei profili, in quanto probabilmente non verranno mai utilizzati.

10.6.3.Interfaccia del firewall



L'interfaccia del componente ***Firewall*** offre alcune informazioni di base sulla funzionalità del componente e una breve panoramica delle statistiche di ***Firewall***:

- ***Il firewall è stato abilitato per***: tempo trascorso dall'avvio del firewall
- ***Pacchetti bloccati***: numero di pacchetti bloccati rispetto all'intera quantità di pacchetti controllati
- ***Totale pacchetti***: numero di tutti i pacchetti controllati durante l'esecuzione del firewall

Impostazioni del firewall sezione

- ***Seleziona profilo firewall***: dal menu a discesa scegliere uno dei profili definiti : due profili sono disponibili in ogni momento (i *profili predefiniti denominati* ***Permetti tutto*** *e* ***Blocca tutto***), altri profili sono stati aggiunti durante la ***Configurazione guidata del firewall*** o mediante la modifica dei profili nella finestra di dialogo ***Profili*** in ***Impostazioni del firewall***.
- Stato del firewall:
    - ***Firewall abilitato***: selezionare questa opzione per consentire la

comunicazione a queste applicazioni assegnate come 'consentite' nell'insieme di regole definito all'interno del profilo ***Firewall*** selezionato

- ***Firewall disabilitato*** - questa opzione consente di disattivare completamente il componente ***Firewall***. Tutto il traffico di rete viene consentito ma non controllato.

- ***Modalità di emergenza (blocca tutto il traffico Internet)***: selezionare questa opzione per bloccare tutto il traffico su ogni singola porta di rete; ***Firewall*** è ancora in esecuzione ma tutto il traffico di rete è stato interrotto

- ***Abilita modalità gioco***: selezionare questa opzione per accertarsi che durante l'esecuzione di applicazioni a schermo intero (giochi, presentazioni PowerPoint e così via) il ***Firewall*** non visualizzi finestre di dialogo in cui viene richiesto se si desidera consentire o bloccare la comunicazione per applicazioni sconosciute. Se un'applicazione sconosciuta tenta di comunicare sulla rete in quel momento, il ***Firewall*** autorizza o blocca automaticamente il tentativo in base alle impostazioni presenti nel profilo corrente.

Nota: *il fornitore di software ha impostato tutti i componenti AVG per fornire prestazioni ottimali. A meno che non ci sia una ragione valida, si consiglia di non modificare la configurazione di AVG. Tutte le eventuali modifiche alle impostazioni dovrebbero essere eseguite da un utente esperto. Se è necessario modificare la configurazione di Firewall, selezionare la voce di menu di sistema* ***File / Impostazioni del firewall*** *e modificare la configurazione di Firewall nella finestra di dialogo* ***Impostazioni del firewall*** *visualizzata.*

Pulsanti di controllo disponibili:

- ***Configurazione guidata***: premere il pulsante per avviare la ***Configurazione guidata del firewall*** che consente di eseguire la configurazione del componente ***Firewall***

- ***Salva modifiche***: premere questo pulsante per salvare e applicare le eventuali modifiche eseguite in questa finestra di dialogo

- ***Annulla***: premere questo pulsante per tornare all'impostazione predefinita dell'interfaccia utente di AVG (*panoramica dei componenti*)

10.7.Scansione e-mail

10.7.1.Principi di Scansione e-mail

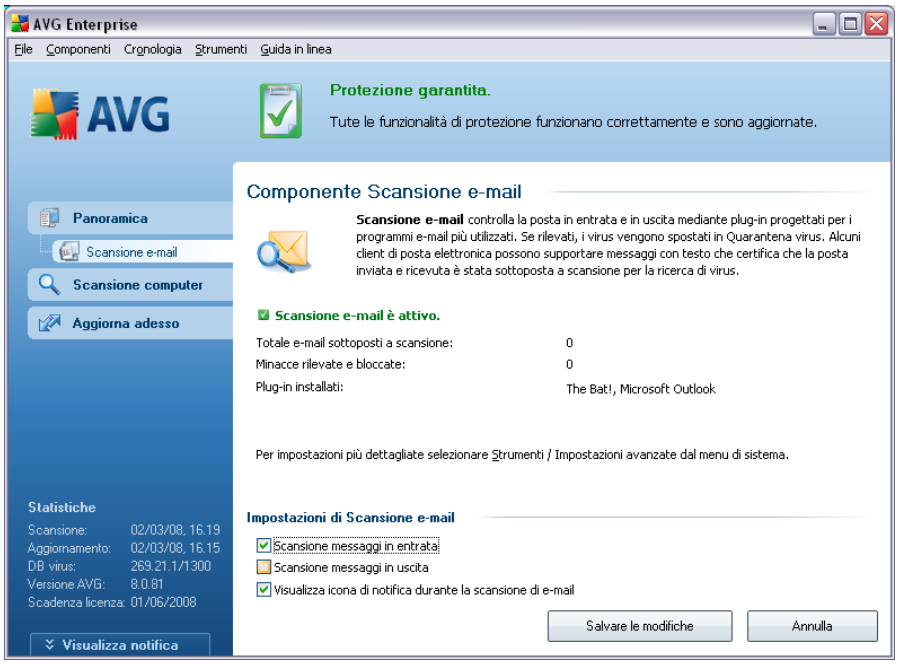
Una delle origini più comuni di virus e trojan è la posta elettronica. Phishing e spam make rendono la posta elettronica una grande fonte di rischio. Gli account di posta elettronica gratuiti sono quelli con più probabilità di ricevere quessto tipo di messaggi dannosi, poiché raramente impiegano una tecnologia antispam, e gli utenti domestici si affidano moltissimo a questo tipo di posta elettronica. Inoltre, gli utenti domestici aumentano l'esposizione ad attacchi tramite posta elettronica poiché navigano spesso in siti sconosciuti e compilano moduli in linea con dati personali, quali il proprio indirizzo di posta elettronica. Di solito le società utilizzano account aziendali, filtri antispam e altri accorgimenti per ridurre il rischio.

Il componente ***Scansione E-mail*** controlla ogni messaggio di posta elettronica inviato o ricevuto e in tal modo fornisce la necessaria protezione dalle minacce che si celano nella posta elettronica. AVG supporta tutti i principali client e-mail, inclusi MS Outlook, The Bat!, Eudora e tutti gli altri client e-mail basati su POP3/SMTP, come Outlook Express. Sono supportate anche le connessioni crittografate con SSL.

Nota: *il componente Scansione E-mail di AVG non è destinato alle piattaforme server.*

Se rilevati, i virus vengono immediatamente inseriti in ***Quarantena virus***. Alcuni client e-mail possono supportare messaggi di testo che certificano che la posta inviata e ricevuta è stata sottoposta a scansione per la ricerca di virus.

10.7.2.Interfaccia di Scansione e-mail



Nella finestra di dialogo del componente ***Scansione E-mail*** è contenuto un breve testo che descrive la funzionalità del componente e fornisce le informazioni sul relativo stato corrente (*Scansione E-mail è attivo.*) e le seguenti statistiche:

- ***Totale e-mail sottoposte a scansione***: indica il numero dei messaggi e-mail sottoposti a scansione dall'ultimo avvio di ***Scansione E-mail*** (*se necessario, questo valore può essere reimpostato, ad esempio per scopi statistici - Ripristina valore*)
- ***Minacce rilevate e bloccate***: indica il numero di infezioni trovate nei messaggi e-mail dall'ultimo avvio di ***Scansione E-mail***
- ***Protezione e-mail installata***: informazioni su uno specifico plug-in per la protezione dell'e-mail relativo al client e-mail predefinito installato

Configurazione di base del componente

Nella parte inferiore della finestra di dialogo è contenuta una sezione denominata ***impostazioni di scansione e-mail*** che consente di modificare alcune funzionalità di base del funzionamento del componente:

- ***Scansione messaggi in entrata***: selezionare l'elemento per specificare che tutti i messaggi e-mail recapitati all'account devono essere sottoposti a scansione per il rilevamento di virus (*per impostazione predefinita, questa opzione è attiva e si consiglia di non modificarne l'impostazione.*)
- ***Scansione messaggi in uscita***: selezionare la voce per confermare che tutte le e-mail inviate dall'account devono essere sottoposte a scansione per il rilevamento di virus (*per impostazione predefinita, questa voce è disattivata*)
- ***Visualizza icona di notifica durante la scansione di e-mail***: durante la scansione, il componente ***Scansione E-mail*** visualizza una finestra di dialogo di notifica per informare l'utente sull'attività attualmente elaborata dal componente (*connessione al server, download di un messaggio, scansione del messaggio e così via*).

la configurazione avanzata del componente ***Scansione E-mail*** è accessibile da ***File/ Impostazioni avanzate*** del menu di sistema; tuttavia, si consiglia la configurazione avanzata solo a utenti esperti.

Nota: *il fornitore di software ha impostato tutti i componenti AVG per fornire prestazioni ottimali. A meno che non ci sia una ragione valida, si consiglia di non*

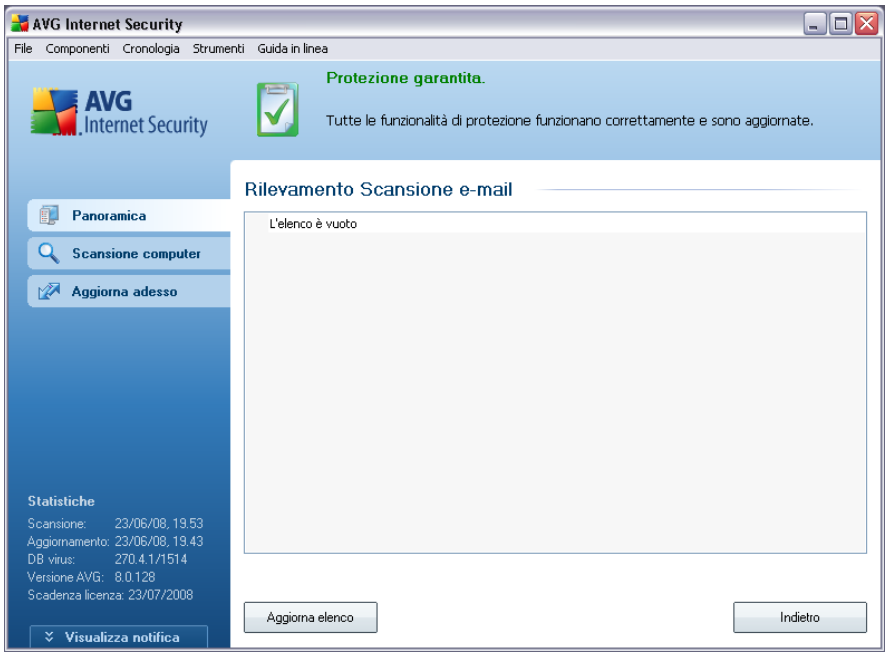
modificare la configurazione di AVG. Tutte le eventuali modifiche alle impostazioni dovrebbero essere eseguite da un utente esperto. Se è necessario modificare la configurazione di AVG, selezionare la voce di menu di sistema ***Strumenti / Impostazioni avanzate*** *e modificare la configurazione di AVG nella finestra di dialogo Impostazioni AVG avanzate visualizzata.*

Pulsanti di controllo

I pulsanti di controllo disponibili nell'interfaccia ***Scansione E-mail*** sono i seguenti:

- ***Salva modifiche***: premere questo pulsante per salvare e applicare le eventuali modifiche eseguite in questa finestra di dialogo
- ***Annulla***: premere questo pulsante per tornare all'impostazione predefinita dell'interfaccia utente di AVG (panoramica dei componenti)

10.7.3.Rilevamento scansione e-mail



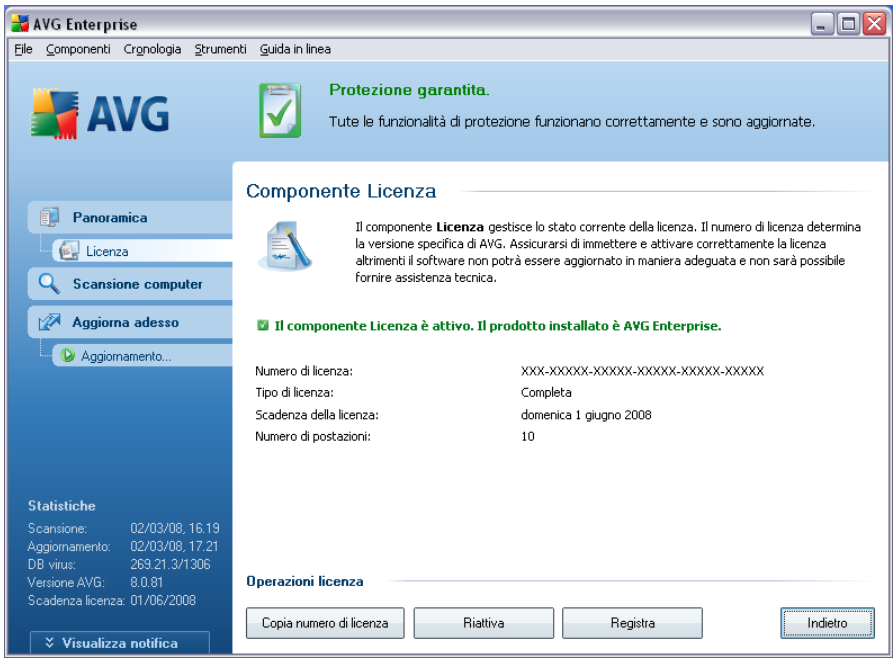
Nella finestra di dialogo ***Rilevamento scansione e-mail*** (*accessibile tramite l'opzione del menu di sistema Cronologia/Rilevamento scansione e-mail*) sarà possibile visualizzare un elenco di tutti i rilevamenti effettuati dal componente ***Scansione E-mail*** . Per ogni oggetto rilevato vengono fornite le seguenti

informazioni:

- ***Infezione***: descrizione (possibilmente anche il nome) dell'oggetto rilevato.
- ***Oggetto***: posizione dell'oggetto.
- ***Risultato***: azione eseguita sull'oggetto rilevato.
- ***Tipo di oggetto***: tipo di oggetto rilevato.

Nella parte inferiore della finestra di dialogo, sotto l'elenco, sono disponibili informazioni sul numero totale degli oggetti rilevati elencati in alto. È inoltre possibile esportare l'intero elenco di oggetti rilevati in un file (***Esporta elenco in file***) ed eliminare tutte le voci relative agli oggetti rilevati (***Svuota elenco***).

10.8.Licenza



Nell'interfaccia del componente ***Licenza*** sono contenute una breve descrizione della funzionalità del componente, le informazioni sul relativo stato (*il componente Licenza*

è attivo.) e le seguenti informazioni:

- ***Numero di licenza***: fornisce il formato esatto del numero di licenza. Quando si immette il numero di licenza, è necessario essere precisi digitandolo esattamente come viene indicato. Per facilitare questa operazione, sulla finestra di dialogo ***Licenza*** è presente il pulsante ***Copia numero licenza***: premere il pulsante per copiare il numero di licenza negli appunti, quindi incollarlo dove si preferisce (***CTRL+V***).

- ***Tipo di licenza***: specifica l'edizione del prodotto definita dal numero di licenza.

- ***Scadenza licenza***: questa data determina il periodo di validità della licenza. Se si desidera continuare a utilizzare AVG dopo questa data, sarà necessario rinnovare la licenza. Il rinnovo della licenza può essere effettuato in linea dal sito Web di AVG.

- ***Numero di postazioni*** : indica il numero di workstation nelle quali è possibile installare AVG.

Pulsanti di controllo

- ***Copia numero di licenza***: premere il pulsante per immettere il numero di licenza in uso negli Appunti (*come con CTRL+C*) e incollare dove necessario

- ***Riattiva***: consente di aprire la finestra di dialogo ***Attiva AVG*** con i dati immessi nella finestra di dialogo ***Personalizza AVG*** del processo di installazione. In questa finestra di dialogo è possibile immettere il numero di licenza per sostituire il numero di vendita (*il numero con cui è stata eseguita l'installazione di AVG*) o il numero di licenza in uso (*ad esempio, durante l'aggiornamento a un nuovo prodotto AVG*).

- ***Registra***: consente di connettersi al sito Web di registrazione all'indirizzo www.avg.com. Immettere i dati di registrazione; solo i clienti che registrano il proprio prodotto AVG possono ricevere assistenza tecnica gratuita.

- ***Indietro***: premere questo pulsante per tornare all'interfaccia utente di AVG predefinita (panoramica dei componenti)

10.9.Link Scanner

10.9.1.Principi Link Scanner

LinkScanner funziona con Internet Explorer e Firefox (*versioni 1.5 e successive*) e include due funzionalità: ***AVG Active Surf-Shield*** e ***AVG Search Shield***.

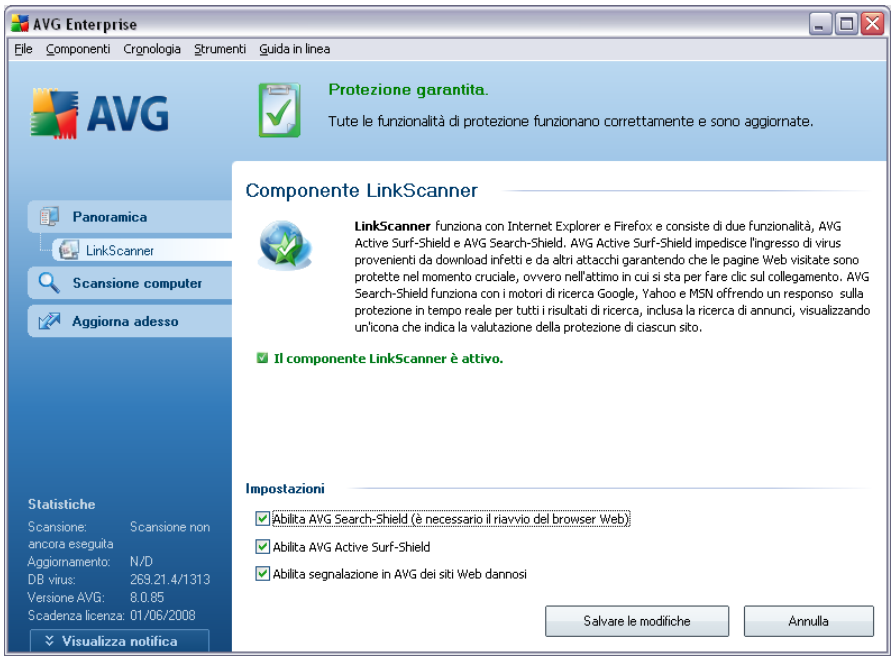
AVG Active Surf-Shield impedisce l'ingresso di virus provenienti da download infetti e da altri attacchi garantendo che le pagine Web visitate sono protette nel momento cruciale, ovvero nell'attimo in cui si sta per fare clic sul collegamento.

AVG Search Shield funziona con i motori di ricerca Google, Yahoo! e MSN offrendo un responso sulla protezione in tempo reale per tutti i risultati di ricerca, inclusa la ricerca di annunci, visualizzando un'icona che indica il grado di protezione di ciascun sito.

Nota: *il componente AVG Link Scanner non è destinato alle piattaforme server.*

10.9.2.Interfaccia Link Scanner

Il componente ***LinkScanner*** include due parti che è possibile attivare e disattivare nell'interfaccia del ***componente LinkScanner***:



- ***Abilita AVG Search-Shield***: (*attivata per impostazione predefinita*) icone informative relative ai siti restituiti da ricerche eseguite in Google, Yahoo o MSN il cui contenuto è stato precedentemente controllato. I browser

supportati sono Internet Explorer e Firefox.

- ***Abilita AVG Active Surf-Shield***: *(attivata per impostazione predefinita)* protezione attiva (*in tempo reale*) da siti dannosi al momento dell'accesso. Le connessioni a siti dannosi conosciuti e il loro contenuto vengono bloccati non appena l'utente esegue l'accesso mediante un browser Web (*o qualsiasi altra applicazione che utilizza HTTP*).

- ***Segnalazione siti Web dannosi*** : contrassegnare questa voce per consentire la segnalazione di exploit e di siti dannosi trovati dall'utente mediante ***Safe Surf*** o ***Safe Search*** per consentire la raccolta di informazioni sul database in merito ad attività dannose sul Web.

10.9.3.AVG Search-Shield

Quando si eseguono ricerche in Internet con ***AVG Search-Shield*** attivato, tutti i risultati di ricerca restituiti dai motori di ricerca più comuni quali Yahoo!, Google, MSN e così via vengono valutati per rilevare collegamenti pericolosi o sospetti. Con il controllo dei collegamenti e l'assegnazione di un contrassegno ai collegamenti dannosi, ***AVG Security Toolbar*** avvisa l'utente prima che faccia clic su collegamenti pericolosi o sospetti così da garantire l'accesso solo ai siti Web sicuri.

Durante la valutazione di un collegamento nella pagina dei risultati della ricerca, verrà visualizzato un simbolo grafico vicino al collegamento per informare che la verifica è in corso. Una volta terminata la valutazione, verrà visualizzata la rispettiva icona informativa:

La pagina collegata è sicura (*con il motore di ricerca Yahoo! in AVG Security Toolbar, non verrà visualizzata questa icona rotante*).

La pagina alla quale fa riferimento il collegamento non contiene minacce ma risulta sospetta (*origine o motivazione dubbia, pertanto non è consigliabile utilizzarla per l'e-shopping e così via*).

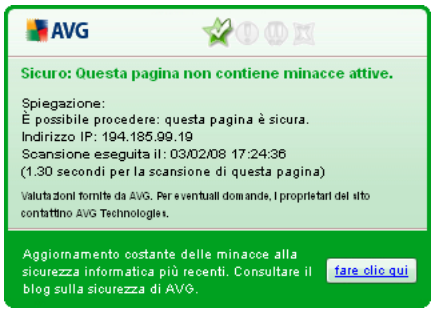
La pagina stessa alla quale fa riferimento il collegamento potrebbe essere sicura, ma contenente a sua volta dei collegamenti a pagine decisamente pericolose oppure la pagina potrebbe contenere del codice sospetto, anche se al momento non presenta minacce dirette.

La pagina collegata contiene minacce attive. Per motivi di protezione, non sarà consentito visitare questa pagina.

La pagina collegata non è accessibile, pertanto non è stato possibile

eseguirne la scansione.

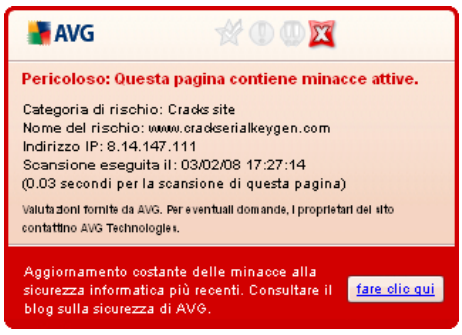
Se si passa il mouse sopra una singola icona che indica la valutazione verranno visualizzati i dettagli relativi al collegamento specifico. Nelle informazioni sono inclusi gli eventuali dettagli aggiuntivi relativi alla minaccia, l'indirizzo IP del collegamento e il momento in cui è stata eseguita la scansione da AVG:



10.9.4.AVG Active Surf-Shield

Si tratta di un potente strumento di protezione che blocca il contenuto pericoloso delle pagine Web quando si tenta di aprirle, impedendone il download sul computer. Se questa funzionalità è abilitata, quando si fa clic sul collegamento o si digita l'URL di un sito pericoloso, l'apertura della pagina Web verrà bloccata immediatamente impedendo che il PC dell'utente venga infettato. È importante tenere presente che le pagine Web dannose possono infettare il computer con il semplice accesso al sito infetto. È per questo che quando si richiedono pagine Web contenenti exploit o altre minacce serie, ***AVG Security Toolbar*** non ne consentirà la visualizzazione.

Se si trovano siti Web dannosi, all'interno del browser, ***AVG Security Toolbar*** visualizzerà un avviso simile a quello seguente:



se si desidera comunque accedere alla pagina infetta, è disponibile sulla schermata un collegamento alla pagina. ***Tuttavia, non è consigliabile procedere con pagine***

simili.

10.1(Web Shield

10.10.1Principi di Web Shield

Web Shield è un tipo di protezione permanente in tempo reale; esegue la scansione del contenuto delle pagine Web visitate (e dei possibili file in esse contenuti) persino prima che vengano visualizzate nel browser Web o scaricate nel computer.

Web Shield rileva che la pagina che sta per essere aperta contiene alcuni javascript dannosi e impedisce così la visualizzazione della pagina. Inoltre, riconosce il malware contenuto in una pagina arrestandone immediatamente il download per impedirne il trasferimento nel computer.

Nota: *il componente AVG Web Shield non è destinato alle piattaforme server.*

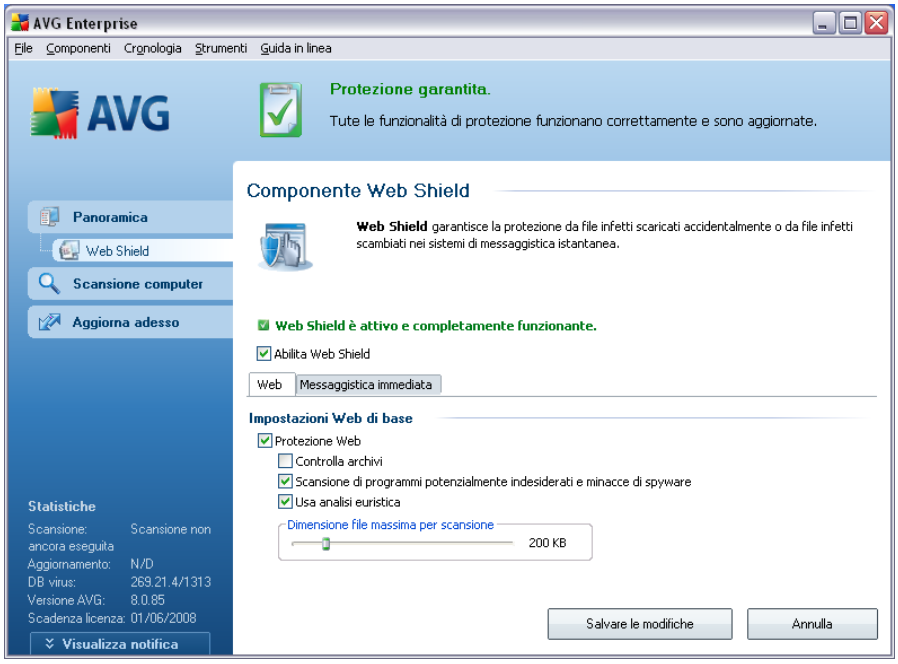
10.10.2Interfaccia di Web Shield

L'interfaccia del componente ***Web Shield*** descrive questo tipo di protezione. Inoltre, è possibile trovare informazioni sullo stato corrente del componente (*Web Shield è attivo e completamente funzionante.*). Nella parte inferiore della finestra di dialogo sono presenti le opzioni di modifica di base del componente.

Configurazione di base del componente

Innanzitutto, è disponibile l'opzione per attivare/disattivare immediatamente ***Web Shield*** selezionando la voce ***Abilita Web Shield***. Questa opzione è abilitata per impostazione predefinita e il componente ***Web Shield*** è attivo. Tuttavia, se non esiste una motivazione valida per modificare queste impostazioni, è consigliabile mantenere attivo il componente. Se la voce è selezionata e ***Web Shield*** è in esecuzione, più opzioni di configurazione saranno disponibili e modificabili su due schede:

- ***Web***: è possibile modificare la configurazione del componente relativa alla scansione del contenuto del sito Web. L'interfaccia di modifica consente di configurare le seguenti opzioni di base:

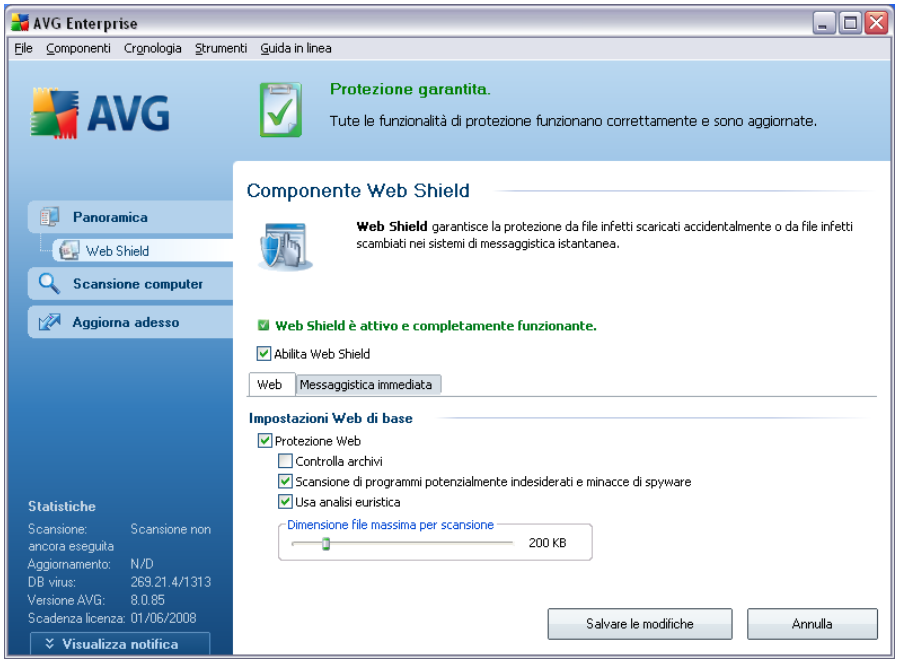


o ***Protezione Web***: questa opzione conferma l'esecuzione della scansione del contenuto delle pagine Web da parte del componente ***Web Shield***. Se questa opzione è attiva (*per impostazione predefinita*), è possibile attivare/disattivare le voci seguenti:

- ***Controlla archivi***: consente di eseguire la scansione del contenuto di possibili archivi inclusi nella pagina Web da visualizzare
- ***Scansione di programmi potenzialmente indesiderati***: consente di eseguire la scansione di programmi potenzialmente indesiderati (*programmi eseguibili che possono funzionare come spyware o adware*) inclusi nella pagina Web da visualizzare
- ***Usa analisi euristica***: consente di eseguire la scansione del contenuto della pagina da visualizzare utilizzando il metodo analisi euristica *(emulazione dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale. Vedere il capitolo Principi Antivirus*)
- ***Dimensione file massima per scansione***: se i file inclusi sono presenti nella pagina visualizzata, è anche possibile eseguire la scansione del contenuto relativo prima che vengano scaricati nel computer. Tuttavia, la scansione di file di grandi dimensioni richiede

parecchio tempo rallentando notevolmente il download della pagina Web. È possibile utilizzare la barra di scorrimento per specificare la dimensione massima di un file che deve ancora essere sottoposto a scansione con ***Web Shield***. Anche se le dimensioni del file scaricato sono superiori a quelle specificate e il file non verrà sottoposto a scansione da ***Web Shield***, il computer è comunque protetto: se il file fosse infetto, verrebbe immediatamente rilevato da ***Resident Shield*** .

- ***Messaggistica immediata***: consente di modificare le impostazioni dei componenti relativi alla scansione della messaggistica immediata (*ad esempio ICQ, MSN Messenger, Yahoo e così via*).



-

  - Protezione Messaggistica immediata: selezionare questa voce se si desidera che Web Shield verifichi che la comunicazione in linea non includa virus. Se questa opzione è attivata, è possibile specificare inoltre l'applicazione di messaggistica immediata da controllare. Attualmente **AVG 8.5 Internet Security** supporta le applicazioni ICQ, MSN e Yahoo.

Nota: il *fornitore di software ha impostato tutti i componenti AVG per fornire prestazioni ottimali. A meno che non ci sia una ragione valida, si consiglia di non modificare la configurazione di AVG. Tutte le eventuali modifiche alle impostazioni dovrebbero essere eseguite da un utente esperto. Se è necessario modificare la*

*configurazione di AVG, selezionare la voce di menu di sistema **Strumenti / Impostazioni avanzate** e modificare la configurazione di AVG nella finestra di dialogo Impostazioni AVG avanzate visualizzata.*

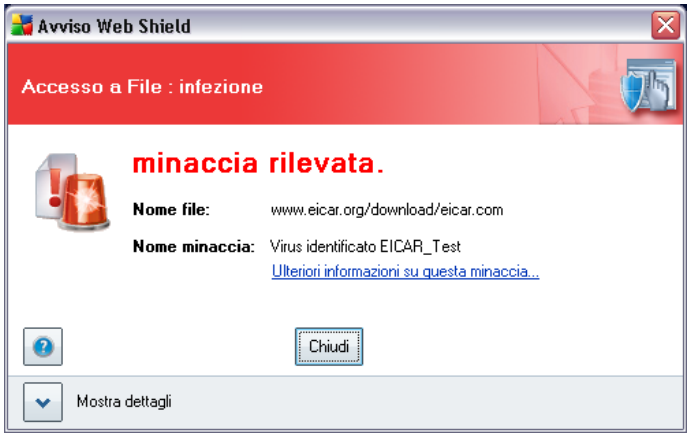
Pulsanti di controllo

I pulsanti di controllo disponibili nell'interfaccia di ***Web Shield*** sono i seguenti:

- ***Salva modifiche***: premere questo pulsante per salvare e applicare le eventuali modifiche eseguite in questa finestra di dialogo
- ***Annulla***: premere questo pulsante per tornare all'impostazione predefinita dell'interfaccia utente di AVG (*panoramica dei componenti*)

10.10. Rilevamento Web Shield

Web Shield esegue la scansione del contenuto delle pagine Web visitate e dei possibili file in esse contenuti prima che queste vengano visualizzate nel browser Web o scaricate nel computer. Se viene rilevata una minaccia, l'utente verrà avvisato immediatamente tramite la seguente finestra di dialogo:



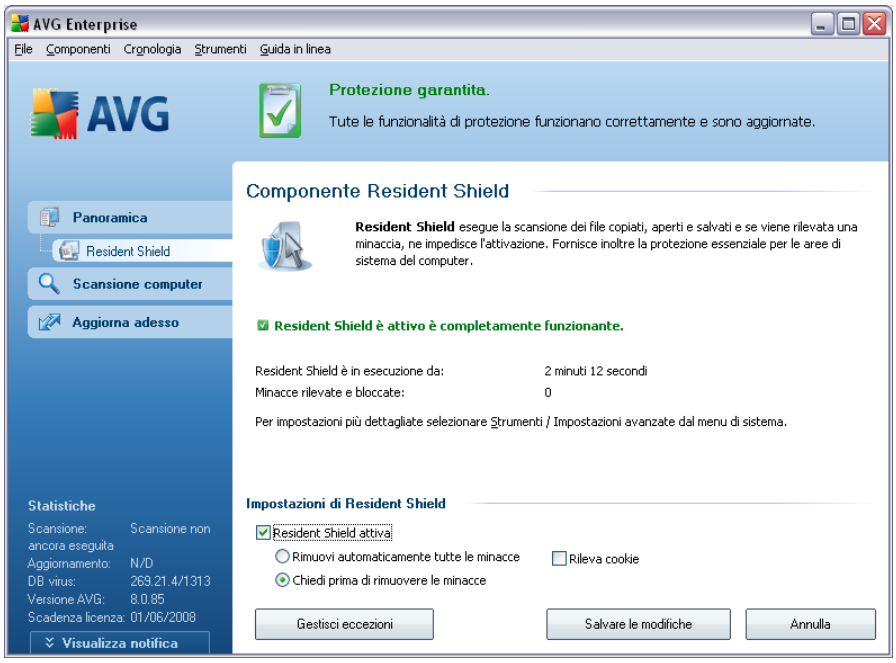
La pagina Web sospetta non verrà aperta e il rilevamento della minaccia verrà registrato nell'elenco ***Rilevamenti di Web Shield*** (*accessibile tramite il menu di sistema Cronologia / Rilevamenti di Web Shield*).

10.11. Resident Shield

10.11.1. Resident Shield Principi

Resident Shield esegue la scansione dei file mentre vengono copiati, aperti o salvati. Quando ***Resident Shield*** rileva un virus durante l'accesso a un file, arresta l'operazione in corso impedendo l'attivazione del virus. Il componente ***Resident Shield***, caricato nella memoria del computer durante l'avvio del sistema, fornisce inoltre un livello di protezione fondamentale per le aree di sistema del computer.

10.11.2. Interfaccia Resident Shield



Oltre a una panoramica dei principali dati statistici e delle principali informazioni sullo stato corrente del componente (*Resident Shield è attivo e completamente funzionante*), l'interfaccia di ***Resident Shield*** offre anche alcune opzioni di impostazione di base del componente. Le statistiche sono le seguenti:

- ***Resident Shield è stato attivo per***: fornisce il tempo trascorso dall'ultimo avvio del componente
- ***Minacce rilevate e bloccate***: numero di infezioni rilevate di cui è stata impedita l'esecuzione/l'apertura (*se necessario, questo valore può essere*

reimpostato, ad esempio per scopi statistici - Ripristina valore)

Configurazione di base del componente

Nella parte inferiore della finestra di dialogo è presente la sezione ***Impostazioni Resident Shield*** dove è possibile modificare alcune impostazioni di base del funzionamento del componente (*la configurazione dettagliata, come per tutti gli altri componenti, è disponibile dall'impostazione File/Impostazioni avanzate del menu di sistema*).

L'opzione ***Resident Shield è attivo*** consente di attivare/disattivare facilmente la protezione permanente. Per impostazione predefinita, la funzione è attivata. Mediante la protezione permanente è possibile decidere come trattare (rimuovere) le eventuali infezioni rilevate:

- automaticamente (***Rimuovi automaticamente tutte le minacce***)
- o solo dopo l'approvazione dell'utente (***Chiedi prima di rimuovere le minacce***)

La scelta non avrà alcun effetto sul livello di protezione, in quanto riflette esclusivamente le preferenze dell'utente.

In entrambi i casi, è ancora possibile selezionare se utilizzare l'opzione ***Rimuovi cookie automaticamente.*** In casi specifici è possibile attivare questa opzione per ottenere i livelli di massima protezione; tuttavia per impostazione predefinita l'opzione è disattivata. (*cookie = pacchetti di testo inviati da un server a un browser Web e reinviati intatti dal browser ogni volta che esegue l'accesso al server. I cookie HTTP sono utilizzati per autenticare, rilevare e mantenere informazioni specifiche sugli utenti, quali le preferenze dei siti e il contenuto dei carrelli elettronici*).

Nota: il *fornitore di software ha impostato tutti i componenti AVG per fornire prestazioni ottimali. A meno che non ci sia una ragione valida, si consiglia di non modificare la configurazione di AVG. Tutte le eventuali modifiche alle impostazioni dovrebbero essere eseguite da un utente esperto. Se è necessario modificare la configurazione di AVG, selezionare la voce di menu di sistema* ***Strumenti / Impostazioni avanzate*** *e modificare la configurazione di AVG nella finestra di dialogo Impostazioni AVG avanzate visualizzata.*

Pulsanti di controllo

I pulsanti di controllo disponibili nell'interfaccia ***Resident Shield*** sono i seguenti:

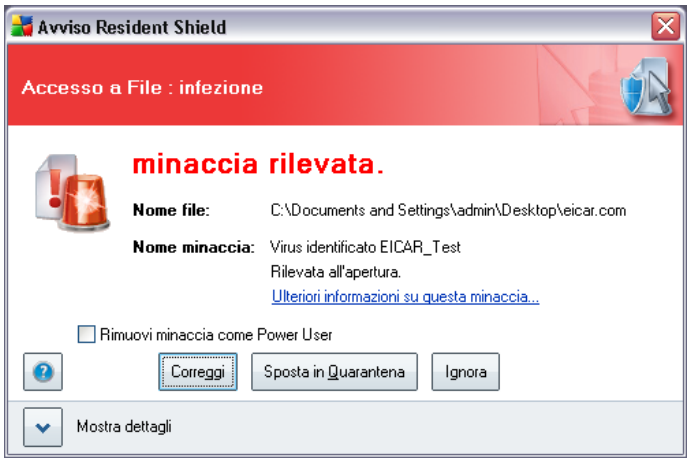
- ***Gestisci eccezioni*** - consente di aprire la finestra di dialogo ***Esclusioni da Resident Shield*** in cui è possibile definire le cartelle da escludere dalla scansione di ***Resident Shield***

- ***Salva modifiche***: premere questo pulsante per salvare e applicare le eventuali modifiche eseguite in questa finestra di dialogo

- ***Annulla***: premere questo pulsante per tornare all'impostazione predefinita dell'***interfaccia utente di AVG*** (panoramica dei componenti)

10.11.3Rilevamento Resident Shield

Resident Shield esegue la scansione dei file mentre vengono copiati, aperti o salvati. Quando viene rilevato un virus o altra minaccia, l'utente viene avvisato immediatamente tramite la successiva finestra di dialogo:

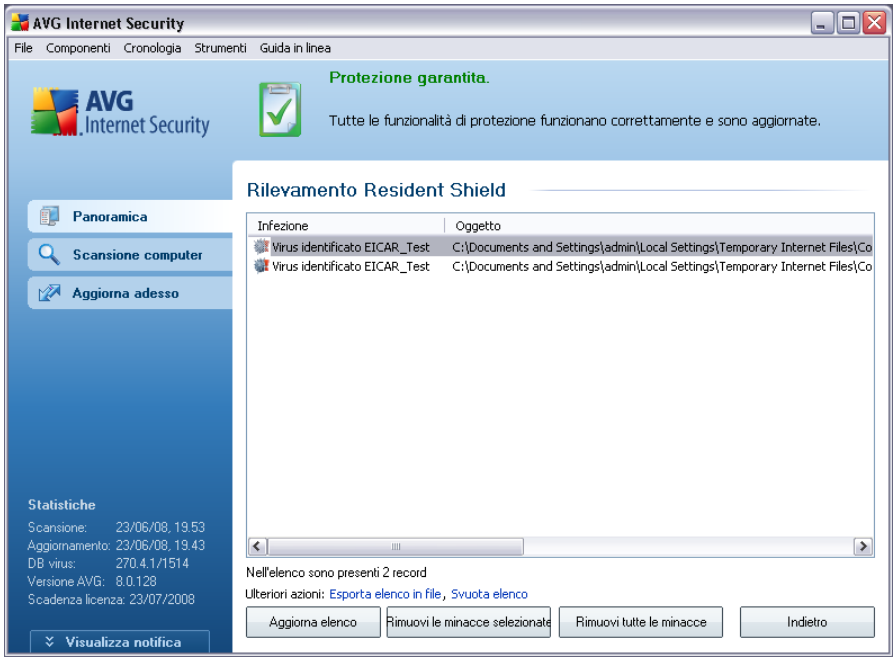


La finestra di dialogo fornisce informazioni sulla minaccia rilevata e richiede all'utente di decidere quale azione dovrà essere intrapresa:

- ***Correggi***: se è disponibile un rimedio, AVG correggerà il file infetto automaticamente; questa opzione rappresenta l'azione consigliata da intraprendere

- ***Sposta in Quarantena***: il virus verrà spostato in ***Quarantena virus AVG***

- ***Ignora***: si consiglia di NON utilizzare questa opzione a meno che non sussista un motivo valido per farlo



In ***Rilevamento Resident Shield*** è disponibile una panoramica di oggetti rilevati da ***Resident Shield***, classificati come pericolosi e corretti o spostati in ***Quarantena virus***. Per ogni oggetto rilevato vengono fornite le seguenti informazioni:

- ***Infezione***: descrizione (possibilmente anche il nome) dell'oggetto rilevato
- ***Oggetto***: posizione dell'oggetto.
- ***Risultato***: azione eseguita sull'oggetto rilevato.
- ***Tipo di oggetto***: tipo di oggetto rilevato
- ***Processo***: operazione eseguita per richiamare e rilevare l'oggetto potenzialmente pericoloso

Nella parte inferiore della finestra di dialogo, sotto l'elenco, sono disponibili informazioni sul numero totale degli oggetti rilevati elencati in alto. È inoltre possibile esportare l'intero elenco di oggetti rilevati in un file (***Esporta elenco in file***) ed eliminare tutte le voci relative agli oggetti rilevati (***Svuota elenco***). Il pulsante ***Aggiorna elenco*** aggiorna l'elenco dei rilevamenti effettuati da ***Resident Shield***. Il pulsante ***Indietro*** consente di tornare all'***interfaccia utente di AVG*** predefinita (panoramica dei componenti).

10.12. Aggiornamenti

10.12.1. Principi di Aggiornamenti

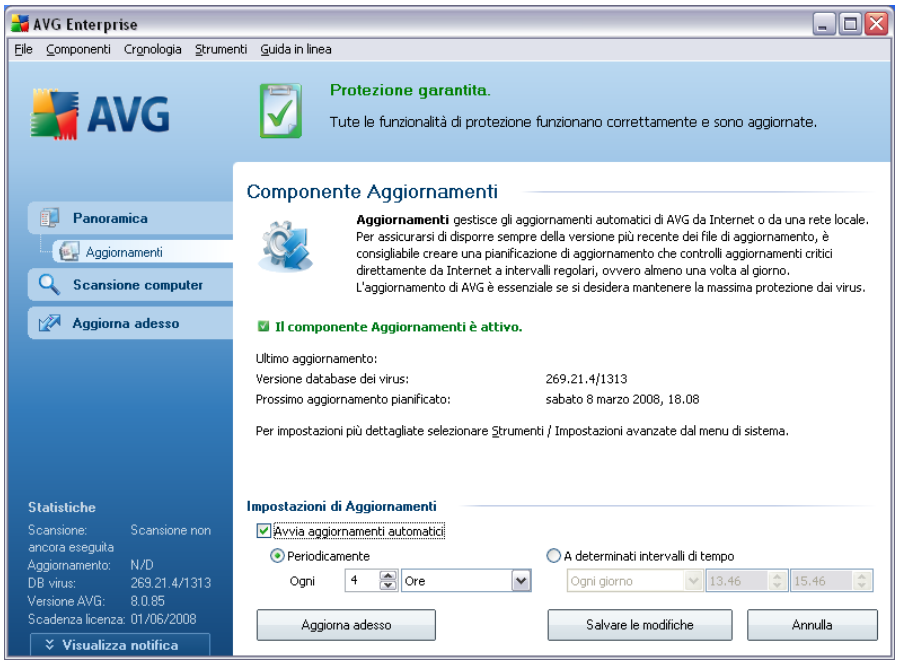
Nessun software per la protezione è in grado di garantire una vera e propria protezione da vari tipi di minacce se non viene aggiornato con regolarità. Gli autori di virus vanno sempre alla ricerca di nuove imperfezioni che possano sfruttare sia nei sistemi operativi che nel software. Tutti i giorni si presentano nuovi virus, nuovo malware e nuovi attacchi di hacker. Per questa ragione, i fornitori di software rilasciano continuamente aggiornamenti e patch di protezione per correggere eventuali difetti di protezione che vengono rilevati.

È fondamentale aggiornare AVG con regolarità.

Gestore aggiornamenti consente di controllare gli aggiornamenti con regolarità. All'interno di questo componente è possibile pianificare download automatici dei file di aggiornamento da Internet o dalla rete locale. La definizione dei virus principali dovrebbe essere eseguita ogni giorno, se possibile. Gli aggiornamenti di programmi meno urgenti, invece, dovrebbero essere eseguiti settimanalmente.

Nota: *per ulteriori informazioni sui livelli e sui tipi di aggiornamenti, leggere attentamente il capitolo Aggiornamenti di AVG.*

10.12. Interfaccia di Aggiornamenti



Nell'interfaccia di ***Gestore aggiornamenti*** vengono visualizzate le informazioni sulla funzionalità del componente e sul relativo stato corrente (*Gestore aggiornamenti è attivo.*) oltre ai dati statistici pertinenti:

- ***Ultimo aggiornamento***: specifica quando e a che ora è stato eseguito l'aggiornamento del database
- ***Versione database dei virus***: indica il numero della versione più recente del database di virus. Il numero aumenta dopo ogni aggiornamento di base dei virus

Configurazione di base del componente

Nella parte inferiore della finestra di dialogo è contenuta una sezione denominata ***impostazioni Gestore aggiornamenti*** che consente di apportare modifiche alle regole dell'avvio del processo di aggiornamento. È possibile definire se si desidera scaricare i file di aggiornamento automaticamente (***Avvia aggiornamenti automatici***) o su richiesta. Per impostazione predefinita, l'opzione ***Avvia aggiornamenti automatici*** è attivata e si consiglia di non modifcarla. Il download regolare dei file di aggiornamento più recenti è fondamentale per il corretto

funzionamento di tutti i software per la protezione.

Inoltre, è possibile definire la frequenza di avvio dell'aggiornamento:

- ***Periodicamente***: definisce l'intervallo di tempo
- ***In un momento specifico***: definisce l'ora e la data esatte

Per impostazione predefinita, l'aggiornamento è impostato per essere eseguito ogni 4 ore. Si consiglia di mantenere questa impostazione a meno che siano presenti ragioni valide per modificarla.

Nota: il fornitore di software di *ha impostato tutti i componenti AVG per fornire prestazioni ottimali. A meno che non ci sia una ragione valida, si consiglia di non modificare la configurazione di AVG. Tutte le eventuali modifiche alle impostazioni dovrebbero essere eseguite da un utente esperto. Se è necessario modificare la configurazione di AVG, selezionare la voce di menu di sistema* ***Strumenti / Impostazioni avanzate*** *e modificare la configurazione di AVG nella finestra di dialogo Impostazioni AVG avanzate visualizzata.*

Pulsanti di controllo

pulsanti di controllo disponibili nell'interfaccia ***Gestore aggiornamenti*** sono i seguenti:

- ***Aggiorna subito***: consente di avviare un aggiornamento immediato su richiesta
- ***Salva modifiche***: premere questo pulsante per salvare e applicare le eventuali modifiche eseguite in questa finestra di dialogo
- ***Annulla***: premere il pulsante per tornare all'***interfaccia utente AVG*** predefinita (panoramica dei componenti)

10.13. AVG Security Toolbar

AVG Security Toolbar è progettata per funzionare con ***MS Internet Explorer*** (*versione 6.0 o superiore*) e ***Mozilla Firefox*** (*versione 1.5 o superiore*).

Nota: *il componente AVG Security Toolbar non è destinato alle piattaforme server.*

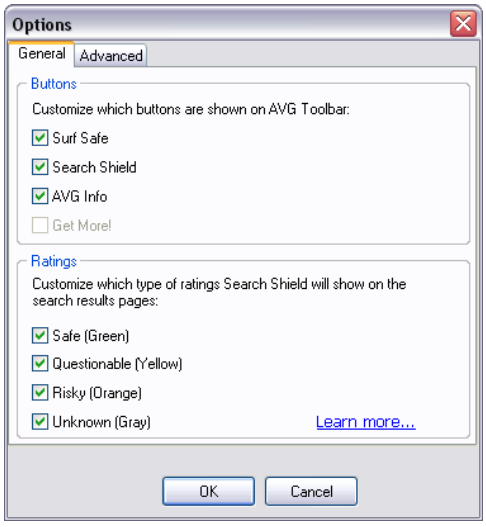
Una volta installata, per impostazione predefinita, ***AVG Security Toolbar*** verrà posizionata sotto la barra degli indirizzi dei browser:

AVG Security Toolbar è composta di quanto segue:

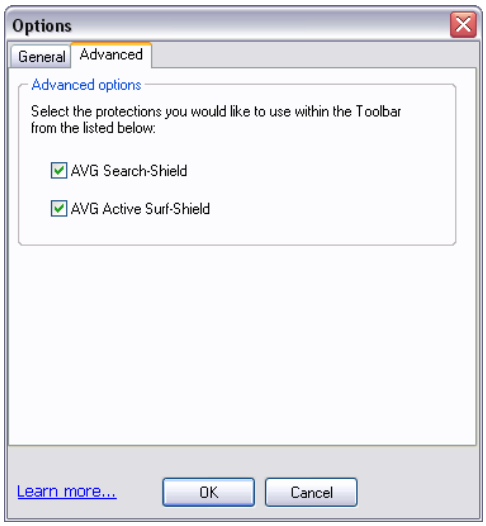
- ***Pulsante logo AVG***: consente di accedere alle voci generali della barra degli strumenti. Fare clic sul pulsante del logo per essere reindirizzati al sito Web di AVG (www.avg.com). Se si fa clic sul puntatore accanto all'icona AVG, verrà visualizzato quanto segue:
    - ***Informazioni barra degli strumenti***: consente di accedere alla pagina principale di ***AVG Security Toolbar*** con informazioni dettagliate sulla protezione della barra degli strumenti
    - ***Avvia AVG 8.0***: consente di aprire l'interfaccia utente di AVG 8
    - ***Opzioni***: consente di aprire una finestra di dialogo di configurazione in cui è possibile modificare le impostazioni di ***AVG Security Toolbar*** in base alle proprie esigenze; la finestra di dialogo è suddivisa in due schede:
        - ***Generale*** - su questa scheda è possibile trovare sezioni denominate ***Pulsanti*** and ***Valutazioni***.

          La sezione ***Pulsanti*** consente di configurare i pulsanti da visualizzare o nascondere in ***AVG Security Toolbar***. Per impostazione predefinita tutti i pulsanti sono visualizzati.

          La sezione ***Valutazioni*** consente di determinare il tipo di valutazione che si desidera visualizzare per i risultati della ricerca. Per impostazione predefinita, tutte le valutazioni sono visualizzate ma è tuttavia possibile nasconderne alcune (*quando si esegue la ricerca dalla casella di ricerca di Yahoo!, vengono visualizzati solo i risultati sicuri*).



➢ ***Avanzate***: questa scheda consente di modificare le funzionalità di protezione di ***AVG Security Toolbar***. Per impostazione predefinita, entrambe le funzionalità ***AVG Search-Shield*** e ***AVG Active Surf-Shield*** sono abilitate.



o ***Aggiorna***: consente di controllare la disponibilità di nuovi aggiornamenti per ***AVG Security Toolbar.***

o ***Guida***: fornisce le opzioni per aprire il file della guida, contattare l' ***Assistenza tecnica*** oppure visualizzare i dettagli della versione

corrente della barra degli strumenti

- ***Casella di ricerca con tecnologia Yahoo!***: un modo sicuro e conveniente di eseguire ricerche utilizzando il motore di ricerca Yahoo!. Immettere una parola o una frase nella casella di ricerca, premere ***Ricerca*** per iniziare la ricerca direttamente sul server Yahoo! indipendentemente dalla pagina correntemente visualizzata. Nella casella di ricerca viene inoltre elencata la cronologia della ricerca. Le ricerche eseguite dalla casella di ricerca vengono analizzate da AVG Search-Shield.

- ***Pulsante AVG Active Surf-Shield***: il pulsante attivato/disattivato controlla lo stato di protezione di ***AVG Active Surf-Shield***

- ***Pulsante AVG Search-Shield***: il pulsante attivato/disattivato controlla lo stato di protezione di ***AVG Search-Shield***

- ***Pulsante Info AVG***: fornisce il collegamento a informazioni importanti contenute nel sito Web di AVG (www.avg.com).

11. Identity_Protection

Identity Protection è un componente autonomo precedentemente noto con il nome di Sana ed è stato recentemente integrato in **AVG 8.5 Internet Security** . Viene installato dallo stesso file di installazione con l'appropriato numero di licenza (*per dettagli sulla selezione del prodotto e le relative licenze si prega di consultare AVG Download Manager*).

Identity Protection è al momento disponibile solo in lingua Inglese.

11.1.Identity_Protection_Principles

Software di prevenzione dei furti di identità

La tecnologia di Sana proviene dal software di sicurezza basato sul comportamento Dato che rileva le caratteristiche e il comportamento delle minacce e dei malware, Sana è un software unico e versatile che previene attacchi al PC da minacce nuove ed emergenti in tempo reale (protezione in zero-day). Secondo le affermazioni dello staff di Sana; "Protezione istantanea e costante".

11.2.Identity_Protection_Interface

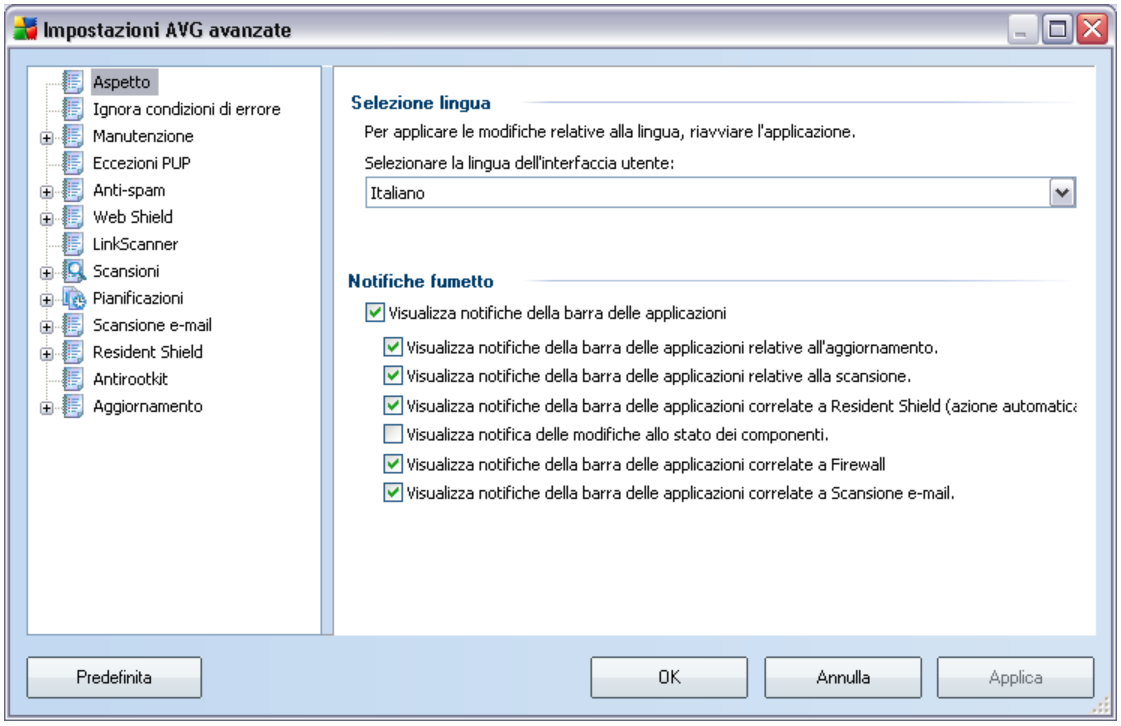
Immettere qui il testo dell'argomento

12. Impostazioni AVG avanzate

La finestra di dialogo della configurazione avanzata di **AVG 8.5 Internet Security** viene aperta in una nuova finestra denominata ***Impostazioni AVG avanzate***. La finestra è suddivisa in due sezioni: la parte sinistra fornisce una struttura di esplorazione per accedere alle opzioni di configurazione del programma. Selezionare il componente di cui si desidera modificare la configurazione (*o una parte specifica*) per aprire la finestra di dialogo di modifica nella sezione destra della finestra.

12.1.Aspetto

La prima voce della struttura di esplorazione, ***Aspetto***, fa riferimento alle impostazioni generali di Interfaccia utente di AVG e ad alcune opzioni di base del comportamento dell'applicazione:



Selezione lingua

Nella sezione ***Selezione lingua*** è possibile scegliere la lingua desiderata dal menu a discesa; tale lingua verrà quindi utilizzata per l'intera interfaccia utente di AVG. Nel menu a discesa sono presenti solo le lingue selezionate in precedenza per essere

installate durante il processo di installazione (vedere il capitolo Installazione personalizzata - Selezione componenti). Tuttavia, per modificare la lingua dell'applicazione, è necessario riavviare l'interfaccia utente. A tale scopo, procedere come segue:

- Selezionare la lingua desiderata dell'applicazione e confermare la selezione premendo il pulsante ***Applica*** (nell'angolo inferiore destro)
- Premere il pulsante ***OK*** per chiudere la finestra di dialogo di modifica ***Impostazioni AVG avanzate***
- Chiudere Interfaccia utente AVG dall'opzione della voce del menu di sistema ***File/Esci***
- Riaprire Interfaccia utente di AVG selezionando una delle seguenti opzioni: fare doppio clic sull'icona di AVG sulla barra delle applicazioni, fare doppio clic sull'icona di AVG sul desktop oppure dal menu ***Start/Tutti i programmi/ AVG 8.0/Interfaccia utente di AVG*** (vedere il capitolo ***Accesso all'interfaccia utente***). L'interfaccia utente verrà quindi visualizzata nella nuova lingua selezionata.

Notifiche tramite balloon

All'interno di questa sezione è possibile disattivare la visualizzazione delle notifiche tramite balloon presenti sulla barra delle applicazioni e che informano sullo stato dell'applicazione. Per impostazione predefinita, è consentita la visualizzazione delle notifiche tramite balloon, si consiglia pertanto di mantenere questa configurazione. In genere le notifiche tramite balloon forniscono informazioni sul cambiamento di stato dei componenti di AVG, vanno pertanto tenute nella dovuta considerazione.

Tuttavia, se per qualche ragione non si desidera visualizzare tali notifiche o visualizzarne solo alcune (correlate a un componente AVG specifico), è possibile definire e specificare le proprie preferenze selezionando/deselezionando le opzioni seguenti:

- ***Visualizza notifiche della barra delle applicazioni***: per impostazione predefinita, questa voce è selezionata (*attivata*) e le notifiche vengono visualizzate. Deselezionarla per disattivare completamente la visualizzazione delle notifiche tramite balloon. Quando è attivata, è possibile selezionare ulteriormente le notifiche specifiche da visualizzare:
  - ***Visualizza notifiche della barra delle applicazioni relative all' aggiornamento***: consente di decidere se visualizzare le informazioni

relative all'avvio, all'avanzamento e alla finalizzazione del processo di aggiornamento di AVG.

- ***Visualizza notifiche della barra delle applicazioni relative alla scansione***: consente di decidere se visualizzare le informazioni relative all'avvio automatico, all'avanzamento e ai risultati della scansione pianificata.

- ***Visualizza notifiche della barra delle applicazioni relative a Resident Shield*** : consente di decidere se visualizzare o sopprimere le informazioni relative ai processi di salvataggio, copia e apertura dei file.

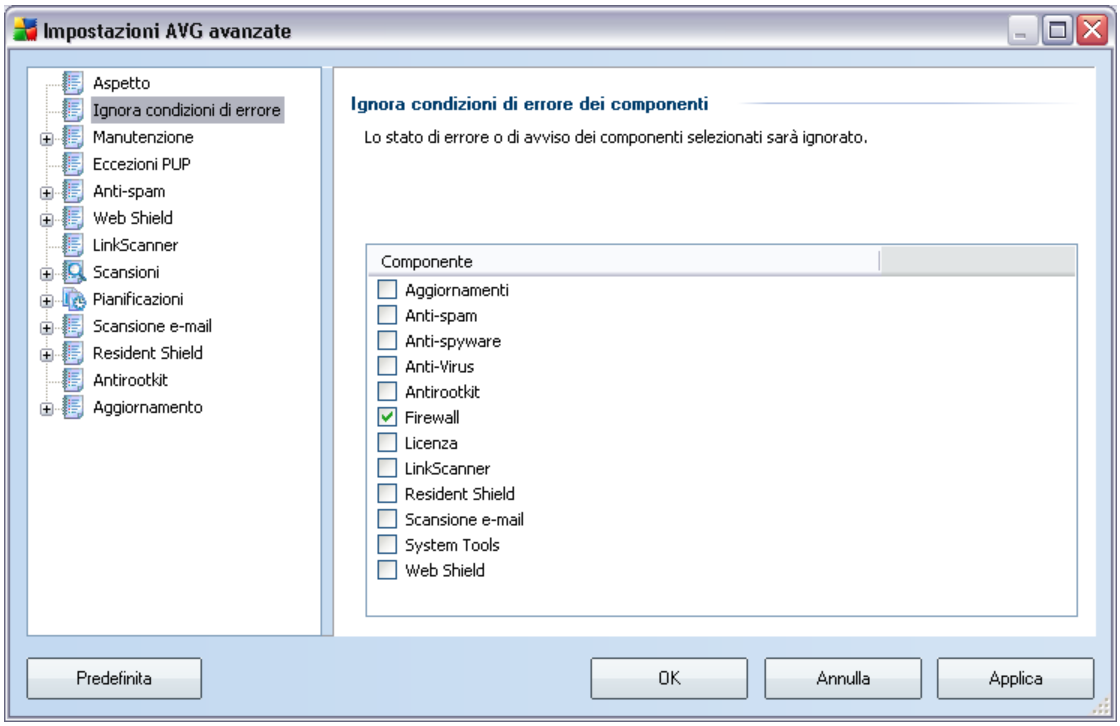
- ***Visualizza notifica delle modifiche allo stato dei componenti***: consente di decidere se visualizzare le informazioni relative allo stato di attività/inattività del componente o a un suo eventuale problema. Quando viene riportato lo stato di errore di un componente, questa opzione equivale alla funzione informativa della icona della barra delle applicazioni (cambio di colore) per indicare un problema in un componente di AVG.

- ***Visualizza notifiche della barra delle applicazioni correlate a Firewall*** : consente di decidere se visualizzare le informazioni relative ai processi e allo stato del firewall, quali avvisi di attivazione/disattivazione del componente, possibile blocco del traffico e così via.

- ***Visualizza notifiche della barra delle applicazioni correlate a Scansione E-mail*** : consente di decidere se visualizzare le informazioni relative alla scansione di tutti i messaggi e-mail in entrata e in uscita.

12.2.Ignora condizioni di errore

Nella finestra di dialogo ***Ignora condizioni di errore dei componenti*** è possibile selezionare i componenti in merito ai quali non si desidera ricevere informazioni:



Per impostazione predefinita, in questo elenco non è selezionato alcun componente. Ciò significa che se per un qualsiasi componente si verifica uno stato di errore, se ne verrà immediatamente informati tramite:

- ***l'icona presente nella barra delle applicazioni***: quando tutte le parti di AVG funzionano correttamente, l'icona viene visualizzata in quattro colori; se si verifica un errore, l'icona viene visualizzata in grigio con un punto esclamativo rosso,

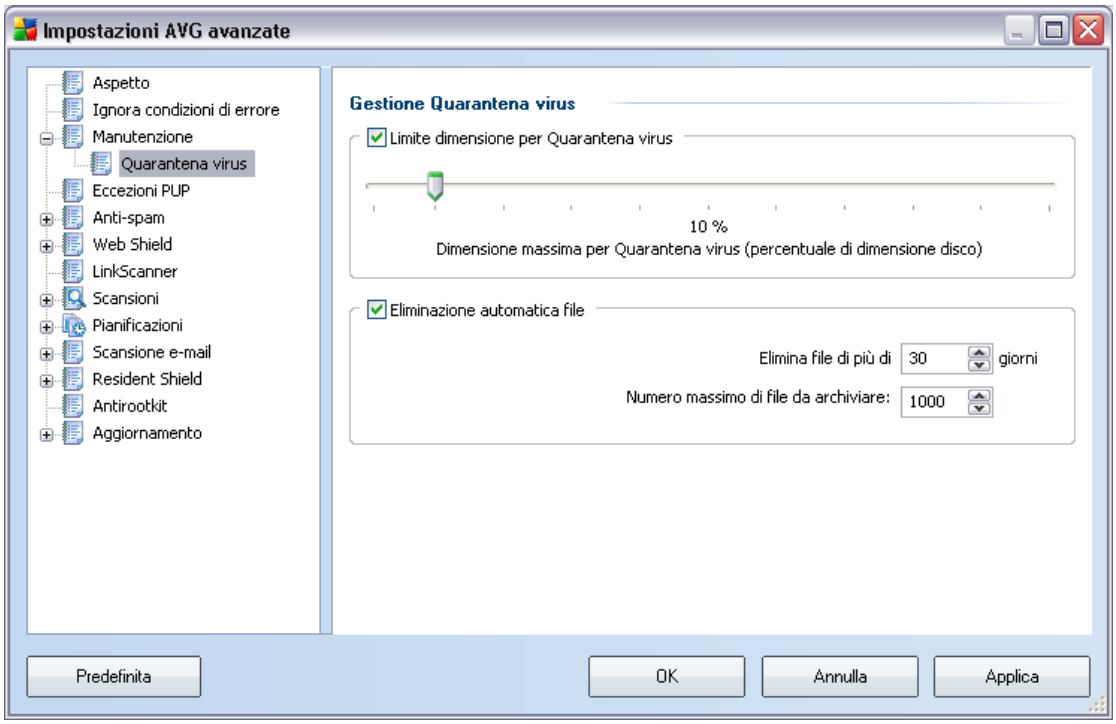
- una descrizione del problema esistente visualizzata nella sezione ***Informazioni sullo stato di protezione*** della finestra principale di AVG

Potrebbe verificarsi una situazione in cui, per qualsiasi motivo, risulti necessario disattivare un componente temporaneamente (*questa operazione tuttavia non è consigliata: si dovrebbe tentare di mantenere tutti i componenti attivati in modo permanente e con la configurazione predefinita*). In tal caso, l'icona presente nella

barra delle applicazioni segnala automaticamente lo stato di errore del componente. In casi del genere, tuttavia, non è possibile parlare di errore effettivo, poiché la condizione è stata indotta deliberatamente dall'utente e si è consapevoli del potenziale rischio. Nel contempo, una volta che viene visualizzata in grigio, l'icona non può più segnalare eventuali errori ulteriori che potrebbero verificarsi.

Per gestire situazioni simili, all'interno della suddetta finestra di dialogo è possibile selezionare i componenti che potrebbero trovarsi in stato di errore (*o disattivati*) in merito ai quali non si desidera ricevere informazioni. Per ***ignorare lo stato di componenti specifici*** è inoltre possibile utilizzare direttamente la panoramica dei componenti presente nella finestra principale di AVG.

12.3.Quarantena virus



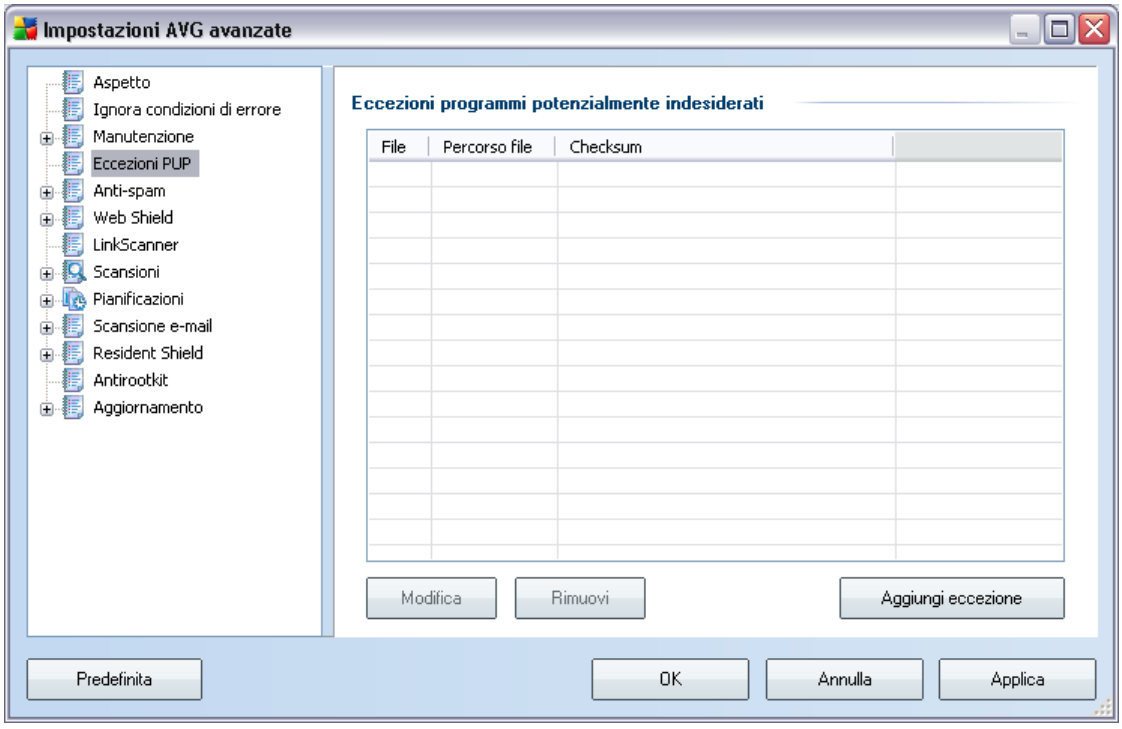
La finestra di dialogo ***Gestione Quarantena virus*** consente di definire diversi parametri relativi alla gestione degli oggetti archiviati in ***Quarantena virus***:

- ***Limite dimensione per Quarantena virus***: utilizzare il dispositivo di scorrimento per impostare la dimensione massima di ***Quarantena virus***. La dimensione è specificata in maniera proporzionale rispetto alla dimensione del disco locale.

- ***Eliminazione automatica file***: questa sezione consente di definire la durata massima di memorizzazione degli oggetti in ***Quarantena virus*** (***Elimina file di più di...giorni***) e il numero massimo di file da memorizzare in ***Quarantena virus*** (***Numero massimo di file da memorizzare***)

12.4.Eccezioni PUP

AVG è in grado di analizzare e rilevare le applicazioni eseguibili o le librerie DLL che potrebbero essere potenzialmente indesiderate nel sistema. In alcuni casi l'utente può desiderare di mantenere alcuni programmi indesiderati sul computer (programmi che sono stati installati intenzionalmente). Alcuni programmi, soprattutto quelli gratuiti, includono adware. Tale adware potrebbe essere rilevato e segnalato da AVG come ***programma potenzialmente indesiderato***. Se si desidera mantenere tali programmi sul computer, è possibile definirli come eccezioni ai programmi potenzialmente indesiderati:



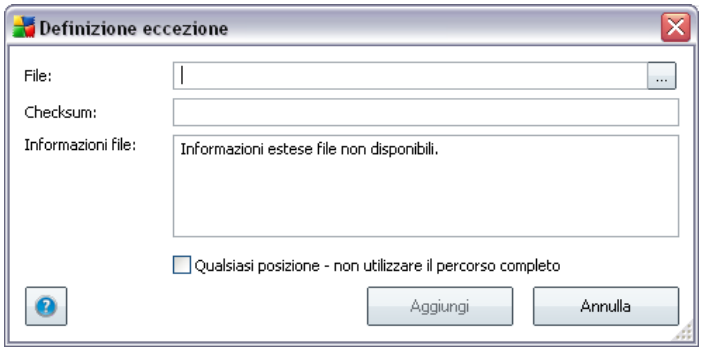
Nella finestra di dialogo ***Eccezioni ai programmi potenzialmente indesiderati*** viene visualizzato un elenco di eccezioni già definite e attualmente valide da programmi potenzialmente indesiderati. È possibile modificare, eliminare o aggiungere nuove eccezioni.

Pulsanti di controllo

- ***Modifica***: consente di aprire una finestra di dialogo per la modifica (*identica alla finestra di dialogo per la definizione di una nuova eccezione, vedere di seguito*) di un'eccezione già definita. In tale finestra è possibile modificare i parametri dell'eccezione.

- ***Rimuovi***: consente di eliminare la voce selezionata dall'elenco di eccezioni.

- ***Aggiungi eccezione***: consente di aprire una finestra di dialogo per la modifica in cui è possibile definire i parametri della nuova eccezione da creare:



  - ***File***: digitare il percorso completo del file da contrassegnare come eccezione.

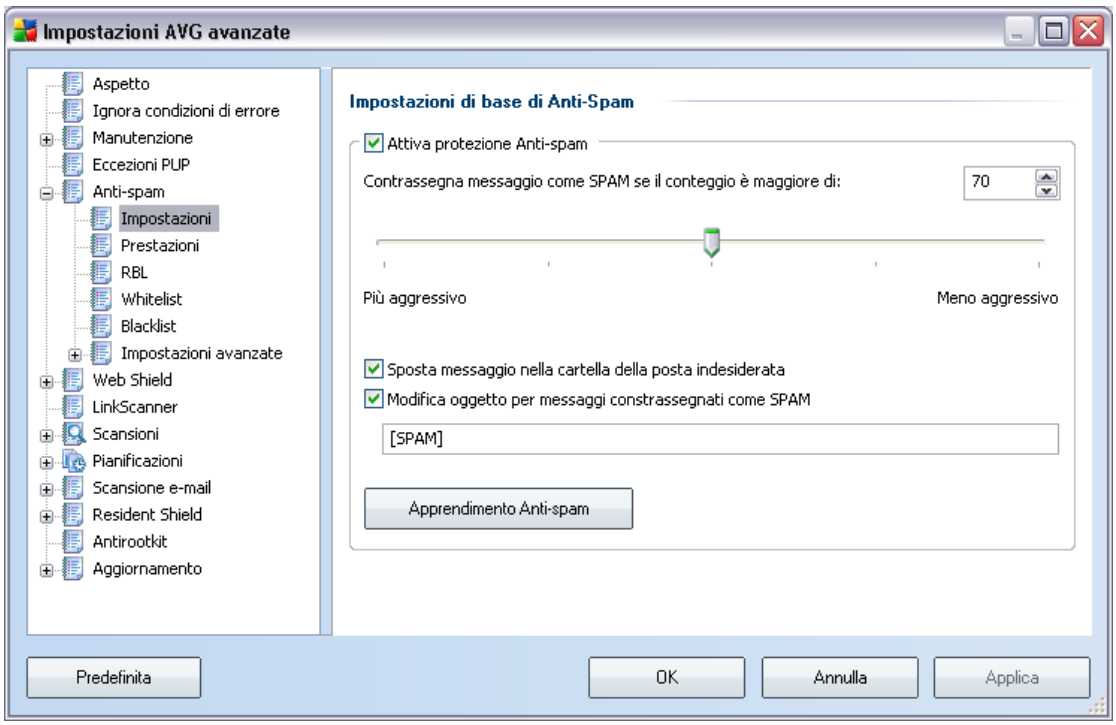
  - ***Checksum***: viene visualizzata la "firma" univoca del file prescelto. Questo checksum è una stringa di caratteri generata automaticamente che consente ad AVG di distinguere in modo inequivocabile il file scelto dagli altri file. Il checksum viene generato e visualizzato dopo che il file è stato aggiunto correttamente.

  - ***Informazioni file***: vengono visualizzate eventuali informazioni aggiuntive disponibili sul file (*sulla licenza, la versione e così via*).

  - ***Qualsiasi posizione - non utilizzare il percorso completo***: per definire il file come eccezione solo per la posizione specifica, lasciare deselezionata questa casella di controllo.

12.5.Anti-Spam

12.5.1.Impostazioni



Nella finestra di dialogo ***Impostazioni delle prestazioni del motore*** è possibile selezionare la casella di controllo ***Attiva protezione Anti-Spam*** per consentire/ impedire la scansione anti-spam delle comunicazioni e-mail.

Nella finestra di dialogo è anche possibile selezionare il grado di "aggressività" della configurazione del conteggio. Il filtro ***Anti-Spam*** assegna a ciascun messaggio un conteggio (*ad esempio, il grado di somiglianza del contenuto del messaggio a SPAM*) in base a diverse tecniche di scansione dinamica. È possibile regolare l'impostazione ***Contrassegna messaggio come spam se il conteggio è maggiore di*** digitando il valore (*da 0 a 100*) oppure spostando il dispositivo di scorrimento verso sinistra o verso destra (*utilizzando il dispositivo di scorrimento, l'intervallo di valori è compreso tra 50 e 90*).

Si consiglia in genere di impostare la soglia tra 50 e 90 oppure, se si è insicuri, su 90. Di seguito viene fornita una panoramica generale della soglia di conteggio:

- ***Valore compreso tra 90 e 99***: la maggior parte dei messaggi e-mail in entrata verranno recapitati normalmente (senza essere contrassegnati come spam). Lo spam identificato più facilmente verrà filtrato, tuttavia si potrebbe ricevere una notevole quantità di spam.

- ***Valore compreso tra 80 e 89***: verranno filtrati i messaggi e-mail il cui contenuto potrebbe essere spam, ma potrebbero essere filtrati anche alcuni messaggi che non ne contengono.

- ***Valore tra 60 e 79***: è considerata una configurazione abbastanza aggressiva. Verranno filtrati i messaggi e-mail il cui contenuto può essere spam, ma potrebbero essere filtrati anche messaggi che non ne contengono.

- ***Valore tra 1 e 59***: configurazione particolarmente aggressiva. È probabile che insieme ai messaggi e-mail contenenti spamvengano filtrati anche i messaggi normali. Questo intervallo di valori non è consigliato.

- ***Valore 0***: in questa modalità, si riceveranno solo i messaggi e-mail provenienti da mittenti inclusi nella ***whitelist***. Gli altri messaggi e-mail verranno considerati spam. ***Questo intervallo di valori non è consigliato.***

Nella finestra di dialogo ***Impostazioni delle prestazioni del motore*** è possibile definire ulteriormente la modalità in cui dovrebbero essere gestiti i messaggi e-mail di spam :

- ***Sposta messaggio nella cartella della posta indesiderata***: selezionare la casella di controllo per specificare che ciascun messaggio di spam rilevato deve essere automaticamente spostato nella cartella specifica della posta indesiderata all'interno del client e-mail;

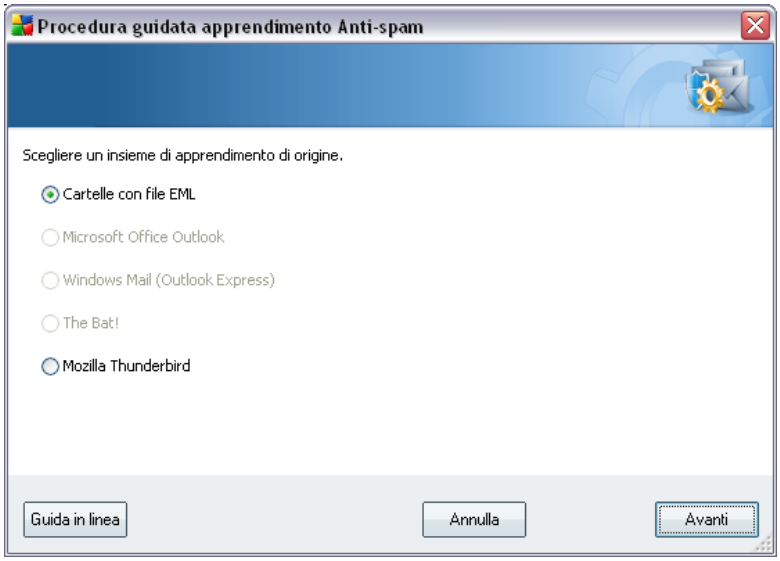
- ***Aggiungi destinatari delle e-mail inviate alla whitelist*** : selezionare questa casella di controllo per confermare che tutti i destinatari delle e-mail inviate sono affidabili e tutti le e-mail provenienti dai relativi account e-mail possono essere consegnate;

- ***Modifica oggetto per messaggi contrassegnati come spam***: selezionare questa casella di controllo se si desidera che tutti i messaggi rilevati come spam vengano contrassegnati con una parola o un carattere specifico nel campo dell'oggetto del messaggio e-mail; il testo desiderato può essere digitato nel campo di testo attivato.

Pulsanti di controllo

Il pulsante Apprendimento Anti-Spam consente di aprire la ***Procedura guidata apprendimento anti-spam*** descritta dettagliatamente nel capitolo successivo.

Nella prima finestra di dialogo della ***Procedura guidata apprendimento anti-spam*** viene richiesto di selezionare l'origine di messaggi e-mail da utilizzare per l'apprendimento. Di norma, si utilizzeranno messaggi e-mail erroneamente contrassegnati come SPAM o messaggi di spam che non sono stati riconosciuti.



Sono disponibili le seguenti opzioni:

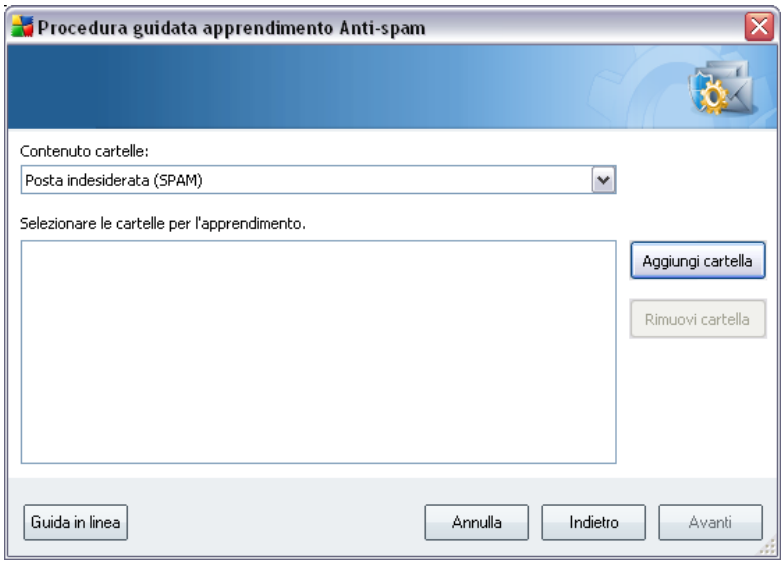
- ***Un client e-mail specifico***: se si utilizza uno dei client e-mail elencati (*MS Outlook, Outlook Express, The Bat!, Mozilla Thunderbird*), selezionare la relativa opzione
- ***Cartella con file EML***: se si utilizza qualsiasi altro programma e-mail, è necessario salvare i messaggi in una cartella specifica (nel *formato .eml*) oppure accertarsi di conoscere il percorso delle cartelle dei messaggi del client e-mail. Quindi, selezionare ***Cartella con file EML***, che consentirà di individuare la cartella desiderata al passaggio successivo

Per un processo di apprendimento più semplice e rapido, è innanzitutto consigliabile ordinare i messaggi e-mail nelle cartelle, in modo che la cartella utilizzata per l'apprendimento contenga solo i messaggi per l'apprendimento (desiderati o indesiderati). Tuttavia, non è necessario, poiché sarà possibile filtrare i messaggi e-mail in seguito.

Selezionare l'opzione appropriata e fare clic su ***Avanti*** per continuare la procedura guidata.

La finestra di dialogo visualizzata a questo passaggio dipende dalla selezione precedente.

Cartelle con file EML



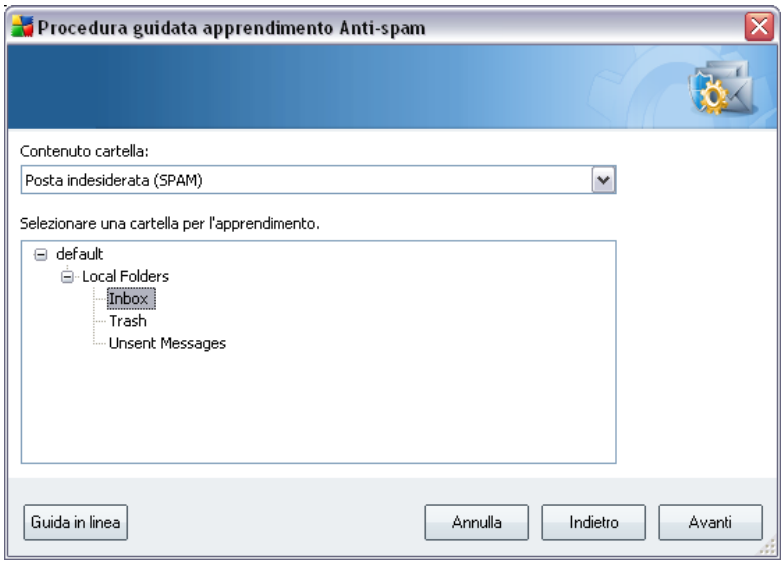
In questa finestra di dialogo selezionare la cartella contenente i messaggi che si desidera utilizzare per l'apprendimento. Fare clic sul pulsante ***Aggiungi cartella*** per individuare la cartella con i file .eml (*messaggi e-mail salvati*). La cartella selezionata verrà visualizzata nella finestra di dialogo.

Nel menu a discesa ***Contenuto delle cartelle*** impostare una delle due opzioni per indicare se la cartella selezionata contiene posta desiderata (*HAM*) o indesiderata (*SPAM*). Notare che al passaggio successivo sarà possibile filtrare i messaggi, pertanto non è necessario che la cartella contenga soltanto i messaggi necessari per l'apprendimento. È inoltre possibile rimuovere le cartelle indesiderate selezionate dall'elenco facendo clic sul pulsante ***Rimuovi cartella***.

Una volta eseguita l'operazione, fare clic su ***Avanti*** e passare a ***Opzioni di filtro dei messaggi***.

E-mail client specifico

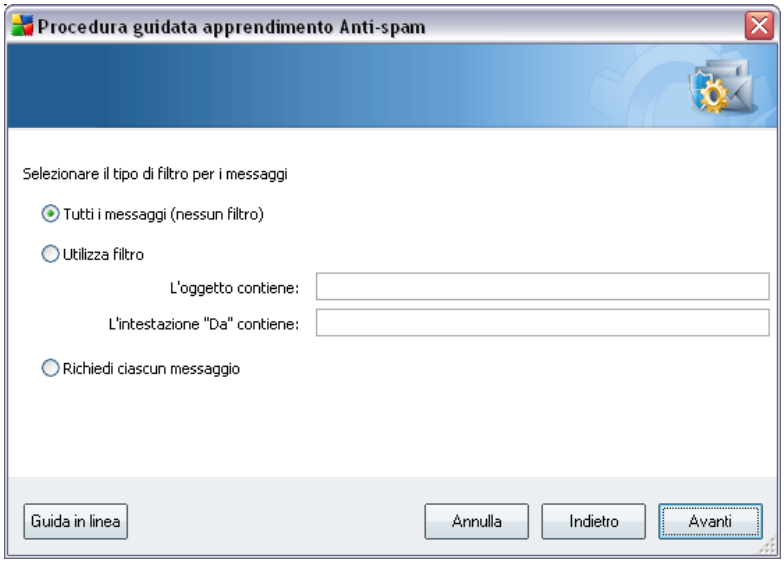
Dopo aver confermato un'opzione, viene visualizzata una nuova finestra di dialogo.



Nota: *se si utilizza Microsoft Office Outlook, verrà richiesto di selezionare il primo profilo di MS Office Outlook.*

Nel menu a discesa ***Contenuto delle cartelle*** impostare una delle due opzioni per indicare se la cartella selezionata contiene posta desiderata (*HAM*) o indesiderata (*SPAM*). Notare che al passaggio successivo sarà possibile filtrare i messaggi, pertanto non è necessario che la cartella contenga soltanto i messaggi necessari per l'apprendimento. Nella sezione principale della finestra di dialogo è già visualizzata una struttura di esplorazione del client e-mail selezionato. Individuare la cartella desiderata nella struttura ed evidenziarla utilizzando il mouse.

Una volta eseguita l'operazione, fare clic su ***Avanti*** e passare a ***Opzioni di filtro dei messaggi***.



In questa finestra di dialogo è possibile impostare il filtro per i messaggi e-mail.

Se si è certi che la cartella selezionata contenga soltanto messaggi che si desidera utilizzare per l'apprendimento, selezionare l'opzione ***Tutti i messaggi (nessun filtro)***.

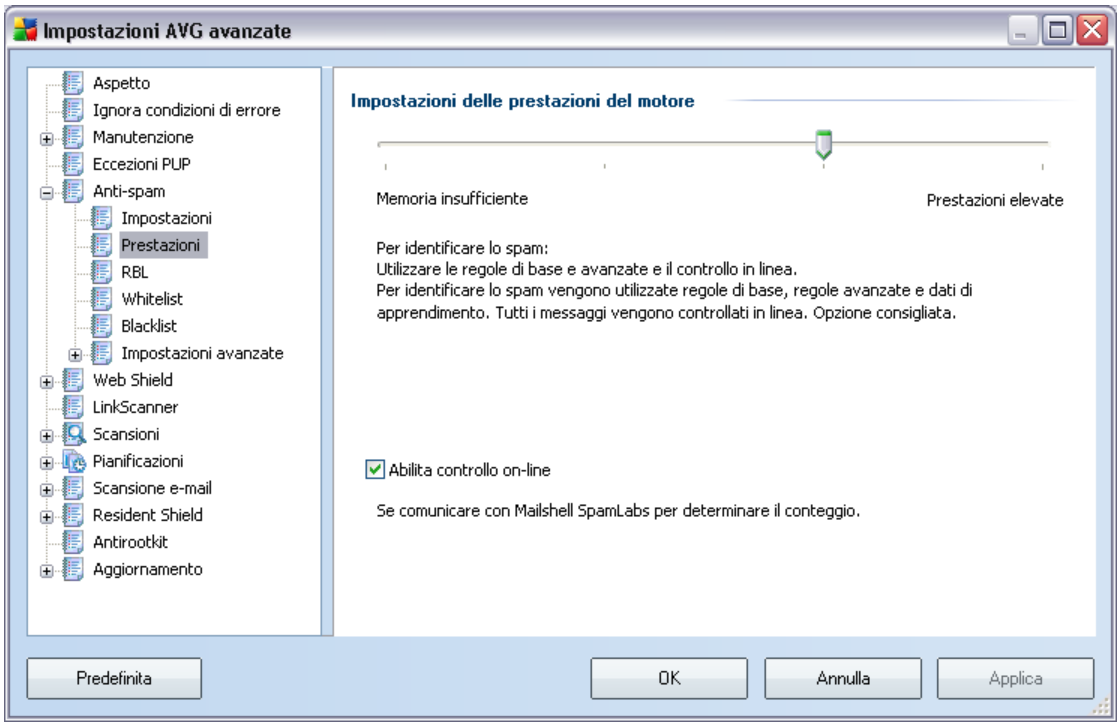
Se non si è certi dei messaggi contenuti nella cartella e si desidera che durante la procedura guidata venga richiesta una conferma per ogni singolo messaggio (al fine di determinare se utilizzarlo o meno per l'apprendimento), selezionare l'opzione ***Chiedi per ogni messaggio***.

Per le opzioni di filtro avanzate, selezionare l'opzione ***Usa filtro***. È possibile inserire una parola (*nome*), una parte di una parola o una frase da ricercare nell'oggetto dell'e-mail e/o nel campo del mittente. Tutti i messaggi che corrispondono esattamente ai criteri specificati verranno utilizzati per l'apprendimento, senza che vengano visualizzate ulteriori richieste di conferma.

Attenzione: *se si compilano entrambi i campi di testo, verranno utilizzati anche gli indirizzi che corrispondono a uno solo dei criteri.*

Dopo aver selezionato l'opzione appropriata, fare clic su ***Avanti***. La finestra di dialogo seguente avrà uno scopo puramente informativo, in quanto indica che la procedura guidata è pronta per l'elaborazione dei messaggi. Per avviare l'apprendimento, fare nuovamente clic su ***Avanti***. L'apprendimento viene avviato in base alle condizioni precedentemente selezionate.

12.5.2.Prestazioni



La finestra di dialogo ***Impostazioni delle prestazioni del motore*** (*accessibile dalla voce* ***Prestazioni*** *del menu di esplorazione visualizzato a sinistra*) offre le impostazioni delle prestazioni del componente ***Anti-Spam***. Spostare il dispositivo di scorrimento a destra o a sinistra per modificare il livello di intervallo delle prestazioni di scansione tra le modalità ***Memoria insufficiente*** / ***Prestazioni elevate***.

- ***Memoria insufficiente***: durante il processo di scansione per l'identificazione dello spam, non viene utilizzata alcuna regola. Per l'identificazione dello spam verranno utilizzati solo i dati di formazione. Questa modalità non è consigliata, a meno che l'hardware del computer sia estremamente limitato.

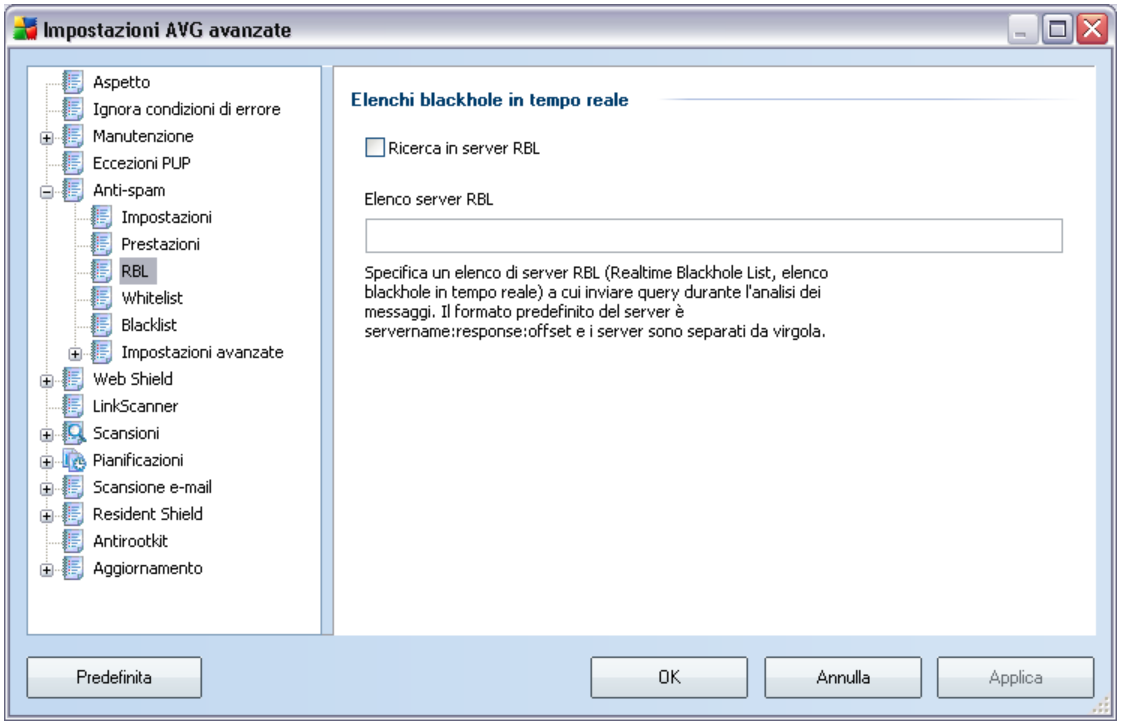
- ***Prestazioni elevate***: questa modalità richiederà una notevole quantità di memoria. Durante il processo di scansione per l'identificazione dello spam, verranno utilizzate le seguenti funzionalità: regole e la cache del database di spam, regole di base e avanzate, indirizzi IP e database di spammer.

La voce ***Abilita controllo on-line*** è attiva per impostazione predefinita. Ne risulta un rilevamento dello spam più preciso tramite la comunicazione con i server Mailshell, ovvero, i dati sottoposti a scansione verranno confrontati con i database Mailshell on-line.

In genere si consiglia di mantenere le impostazioni predefinite e di modificarle solo se esiste un reale motivo per farlo. Le eventuali modifiche alla configurazione devono essere eseguite solo da utenti esperti.

12.5.3.RBL

L'elemento ***RBL*** consente di aprire una finestra di dialogo modificabile denominata ***Elenchi blackhole in tempo reale*** (Realtime Blackhole Lists):



In questa finestra di dialogo è possibile attivare/disattivare la funzione ***Ricerca in server RBL***.

Il server RBL (*Realtime Blackhole List, Elenchi blackhole in tempo reale*) è un server DNS con un vasto database di mittenti di spam noti. Se questa funzione è attivata, tutti i messaggi di posta elettronica verranno verificati in base al database del server RBL e verranno contrassegnati come spam se risultano identici a una delle voci nel database.

I database dei server RBL contengono le impronte digitali di spam più aggiornate, per fornire il rilevamento di spam migliore e più accurato. La funzione è particolarmente utile per gli utenti che ricevono grandi quantità di messaggi di spam normalmente

non rilevati dal motore Anti-Spam.

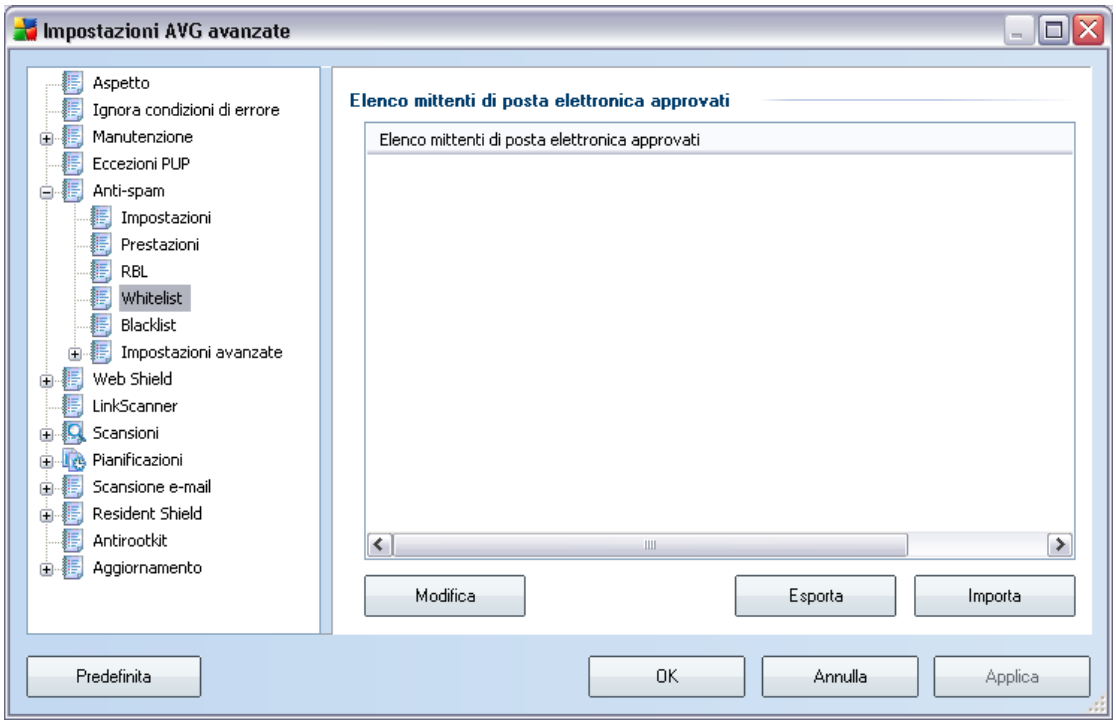
La funzione ***Elenco server RBL*** consente di definire le posizioni dei server RBL specifici. Per impostazione predefinita, sono specificati due indirizzi server RBL. Se non si è un utente esperto e se non si necessita veramente di modificare queste impostazioni, si consiglia di mantenere le impostazioni predefinite.

Nota: *l'abilitazione di questa funzionalità potrebbe rallentare il processo di ricezione dei messaggi e-mail in alcuni sistemi e configurazioni, poiché ogni singolo messaggio deve essere confrontato con il database del server RBL.*

Non vengono inviati dati personali sul server.

12.5.4.Whitelist

La voce ***Whitelist*** consente di aprire una finestra di dialogo con un elenco globale di indirizzi di mittenti e-mail e nomi di dominio approvati i cui messaggi non verranno mai contrassegnati come spam.



Nell'interfaccia di modifica è possibile compilare un elenco di mittenti da cui si ha la certezza che non verranno mai inviati messaggi indesiderati (spam). È inoltre possibile compilare un elenco di nomi di dominio completi (ad esempio *avg.com*), che

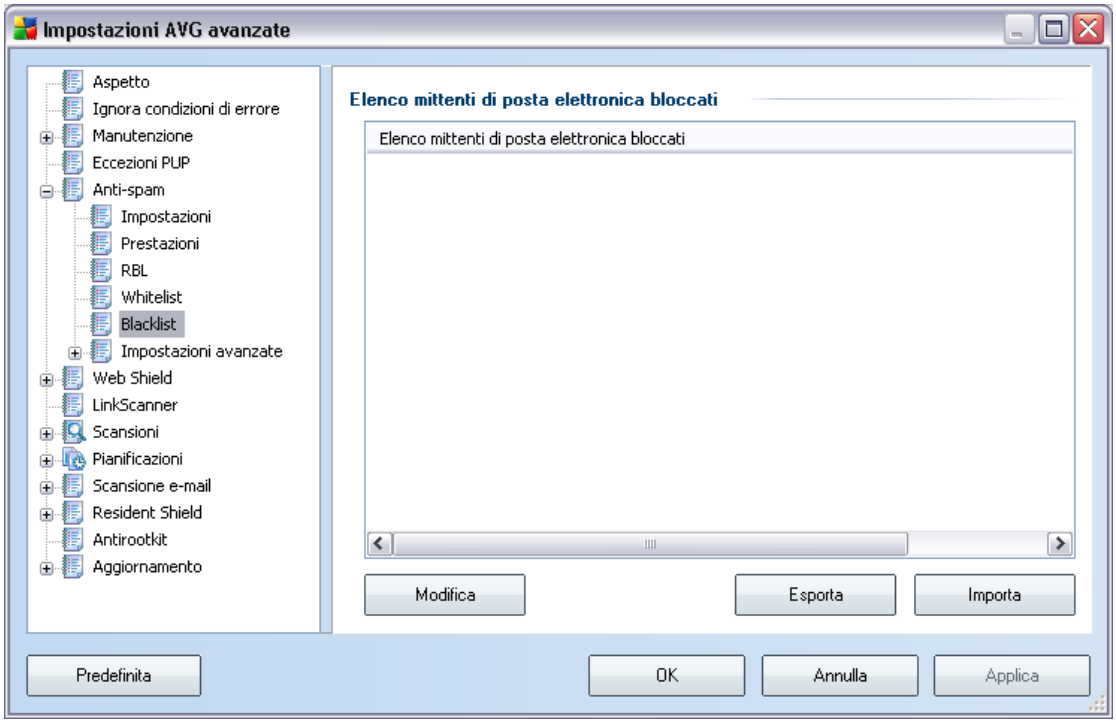
non generanno mai messaggi spam.

Dopo che è stato preparato un simile elenco di mittenti e/o nomi di dominio, è possibile inserirli in due modi diversi: inserendo direttamente ciascun indirizzo e-mail o importando tutto l'elenco di indirizzi. Sono disponibili i seguenti pulsanti di controllo:

- ***Modifica***: premere questo pulsante per aprire una finestra di dialogo, in cui è possibile inserire manualmente un elenco di indirizzi (è possibile anche utilizzare *copia e incolla*). Inserire un singolo elemento (mittente o nome di dominio) per ogni riga.
- ***Importa***: se si possiede già un file di testo di indirizzi di posta elettronica o nomi di dominio, è possibile importare tale file selezionando questo pulsante. Il file di input deve essere in formato di testo normale e il contenuto deve includere un singolo elemento (indirizzo o nome di dominio) per riga.
- ***Esporta***: se per qualsiasi motivo si decide di esportare i record, è possibile fare clic sul pulsante per eseguire l'operazione. Tutti i record verranno salvati in un file di testo normale.

12.5.5.Blacklist

La voce ***Blacklist*** consente di aprire una finestra di dialogo contenente un elenco globale di nomi di dominio e indirizzi e-mail di mittenti bloccati i cui messaggi saranno sempre contrassegnati come spam.



Nell'interfaccia di modifica è possibile compilare un elenco di mittenti da cui si ha la certezza che verranno inviati messaggi indesiderati (spam). È inoltre possibile compilare un elenco di nomi di dominio completi (ad esempio *aziendaspamming.com*), da cui si prevedono o si ricevono messaggi di spam. Tutti i messaggi di posta elettronica ricevuti da tali indirizzi o domini specifici verranno contrassegnati come spam.

Dopo che è stato preparato un simile elenco di mittenti e/o nomi di dominio, è possibile inserirli in due modi diversi: inserendo direttamente ciascun indirizzo e-mail o importando tutto l'elenco di indirizzi. Sono disponibili i seguenti pulsanti di controllo:

- ***Modifica***: premere questo pulsante per aprire una finestra di dialogo, in cui è possibile inserire manualmente un elenco di indirizzi (è possibile anche utilizzare *copia e incolla*). Inserire un singolo elemento (mittente o nome di dominio) per ogni riga.

- ***Importa***: se si possiede già un file di testo di indirizzi di posta elettronica o nomi di dominio, è possibile importare tale file selezionando questo pulsante. Il file di input deve essere in formato di testo normale e il contenuto deve includere un singolo elemento (indirizzo o nome di dominio) per riga.

- ***Esporta***: se per qualsiasi motivo si decide di esportare i record, è possibile fare clic sul pulsante per eseguire l'operazione. Tutti i record verranno salvati in un file di testo normale.

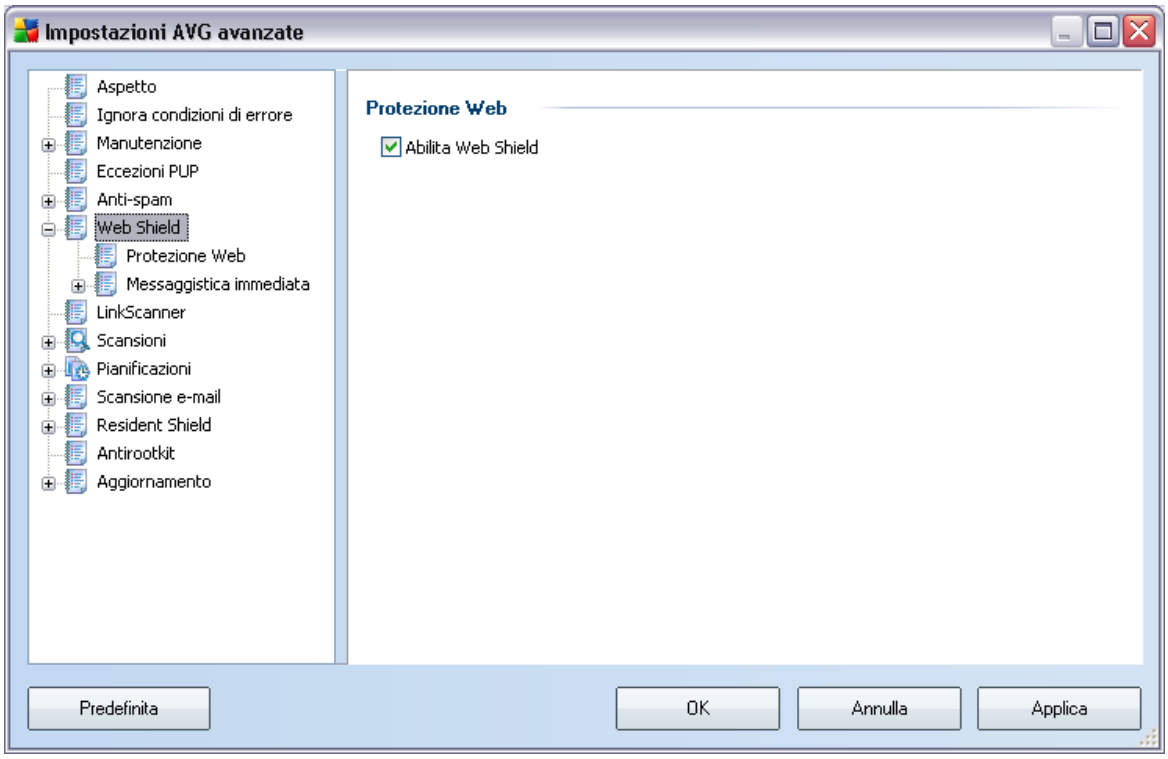
12.5.6.Impostazioni avanzate

In genere si consiglia di mantenere le impostazioni predefinite e di modificarle solo se esiste un reale motivo per farlo. Le eventuali modifiche alla configurazione devono essere eseguite solo da utenti esperti.

Se si ritiene di dover modificare comunque la configurazione ***Anti-Spam*** portandola a un livello molto avanzato, seguire le istruzioni fornite direttamente nell'interfaccia utente. In genere, in ciascuna finestra di dialogo è contenuta una sola funzionalità specifica che può essere modificata. La descrizione relativa è sempre inclusa nella finestra di dialogo:

- ***Cache*** : impronte digitali, reputazione dominio, LegitRepute
- ***Apprendimento***: apprendimento di parole, cronologia conteggio, offset conteggio, numero massimo di parole, soglia di apprendimento automatico, peso, buffer scrittura
- ***Filtraggio***: elenco lingue, elenco paesi, IP approvati, IP bloccati, paesi bloccati, set di caratteri bloccati, mittenti contraffatti
- ***RBL***: server RBL, multihit, soglia, timeout, massimo IP
- ***Controllo della rete***: soglia controllo della rete
- ***Connessione a Internet***: timeout

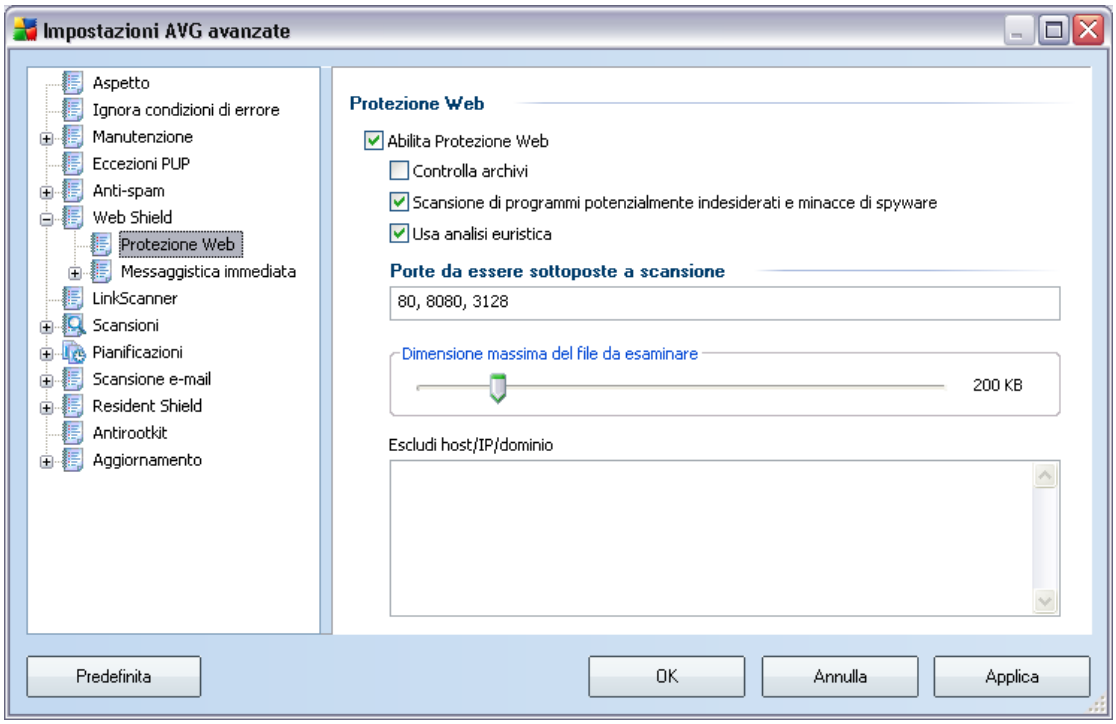
12.6.Web Shield



La finestra di dialogo ***Protezione Web*** consente di attivare/disattivare l'intero componente ***Web Shield*** (*attivato per impostazione predefinita*). Per altre impostazioni avanzate del componente passare alle finestre di dialogo successive elencate nella struttura di esplorazione.

Nella parte inferiore della finestra di dialogo, scegliere in che modo si desidera essere informati circa eventuali minacce rilevate: mediante una finestra popup standard, mediante una notifica tramite fumetto nella barra delle applicazioni oppure mediante indicazioni dell'icona nella barra delle applicazioni.

12.6.1.Protezione Web



La finestra di dialogo ***Protezione Web*** consente di modificare la configurazione del componente relativa alla scansione del contenuto di siti Web. L'interfaccia di modifica consente di configurare le seguenti opzioni di base:

- ***Protezione Web***: questa opzione conferma che ***Protezione Web*** deve eseguire la scansione del contenuto delle pagine Web. Se questa opzione è attiva (*per impostazione predefinita*), è possibile attivare/disattivare le voci seguenti:
    - ***Controlla archivi***: consente di eseguire la scansione del contenuto di archivi possibilmente inclusi nella pagina Web da visualizzare .
    - ***Scansione di programmi potenzialmente indesiderati e minacce di spyware***: consente di eseguire la scansione di programmi potenzialmente indesiderati (*programmi eseguibili che possono funzionare come spyware o adware*) inclusi nella pagina Web da visualizzare, e infezioni spyware.
    - ***Usa analisi euristica***: consente di eseguire la scansione del contenuto

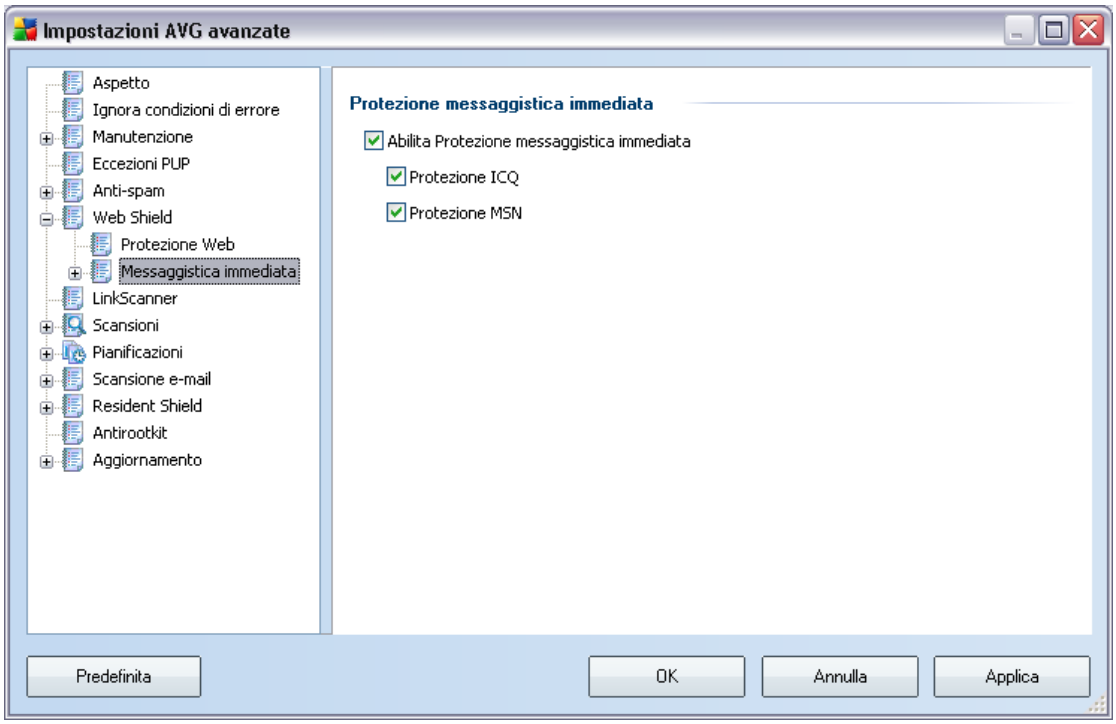
della pagina da visualizzare utilizzando il metodo analisi euristica (*emulazione dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale*).

- ***Porte da scannerizzare*** : questo campo elenca i numeri della porta di comunicazione standard. Se la configurazione del proprio computer è diversa, è possibile cambiare i numeri della porta in base alle esigenze.

- ***Dimensione file massima per scansione***: se i file inclusi sono presenti nella pagina visualizzata, è anche possibile eseguire la scansione del contenuto relativo prima che vengano scaricati nel computer. Tuttavia, la scansione di file di grandi dimensioni richiede parecchio tempo rallentando notevolmente il download della pagina Web. È possibile utilizzare la barra di scorrimento per specificare la dimensione massima di un file che deve ancora essere sottoposto a scansione con ***Web Shield***. Anche se le dimensioni del file scaricato sono superiori a quelle specificate e quindi il file non verrà sottoposto a scansione da Protezione Web, il computer è comunque protetto: se il file fosse infetto, verrebbe rilevato immediatamente da ***Resident Shield***.

- ***Escludi host/IP/dominio***: nel campo è possibile digitare il nome esatto di un server (*host, indirizzo IP, indirizzo IP con maschera o URL*) o un dominio che non deve essere sottoposto a scansione da ***Web Shield***. Pertanto, escludere un host solo se si è assolutamente certi che non fornirà mai contenuti Web pericolosi.

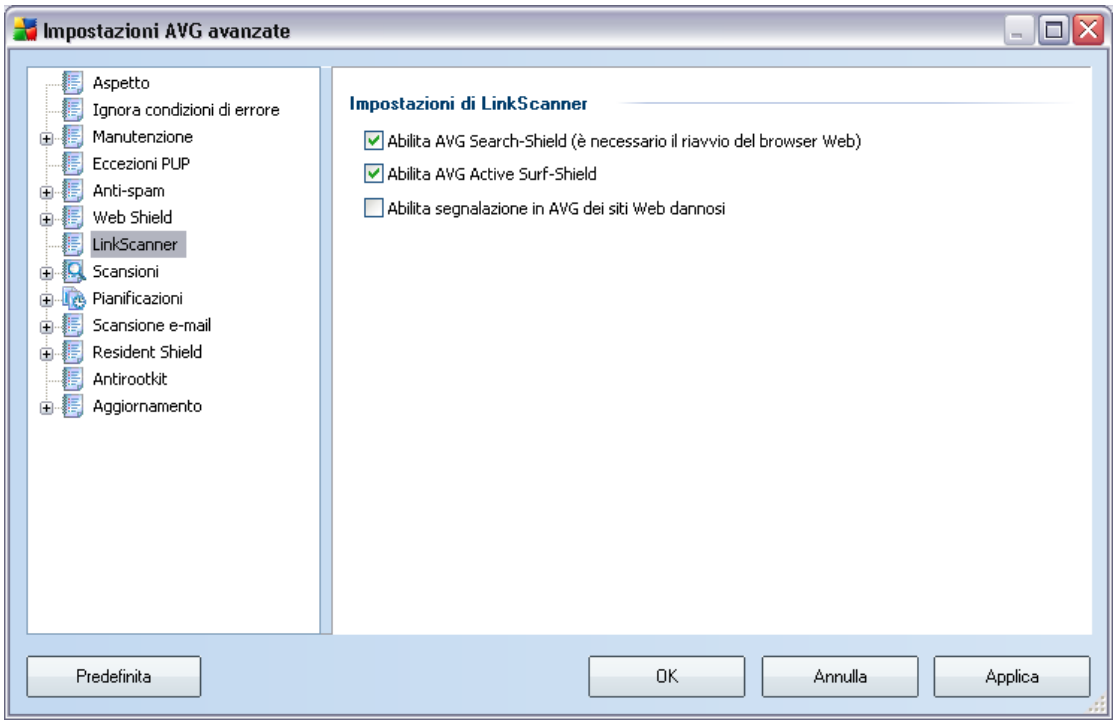
12.6.2.Instant Messaging



Nella finestra di dialogo ***Protezione messaggistica immediata*** è possibile modificare le impostazioni dei componenti di ***Web Shield*** che si riferiscono alla scansione della messaggistica immediata. Attualmente sono supportati tre programmi di messaggistica immediata: ***ICQ***, ***MSN*** e ***Yahoo***. Selezionare la voce corrispondente per ciascuno di essi se si desidera che Web Shield verifichi l'assenza di virus nelle comunicazioni in linea.

Per ulteriori dettagli sugli utenti consentiti/bloccati è possibile visualizzare e modificare la finestra di dialogo corrispondente (***ICQ avanzato***, ***MSN avanzato***) e specificare l'elenco ***Whitelist*** (*l'elenco di utenti che saranno autorizzati a comunicare*) e ***Blacklist*** (*gli utenti che devono essere bloccati*).

12.7.Link Scanner



La finestra di dialogo ***Impostazioni LinkScanner*** consente di attivare/disattivare le due funzionalità di base del componente ***LinkScanner***:

- ***Abilita Safe Search***: (*attivata per impostazione predefinita*) icone informative relative ai siti restituiti da ricerche eseguite in Google, Yahoo o MSN il cui contenuto è stato precedentemente controllato. I browser supportati sono Internet Explorer e Firefox.
- ***Abilita Safe Surf***: (*attivata per impostazione predefinita*) protezione attiva (*in tempo reale*) da siti dannosi al momento dell'accesso. Le connessioni a siti dannosi conosciuti e il loro contenuto vengono bloccati non appena l'utente esegue l'accesso mediante un browser Web (*o qualsiasi altra applicazione che utilizza HTTP*).
- ***Abilita segnalazioni in AVG dei siti Web dannosi*** : (*attivata per impostazione predefinita*): contrassegnare questo elemento in modo da consentire la segnalazione di siti fraudolenti e dannosi trovati dall'utente mediante ***Safe Surf*** o ***Safe Search*** per consentire la raccolta di informazioni nel database in merito ad attività dannose sul Web.

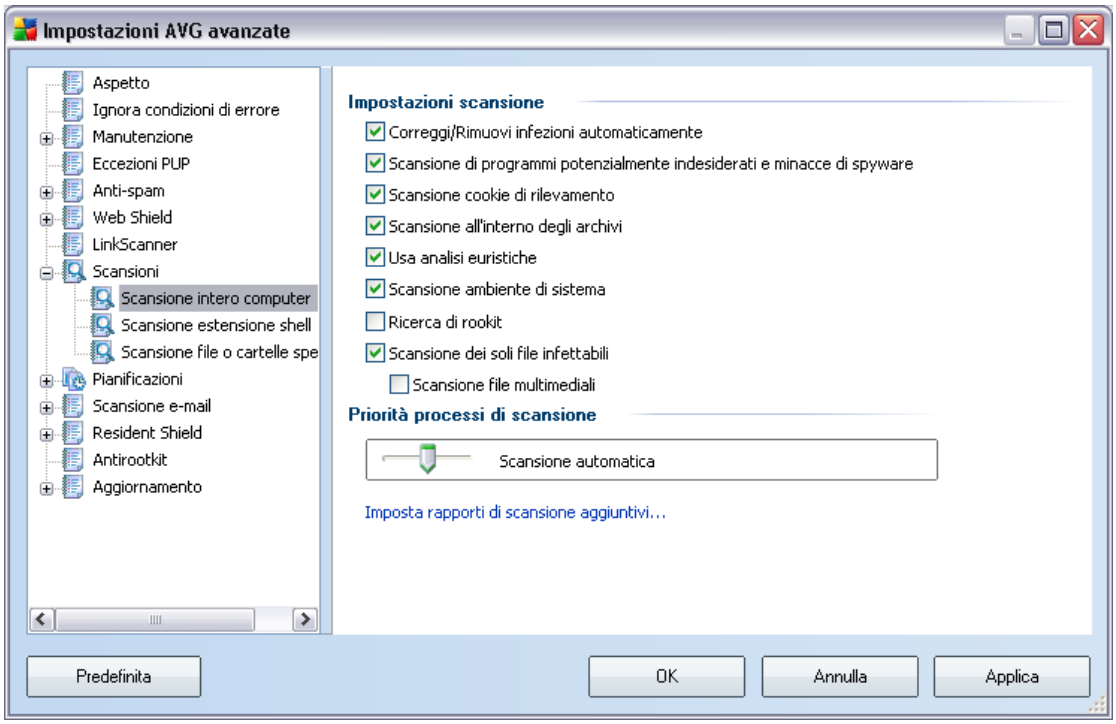
12.8.Scansioni

La sezione delle impostazioni di scansione avanzate è suddivisa in tre categorie che fanno riferimento a specifici tipi di scansione, come quanto definito dal produttore del software:

- ***Scansione intero computer*** : scansione predefinita standard dell'intero computer
- ***Scansione estensione shell*** : scansione specifica di un oggetto selezionato direttamente dall'ambiente Esplora risorse
- ***Scansione file o cartelle specifiche***: scansione predefinita standard di aree selezionate del computer
- ***Scansione dispositivo rimovibile***: scansione specifica di dispositivi rimovibili collegati al computer

12.8.1.Scansione intero computer

L'opzione ***Scansione intero computer*** consente di modificare i parametri di una delle scansioni predefinite dal fornitore di software, ***Scansione intero computer***:



Impostazioni scansione

Nella sezione ***Impostazioni scansione*** è contenuto un elenco di parametri di scansione che possono essere attivati/disattivati a seconda delle necessità:

- ***Correggi/Rimuovi infezioni automaticamente***: se viene identificato un virus durante la scansione può essere corretto automaticamente se è disponibile una soluzione. Se il file infetto non puè essere corretto automaticamente o se si decide di disattivare questa opzione, si riceverà un messaggio di notifica sulla presenza di un virus e si dovrà decidere l'azione da intraprendere sull'infezione rilevata. Il metodo consigliato è spostare il file infetto in Quarantena virus.

- ***Scansione di programmi potenzialmente indesiderati***: questo parametro controlla la funzionalità Anti-Virus che consente il rilevamento di programmi

potenzialmente indesiderati (*file eseguibili che possono essere eseguiti come spyware o adware*) e che possono essere bloccati o rimossi;

- ***Scansione cookie***: questo parametro del componente Anti-Spyware stabilisce che i cookie devono essere rilevati; (*i cookie HTTP vengono utilizzati per autenticare, rilevare e mantenere informazioni specifiche sugli utenti, quali le preferenze dei siti e il contenuto dei carrelli elettronici*)

- ***Scansione all'interno degli archivi***: questo parametro stabilisce che la scansione deve controllare tutti i file anche quelli inclusi all'interno di un archivio, quale ZIP, RAR e così via, ...

- ***Usa analisi euristiche***: l'analisi euristica (*emulazione dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale*) sarà uno dei metodi utilizzati per il rilevamento di virus durante la scansione;

- ***Scansione ambiente di sistema***: la scansione verrà eseguita anche sulle aree di sistema del computer;

- ***Ricerca di rootkit***: selezionare questa voce per includere il rilevamento dei rootkit nella scansione dell'intero computer. Il rilevamento dei rootkit è disponibile anche da solo all'interno del componente ***Anti-Rootkit***;

- ***Scansione dei soli file infettabili***: se l'opzione è attivata, i file non infettabili non verranno sottoposti a scansione. Può trattarsi ad esempio di alcuni file di testo normale o di altri file non eseguibili.

    - ***Scansione file multimediali*** : selezionare questa casella di controllo per eseguire la scansione di file multimediali (video, audio e così via). Se non si seleziona questa casella, il tempo di scansione risulterà ulteriormente ridotto, poiché questi file sono spesso di grandi dimensioni e non sono facilmente infettati da virus.

Priorità processi di scansione

All'interno della sezione ***Priorità processi di scansione*** è inoltre possibile specificare la velocità di scansione desiderata in base all'utilizzo delle risorse di sistema. Per impostazione predefinita, il valore di questa opzione è impostato sul livello medio di utilizzo automatico delle risorse. Se si desidera aumentare la velocità della scansione, il tempo che impiegherà sarà inferiore ma l'utilizzo delle risorse di sistema aumenterà notevolmente durante l'esecuzione e rallenterà le altre attività sul PC (*questa opzione può essere utilizzata quando il computer è acceso ma non è utilizzato*). Tuttavia, è

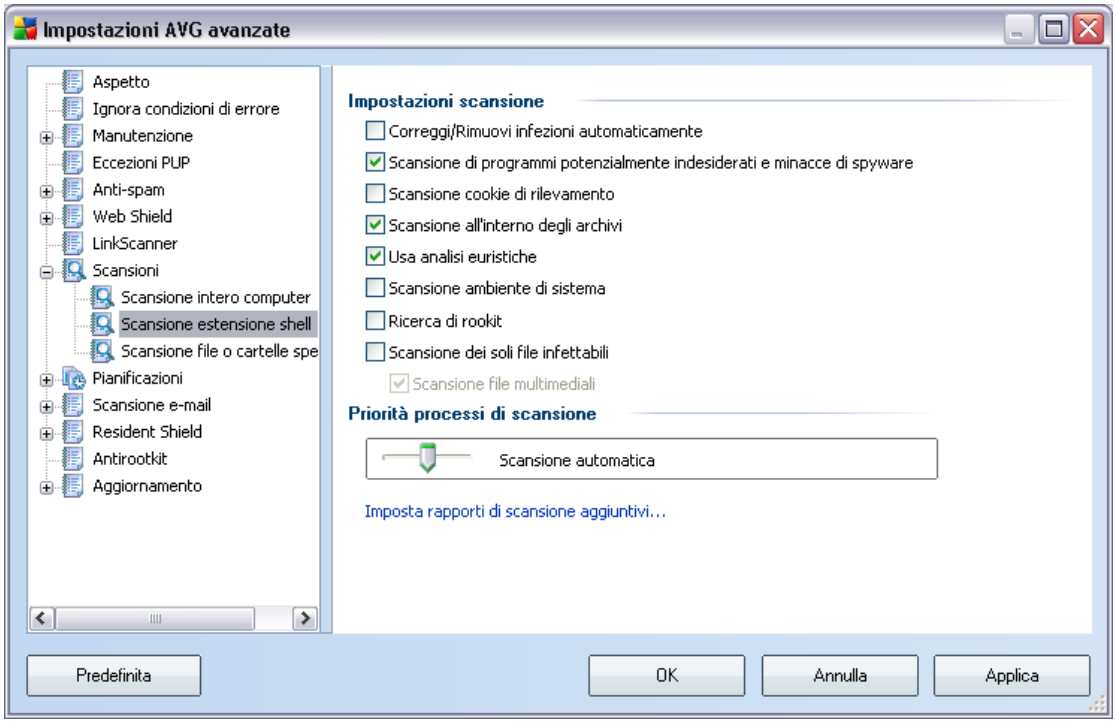
possibile diminuire l'utilizzo delle risorse di sistema aumentando la durata della scansione.

Imposta rapporti di scansione aggiuntivi...

Fare clic sul collegamento ***Imposta rapporti di scansione aggiuntivi...*** per aprire una finestra di dialogo autonoma denominata ***Rapporti di scansione*** in cui è possibile selezionare diversi elementi per definire i tipi di rilevamenti da segnalare:

12.8.2.Scansione estensione shell

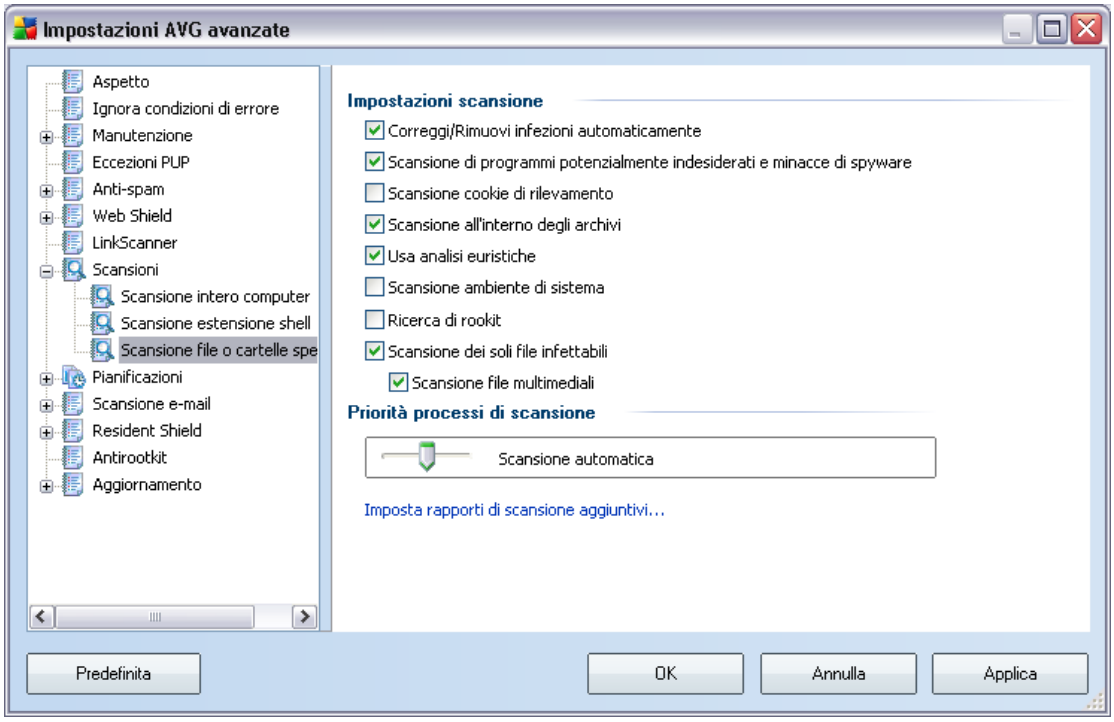
Simile alla voce precedente denominata ***Scansione intero computer*** , ***Scansione estensione shell*** offre anche numerose opzioni per modificare la scansione predefinita dal fornitore di software. In questo caso, la configurazione è relativa alla scansione di oggetti specifici avviati direttamente dall'ambiente Esplora risorse (*estensione shell*), vedere il capitolo***Scansione in Esplora risorse***:



L'elenco dei parametri è identico a quello disponibile per ***Scansione intero computer*** . Tuttavia, le impostazioni predefinite sono diverse: con ***Scansione intero computer*** la maggior parte dei parametri sono selezionati mentre per ***Scansione estensione shell*** (***Scansione in Esplora risorse***) sono attivati solo i parametri pertinenti.

12.8.3.Scansione file o cartelle specifiche

L'interfaccia di modifica di ***Scansione file o cartelle specifiche*** è identica alla finestra di dialogo di modifica ***Scansione intero computer***. Tutte le opzioni di configurazione sono uguali; tuttavia, le impostazioni predefinite sono più restrittive per ***Scansione intero computer***:

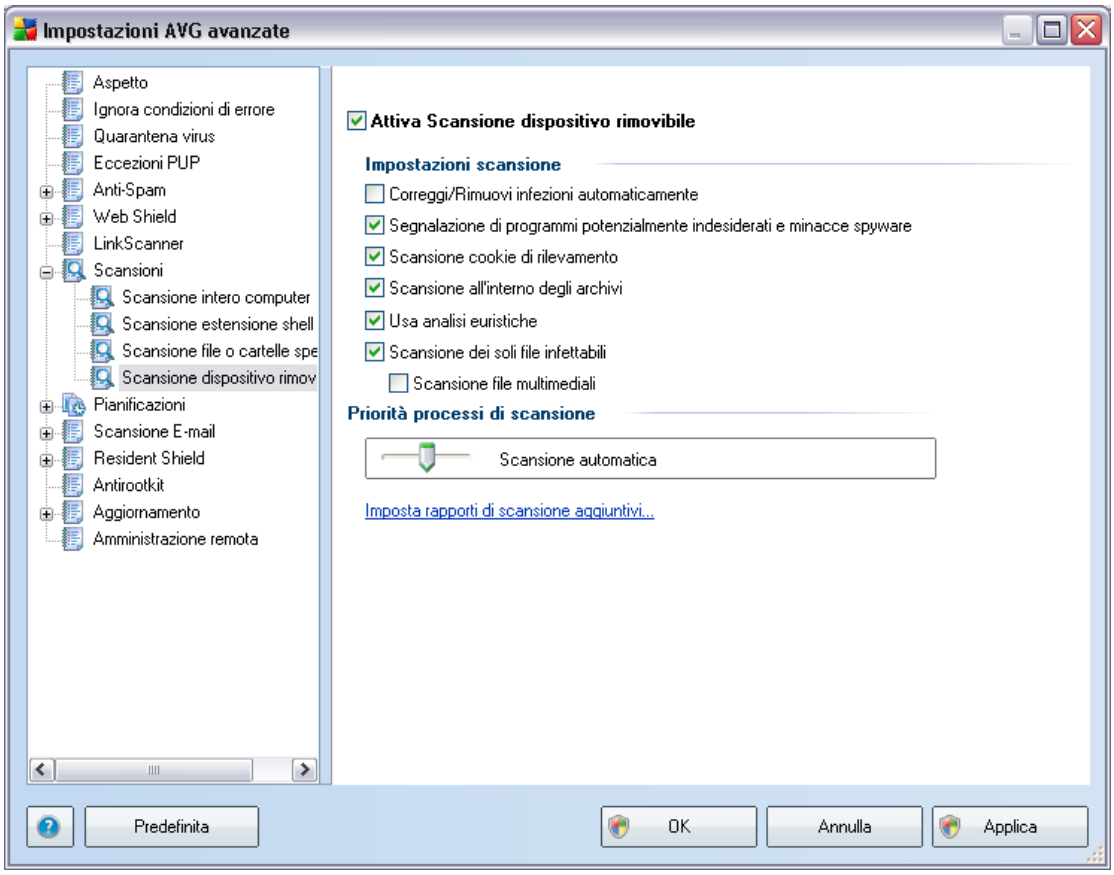


Tutti i parametri impostati in questa finestra di dialogo di configurazione si applicano solo alle aree selezionate per la scansione con il comando ***Scansione file o cartelle specifiche***! Se si seleziona l'opzione ***Ricerca di rootkit*** in questa finestra dialogo di configurazione, verrà eseguito solo un rapido test anti-rootkit, ovvero la ricerca di rootkit verrà eseguita solo nelle aree selezionate.

Nota: *per la descrizione di parametri specifici consultare il capitolo* ***Impostazioni AVG avanzate / Scansione / Scansione intero computer****.*

12.8.4.Scansione dispositivo rimovibile

L'interfaccia di modifica di ***Scansione dispositivo rimovibile*** è inoltre molto simile alla finestra di dialogo di modifica ***Scansione intero computer***:



La ***Scansione dispositivo rimovibile*** viene avviata automaticamente quando viene collegato un dispositivo rimovibile al computer. Per impostazione predefinita, questa scansione è disattivata. Tuttavia, è molto importante effettuare la scansione dei dispositivi rimovibili per verificare la presenza di potenziali minacce poiché tali dispositivi rappresentano una delle fonti di infezione principali. Per avviare automaticamente questo tipo di scansione quando necessario, selezionare l'opzione ***Abilita scansione dispositivo rimovibile***.

Nota: *per la descrizione di parametri specifici consultare il capitolo* ***Impostazioni AVG avanzate / Scansione / Scansione intero computer***.

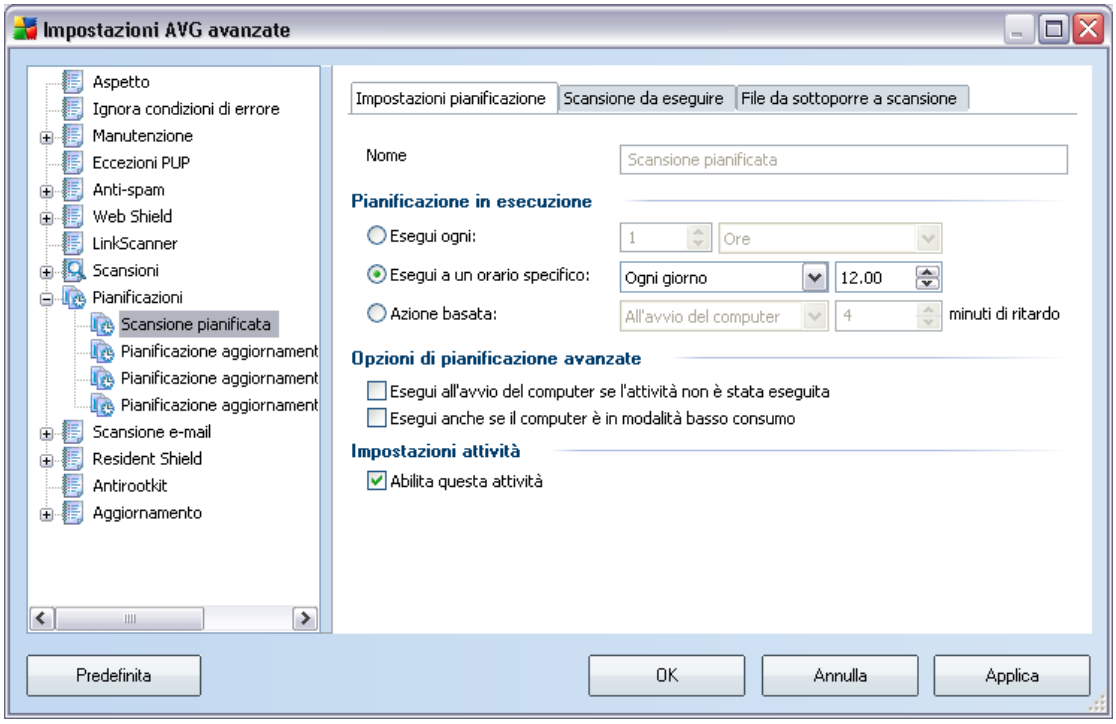
12.9.Pianificazioni

Nella sezione ***Pianificazioni*** è possibile modificare le impostazioni predefinite di:

- Pianificazione scansione intero computer
- Pianificazione aggiornamento del database di virus
- Pianificazione aggiornamento del programma
- Pianificazione aggiornamenti Anti-Spam

12.9.1.Scansione pianificata

È possibile modificare i parametri della scansione pianificata (*o configurare una nuova pianificazione*) in tre schede:



Nella scheda ***Impostazioni attività*** è possibile selezionare/deselezionare la voce ***Abilita questa attività*** per disattivare temporaneamente il controllo pianificato e riattivarlo secondo le necessità.

Quindi, assegnare un nome alla scansione da creare e pianificare. Digitare il nome nel campo di testo dalla voce ***Nome***. Provare a denominare le scansioni assegnando nomi brevi, descrittivi e appropriati per poterle riconoscere più facilmente in futuro.

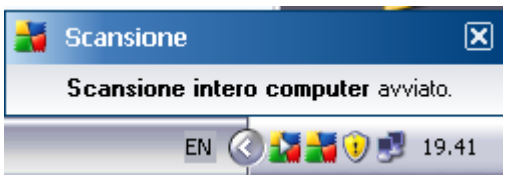
Esempio: *non è appropriato denominare una scansione "Nuova scansione" o "Scansione personale" poiché questi nomi non fanno riferimento agli elementi sottoposti a scansione. Un esempio di un buon nome descrittivo potrebbe essere "Scansione aree di sistema" e così via. Inoltre, non è necessario specificare nel nome della scansione se si tratta di una scansione dell'intero computer oppure relativa solo ai file o alle cartelle selezionati. Le scansioni saranno sempre una versione specifica della scansione dei file e delle cartelle sellezionati.*

In questa finestra di dialogo è possibile definire ulteriormente i seguenti parametri della scansione:

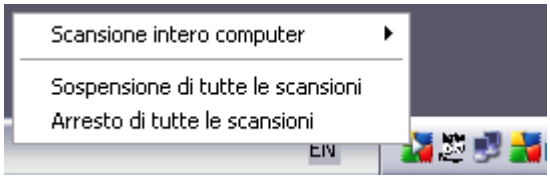
- ***Pianificazione in esecuzione***: consente di specificare gli intervalli di tempo per l'avvio della nuova scansione pianificata. È possibile definire l'ora dall'avvio ripetuto della scansione dopo un certo periodo di tempo (***Esegui ogni...***) o definendo data e ora esatte (***Esegui a un orario specifico...***) oppure definendo un evento a cui dovrà essere associato l'avvio della scansione (***Azione in base all'avvio del computer***).

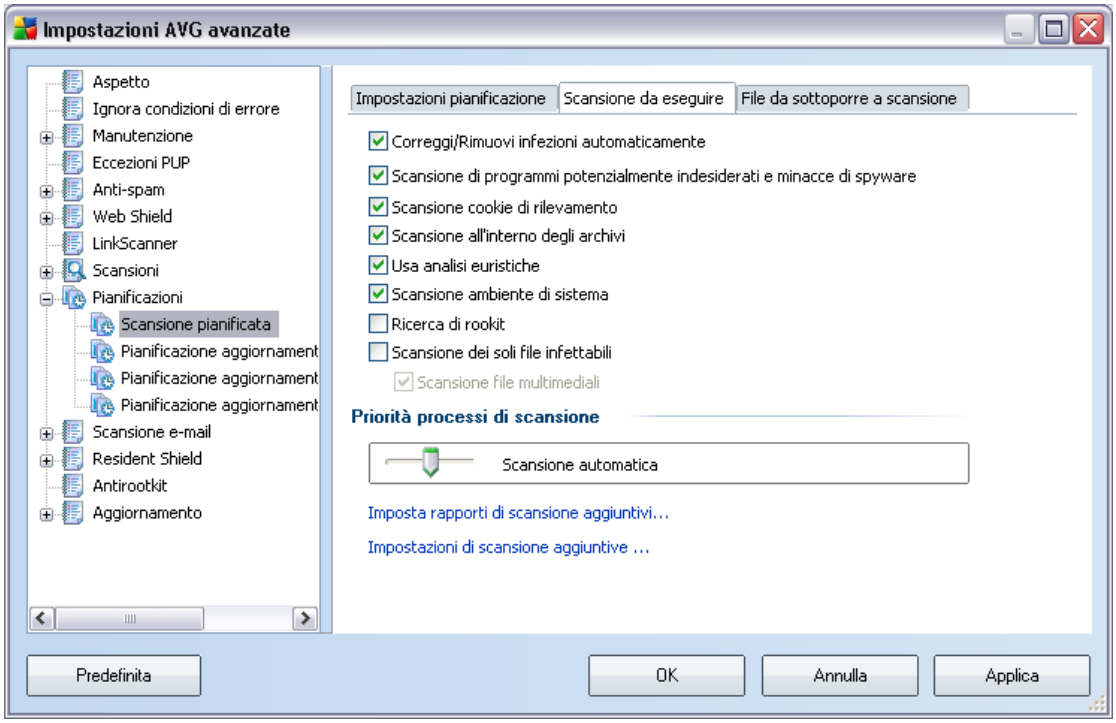
- ***Opzioni di pianificazione avanzate***: questa sezione consente di definire le circostanze in cui deve essere avviata o non avviata la scansione se il computer si trova in modalità basso consumo oppure se è completamente spento.

Quando la scansione pianificata viene avviata in corrispondenza dell'ora specificata, l'utente ne viene informato tramite una finestra a comparsa visualizzata sopra l'icona di AVG presente nella barra delle applicazioni:



Viene quindi visualizzata una nuova icona AVG nella barra delle applicazioni (*completamente colorata e con una freccia bianca, vedere la figura in alto*) per comunicare che è in corso una scansione pianificata. Fare clic con il pulsante destro del mouse sull'icona AVG relativa alla scansione in corso per aprire un menu contestuale in cui è possibile decidere se sospendere o persino arrestare la scansione:





Nella scheda ***Scansione da eseguire*** è presente un elenco di parametri che possono essere attivati o disattivati facoltativamente. Per impostazione predefinita, la maggior parte dei parametri è attivata e la funzionalità verrà applicata durante la scansione. A meno che ci sia una ragione valida per modificare le impostazioni, si consiglia di mantenere la configurazione predefinita:

- ***Correggi/Rimuovi infezioni automaticamente*** : (*attivata per impostazione predefinita*) se viene identificato un virus durante la scansione, può essere corretto automaticamente, se è disponibile una soluzione. Se il file infetto non può essere corretto automaticamente o se si decide di disattivare questa opzione, si riceverà un messaggio di notifica sulla presenza di un virus e si dovrà decidere l'azione da intraprendere sull'infezione rilevata. L'azione consigliata è quella di rimuovere il file infetto in Quarantena virus.

- ***Scansione di programmi potenzialmente indesiderati*** : (*attivata per impostazione predefinita*): questo parametro controlla la funzionalità Antivirus che consente il rilevamento di programmi potenzialmente indesiderati (*file eseguibili che possono essere eseguiti come spyware o adware*) e che possono essere bloccati o rimossi;

- ***Scansione cookie***: (*attivata per impostazione predefinita*): questo parametro del componente Anti-Spyware stabilisce che i cookie devono essere rilevati durante la scansione ; (*i cookie HTTP vengono utilizzati per autenticare, rilevare e mantenere informazioni specifiche sugli utenti, quali le preferenze dei siti i il contenuto dei carrelli elettronici*)

- ***Scansione all'interno degli archivi***: (*attivata per impostazione predefinita*): questo parametro stabilisce che la scansione deve controllare tutti i file anche se inclusi all'interno di un tipo di archivio, quale ZIP, RAR e così via.

- ***Usa analisi euristiche*** : (*attivata per impostazione predefinita*): analisi euristica (*emulazione dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale*) che sarà uno dei metodi utilizzati per il rilevamento di virus durante la scansione;

- ***Scansione ambiente di sistema*** : (*attivata per impostazione predefinita*): la scansione verrà eseguita anche sulle aree di sistema del computer;

- ***Ricerca di rootkit***: selezionare questa voce per includere il rilevamento dei rootkit nella scansione dell'intero computer. Il rilevamento dei rootkit è disponibile anche da solo all'interno del componente ***Anti-Rootkit***;

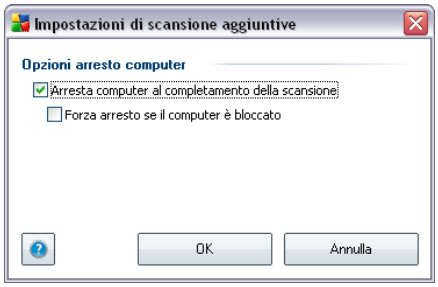
- ***Scansione dei soli file infettabili*** : (*disattivata per impostazione predefinita*): se l'opzione è attivata, la scansione non verrà applicata ai file che non possono essere infettabili. Può trattarsi ad esempio di alcuni file di testo normale o di altri file non eseguibili.

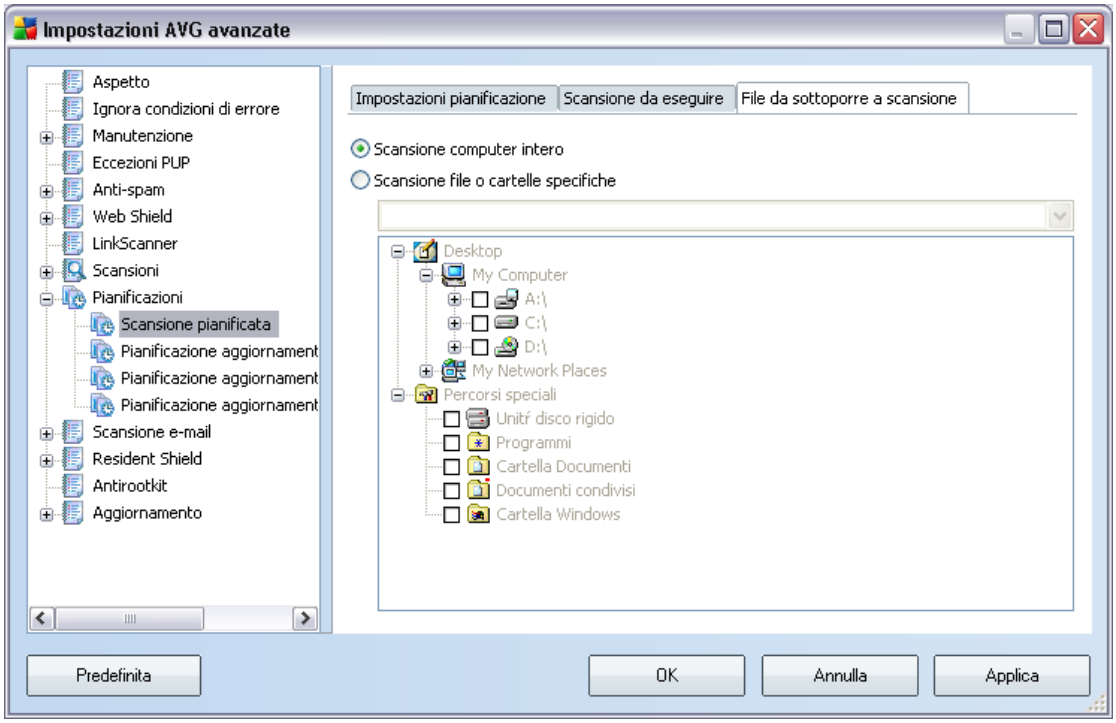
All'interno della sezione ***Priorità processi di scansione*** è inoltre possibile specificare la velocità di scansione desiderata in base all'utilizzo delle risorse di sistema. Per impostazione predefinita, questa opzione è impostata sul livello medio di utilizzo automatico delle risorse. Se si desidera aumentare la velocità della scansione, il tempo che impiegherà sarà inferiore ma l'utilizzo delle risorse di sistema aumenterà notevolmente durante l'esecuzione e rallenterà le altre attività sul PC (*questa opzione può essere utilizzata quando il computer è acceso ma non è utilizzato*). Tuttavia, è possibile diminuire l'utilizzo delle risorse di sistema aumentando la durata della scansione.

Fare clic sul collegamento ***Imposta rapporti di scansione aggiuntivi...*** per aprire una finestra di dialogo autonoma denominata ***Rapporti di scansione*** in cui è

possibile selezionare diversi elementi per definire i tipi di rilevamenti da segnalare:

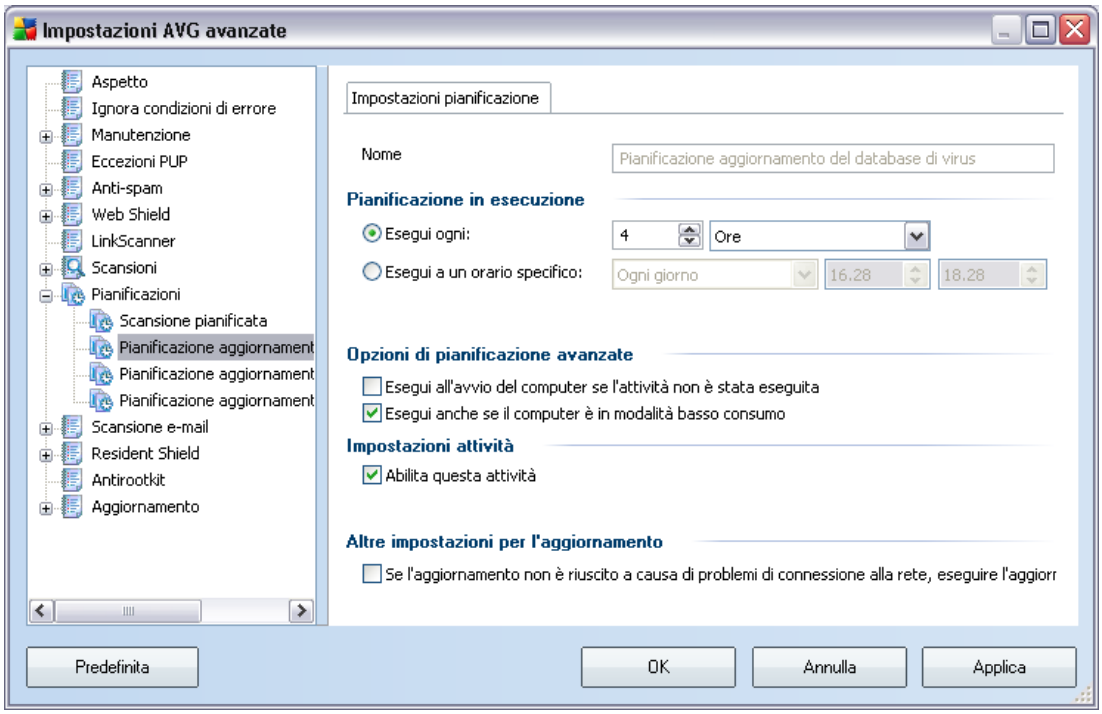
Fare clic su ***Impostazioni di scansione aggiuntive...*** per aprire una nuova finestra di dialogo ***Opzioni arresto computer*** in cui è possibile decidere se il computer deve essere arestato in modo automatico al termine del processo di scansione. Dopo aver confermato questa opzione (***Arresta computer al completamento della scansione***), viene attivata una nuova opzione che consente l'arresto del computer anche se è correntemente bloccato (***Forza arresto se il computer è bloccato***).





Nella scheda ***File da sottoporre a scansione*** è possibile definire se si desidera pianificare la scansione dell'intero computer o la scansione di file o cartelle specifiche. Se si seleziona la scansione di file o cartelle specifiche, nella parte inferiore di questa finestra di dialogo viene attivata la struttura visualizzata che consente di specificare le cartelle da sottoporre a scansione.

12.9.2.Pianificazione dell'aggiornamento dei database dei virus



Nella scheda ***Impostazioni attività*** è possibile selezionare/deselezionare la voce ***Abilita questa attività*** per disattivare temporaneamente l'aggiornamento del database dei virus pianificato e riattivarlo secondo le necessità.

La pianificazione dell'aggiornamento di base del database di virus viene eseguita all'interno del componente ***Aggiornamenti***. Da questa finestra di dialogo è possibile impostare alcuni parametri dettagliati della pianificazione dell'aggiornamento del database di virus:

Assegnare un nome alla pianificazione dell'aggiornamento del database dei virus da creare. Digitare il nome nel campo di testo dalla voce ***Nome***. Provare a denominare le pianificazioni degli aggiornamenti assegnando nomi brevi, descrittivi e appropriati per poterle riconoscere più facilmente in futuro.

- ***Pianificazione in esecuzione***: consente di specificare gli intervalli di tempo per l'avvio del nuovo aggiornamento del database di virus pianificato. È possibile definire l'ora dall'avvio ripetuto dell'aggiornamento dopo un certo periodo di tempo (***Esegui ogni ...***) o definendo data e ora esatte (***Esegui a un orario specifico ...***) oppure definendo un evento a cui dovrà essere associato l'avvio dell'aggiornamento (***Azione in base all'avvio del***

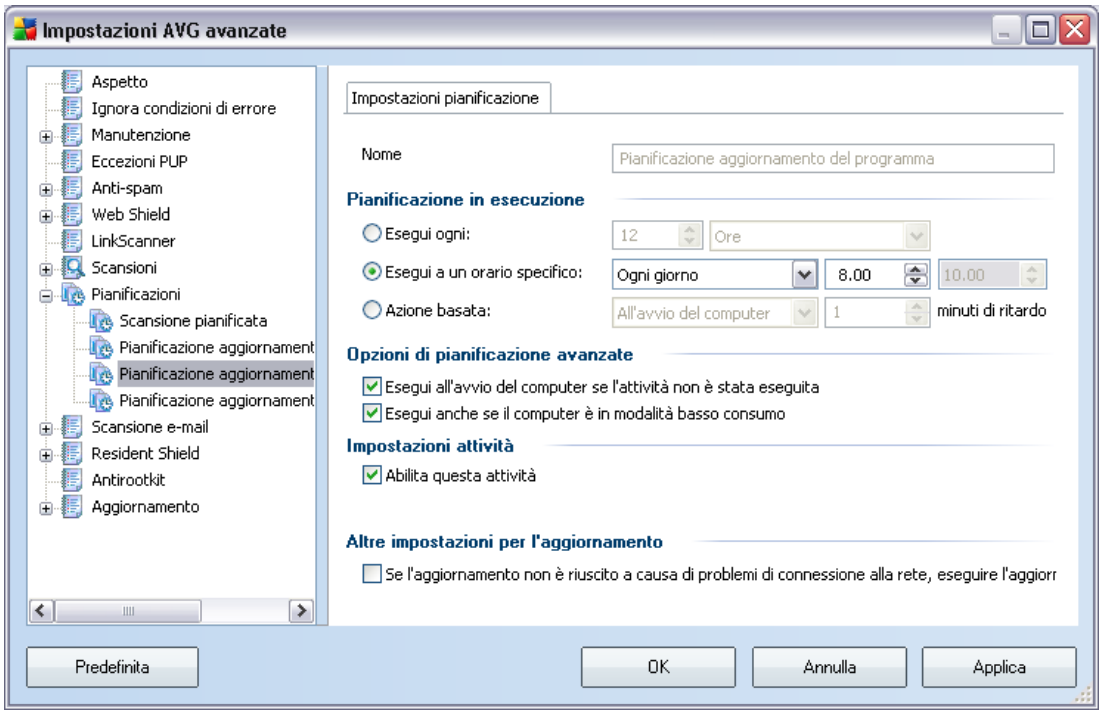
computer).

- ***Opzioni di pianificazione avanzate***: questa sezione consente di definire le circostanze in cui deve o non deve essere avviato l'aggiornamento del database di virus se il computer si trova in modalità basso consumo oppure se è completamente spento.

- ***Altre impostazioni per l'aggiornamento***: selezionare questa opzione per assicurarsi che, se la connessione a Internet viene danneggiata e il processo di aggiornamento ha esito negativo, l'aggiornamento verrà riavviato immediatamente dopo il ripristino della connessione a Internet.

Quando la scansione pianificata viene avviata in corrispondenza dell'ora specificata, l'utente ne viene informato tramite una finestra a comparsa visualizzata sopra l'icona di AVG presente nella barra delle applicazioni (*a condizione che sia stata mantenuta la configurazione predefinita della finestra di dialogo* ***Impostazioni avanzate/ Aspetto***).

12.9.3.Pianificazione dell'aggiornamento del programma



Nella scheda ***Impostazioni attività*** è possibile selezionare/deselezionare la voce ***Abilita questa attività*** per disattivare temporaneamente l'aggiornamento del

programma pianificato e riattivarlo secondo le necessità.

Quindi, assegnare un nome alla pianificazione dell'aggiornamento del programma da creare. Digitare il nome nel campo di testo dalla voce ***Nome***. Provare a denominare le pianificazioni degli aggiornamenti assegnando nomi brevi, descrittivi e appropriati per poterle riconoscere più facilmente in futuro.

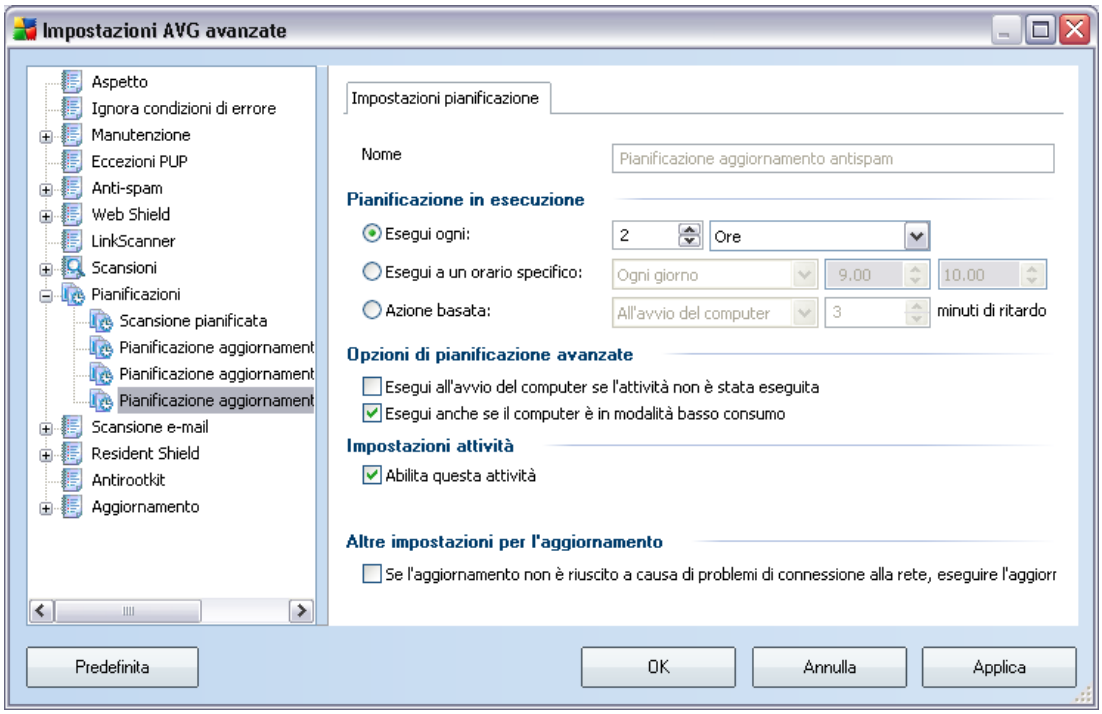
- ***Pianificazione in esecuzione***: consente di specificare gli intervalli di tempo per l'avvio del nuovo aggiornamento del programma pianificato. È possibile definire l'ora dall'avvio ripetuto dell'aggiornamento dopo un certo periodo di tempo (***Esegui ogni ...***) o definendo data e ora esatte (***Esegui a un orario specifico ...***) oppure definendo un evento a cui dovrà essere associato l'avvio dell'aggiornamento (***Azione in base all'avvio del computer***).

- ***Opzioni di pianificazione avanzate***: questa sezione consente di definire le circostanze in cui deve o non deve essere avviato l'aggiornamento del programma se il computer si trova in modalità basso consumo oppure se è completamente spento.

- ***Altre impostazioni per l'aggiornamento***: selezionare questa opzione per assicurarsi che, se la connessione a Internet viene danneggiata e il processo di aggiornamento ha esito negativo, l'aggiornamento verrà riavviato immediatamente dopo il ripristino della connessione a Internet.

Quando la scansione pianificata viene avviata in corrispondenza dell'ora specificata, l'utente ne viene informato tramite una finestra a comparsa visualizzata sopra l'icona di AVG presente nella barra delle applicazioni (*a condizione che sia stata mantenuta la configurazione predefinita della finestra di dialogo* ***Impostazioni avanzate/ Aspetto***).

12.9.4.Pianificazione aggiornamenti Anti-Spam



Nella scheda ***Impostazioni attività*** è possibile selezionare/deselezionare la voce ***Abilita questa attività*** per disattivare temporaneamente l'aggiornamento ***Anti-Spam*** pianificato e riattivarlo secondo le necessità.

La pianificazione dell'aggiornamento ***Anti-Spam*** di base è gestita dal componente ***Aggiornamenti***. Da questa finestra di dialogo è possibile impostare alcuni parametri dettagliati della pianificazione dell'aggiornamento:

Quindi, assegnare un nome alla pianificazione dell'aggiornamento ***Anti-Spam*** da creare. Digitare il nome nel campo di testo dalla voce ***Nome***. Provare a denominare le pianificazioni degli aggiornamenti assegnando nomi brevi, descrittivi e appropriati per poterle riconoscere più facilmente in futuro.

- ***Pianificazione in esecuzione***: consente di specificare gli intervalli di tempo per l'avvio dell'aggiornamento ***Anti-Spam*** che è stato pianificato. È possibile definire l'ora dall'avvio ripetuto dell'aggiornamento ***Anti-Spam*** dopo un certo periodo di tempo (***Esegui ogni ...***) o definendo data e ora esatte (***Esegui a un orario specifico ...***) oppure definendo un evento a cui dovrà essere associato l'avvio dell'aggiornamento (***Azione in base all'avvio del computer***).

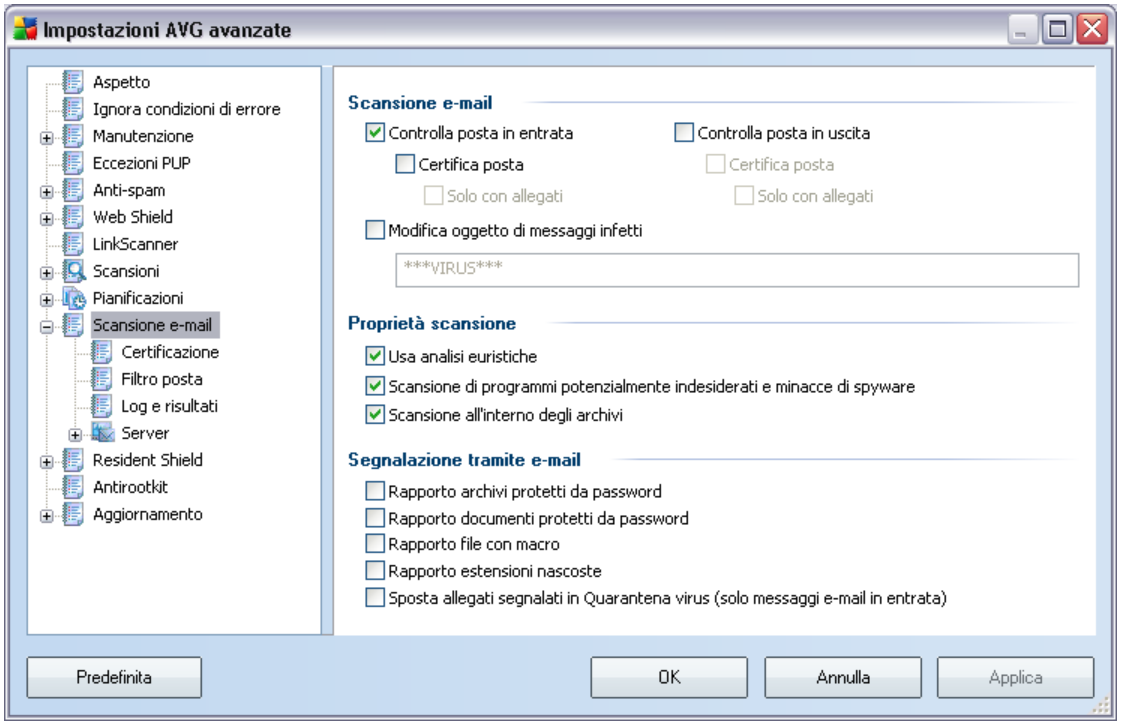
- ***Opzioni pianificazione avanzata***: questa sezione consente di definire le circostanze in cui deve essere avviato o non avviato l'aggiornamento ***Anti-Spam*** se il computer si trova in modalità basso consumo oppure se è completamente spento.

- ***Impostazioni attività***: in questa sezione è possibile deselezionare la voce ***Abilita questa attività*** per disattivare temporaneamente l'aggiornamento ***Anti-Spam*** pianificato e riattivarlo secondo le necessità.

- ***Altre impostazioni per l'aggiornamento***: selezionare questa opzione per assicurarsi che, se la connessione a Internet viene danneggiata e il processo di aggiornamento ***Anti-Spam*** ha esito negativo, l'aggiornamento verrà riavviato immediatamente dopo il ripristino della connessione a Internet.

Quando la scansione pianificata viene avviata in corrispondenza dell'ora specificata, l'utente ne viene informato tramite una finestra a comparsa visualizzata sopra l'icona di AVG presente nella barra delle applicazioni (*a condizione che sia stata mantenuta la configurazione predefinita della finestra di dialogo* ***Impostazioni avanzate/ Aspetto***).

12.1. Scansione e-mail



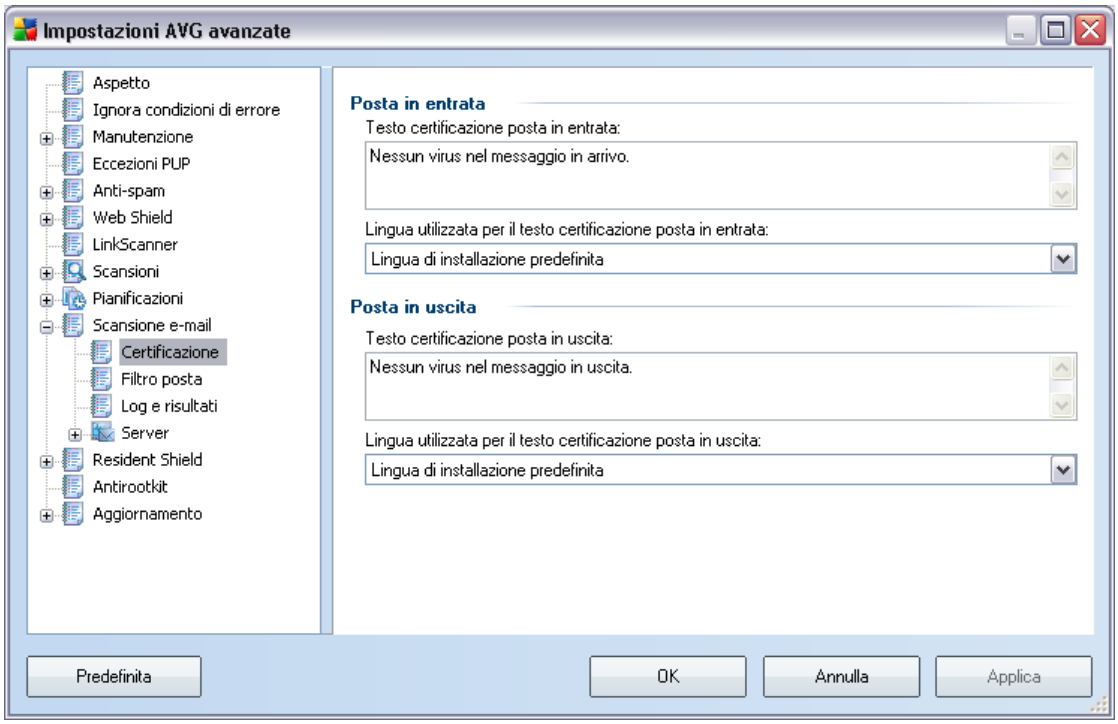
La finestra di dialogo ***Scansione e-mail*** è suddivisa in tre sezioni:

- ***Scansione e-mail***: in questa sezione selezionare se si desidera eseguire la scansione dei messaggi di posta in entrata e in uscita e se tutti i messaggi di posta devono essere certificati o solo in caso di messaggi con allegati (*la certificazione dei messaggi privi di virus non è supportata nel formato HTML/ RTF*). Inoltre, è possibile scegliere che venga modificato l'oggetto dei messaggi che contengono potenziali virus. Selezionare la casella di controllo ***Modifica oggetto di messaggi infetti*** e modificare il testo di conseguenza (*il valore predefinito è* ***).

- ***Proprietà scansione***: specifica se il metodo analisi euristica deve essere utilizzato durante la scansione (***Utilizza analisi euristica***), se si desidera controllare la presenza di programmi potenzialmente indesiderati (***Scansione di programmi potenzialmente indesiderati***) e se è necessario sottoporre a scansione anche gli archivi (***Scansione all'interno degli archivi***).

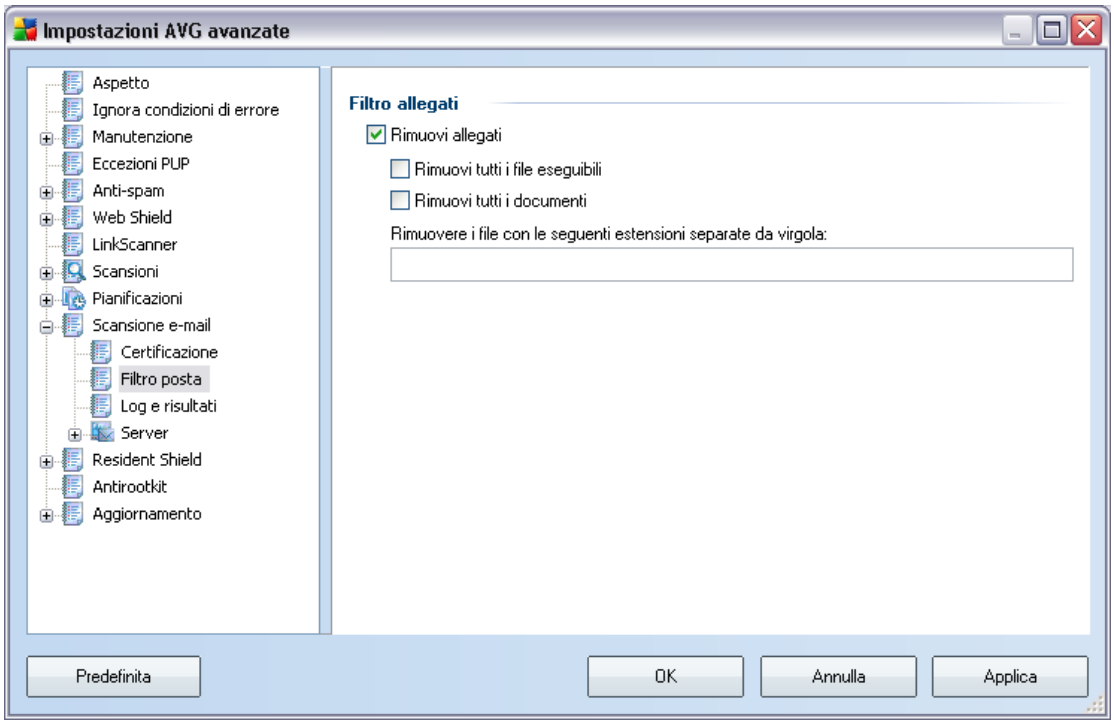
- ***Segnalazione tramite e-mail***: specifica se si desidera ricevere una notifica via e-mail per gli archivi protetti da password, i documenti protetti da password, le macro contenenti file e/o i file con estensione nascosta rilevati come allegato del messaggio e-mail sottoposto a scansione. Se viene identificato un messaggio simile durante la scansione, è possibile stabilire se l'oggetto infetto rilevato deve essere spostato in ***Quarantena virus***.

12.10. Certificazione



Nella finestra di dialogo ***Certificazione*** è possibile specificare con precisione il testo che deve essere contenuto nella nota della certificazione nonché la lingua del testo. È necessario specificare le informazioni separatamente per ***Posta in entrata*** e ***Posta in uscita***.

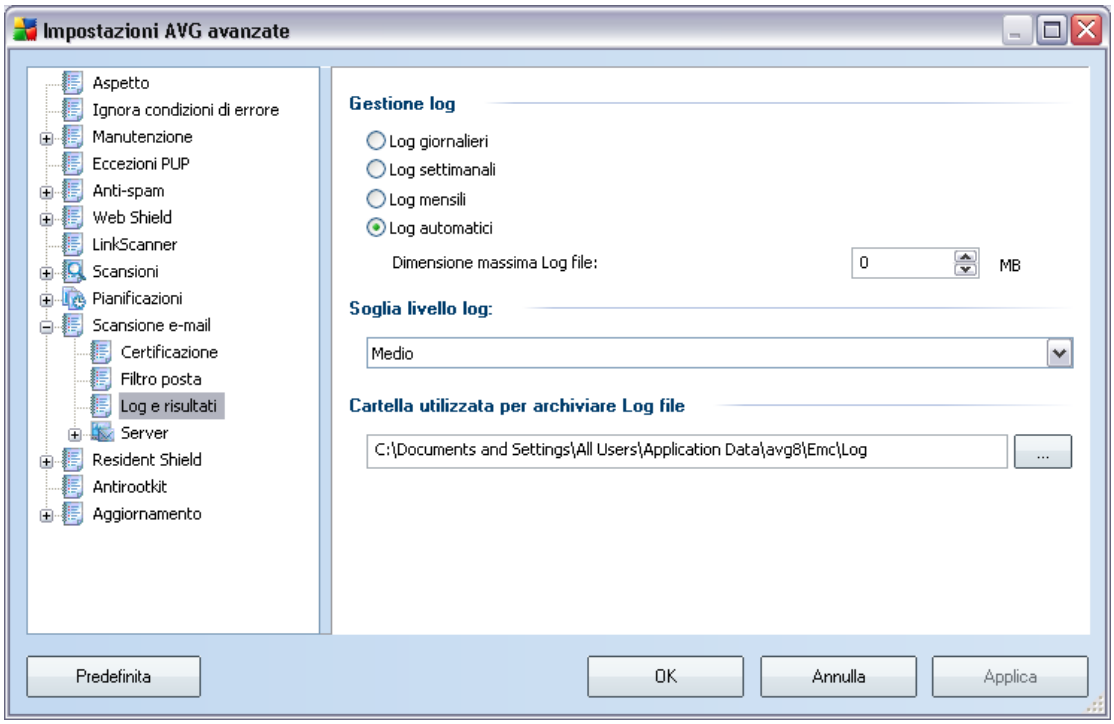
12.10. Filtro posta



La finestra di dialogo ***Filtro allegati*** consente di impostare i parametri per la scansione degli allegati dei messaggi e-mail. Per impostazione predefinita, l'opzione ***Rimuovi allegati*** è disattivata. Se si decide di attivarla, tutti gli allegati dei messaggi e-mail rilevati come infetti o potenzialmente pericolosi verranno rimossi automaticamente. Se si desidera definire tipi specifici di allegati che devono essere rimossi, selezionare l'opzione corrispondente:

- ***Rimuovi tutti i file eseguibili***: tutti i file *.exe verranno eliminati
- ***Rimuovi tutti i documenti***: tutti i file *.doc verranno eliminati
- ***Rimuovi file con estensioni***: verranno rimossi tutti i file con le estensioni specificate

12.10.3 Log e risultati

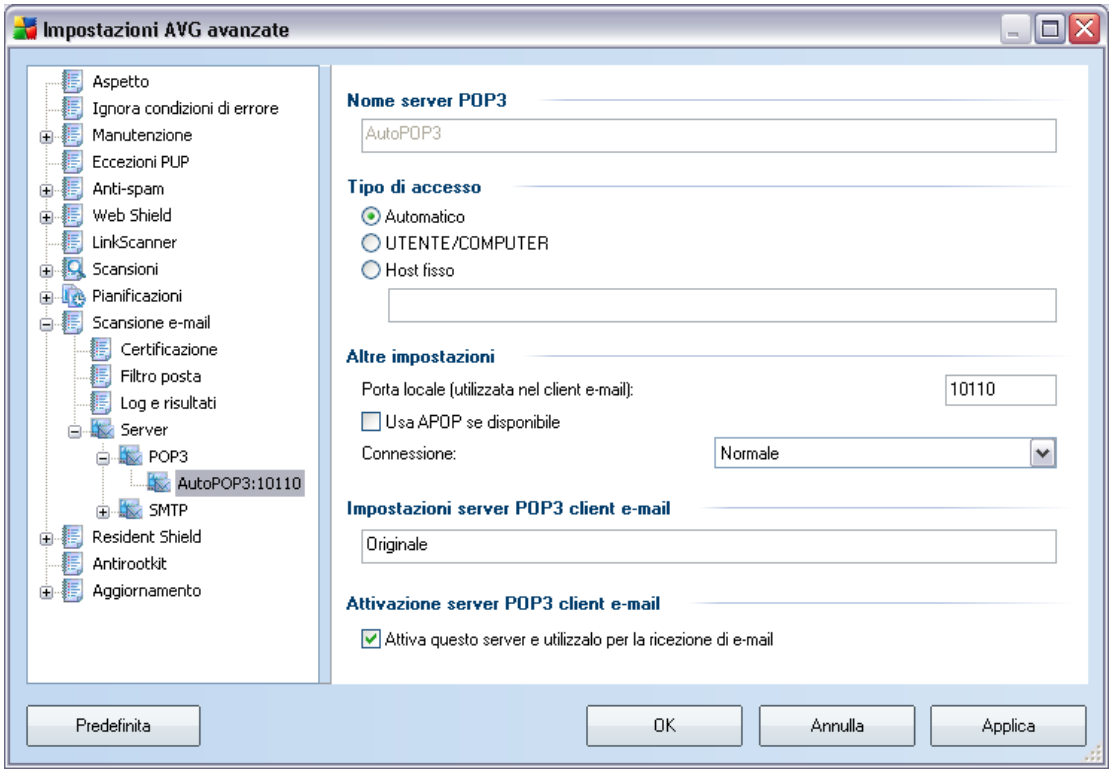


La finestra di dialogo aperta dall'elemento di spostamento ***Log e risultati*** consente di specificare i parametri per la gestione dei risultati di scansione e-mail. La finestra di dialogo è suddivisa in diverse sezioni:

- ***Gestione log***: consente di definire se si desidera registrare le informazioni della scansione dei messaggi e-mail ogni giorno, settimana, mese e così via; consente inoltre di specificare la dimensione massima del Log file in MB
- ***Soglia livello log***: il livello medio è definito per impostazione predefinita. È possibile selezionare un livello inferiore (*registrazione delle informazioni di connessione di base*) o un livello superiore (*registrazione di tutto il traffico*)
- ***Cartella utilizzata per archiviare i Log file***: consente di specificare la posizione per i Log file

12.10.4 Server

Nella sezione ***Server*** è possibile modificare i parametri dei server del componente ***Scansione E-mail*** oppure configurare un nuovo server utilizzando il pulsante ***Aggiungi nuovo server***.



Questa finestra di dialogo (che si apre da ***Server / POP3***) consente di impostare un nuovo server di ***Scansione E-mail*** utilizzando il protocollo POP3 per la posta in entrata:

- ***Nome server POP3***: inserire il nome del server o mantenere il nome AutoPOP3 predefinito
- ***Tipo di accesso***: definisce il metodo per determinare il server e-mail utilizzato per la posta in entrata:
    - Automatico: l'accesso verrà effettuato auotmaticamente in base alle impostazioni del client e-mail.
    - UTENTE/COMPUTER: il metodo più semplice e più utilizzato per determinare il server di posta di destinazione è costituito dal metodo proxy. A questo scopo, specificare il nome, l'indirizzo o la porta come parte del nome utente di accesso per il server di posta specifico, utilizzando come separatore il carattere /. Ad esempio, per l'account

utente1 sul server pop.acme.com e sulla porta 8200, il nome di accesso utilizzato sarebbe utente1/pop.acme.com:8200.

- Host fisso: in questo caso il programma utilizzerà sempre il server specificato. Specificare l'indirizzo o il nome del server di posta. Il nome di accesso non verrà modificato. Per il nome, è possibile utilizzare un nome di dominio (ad esempio pop.acme.com) o un indirizzo IP (ad esempio 123.45.67.89). Se il server di posta utilizza una porta non standard, è possibile specificare il nome della porta dopo quello del server utilizzando come separatore il segno di due punti, ad esempio pop.acme.com:8200. La porta standard per la comunicazione POP3 è la numero 110.

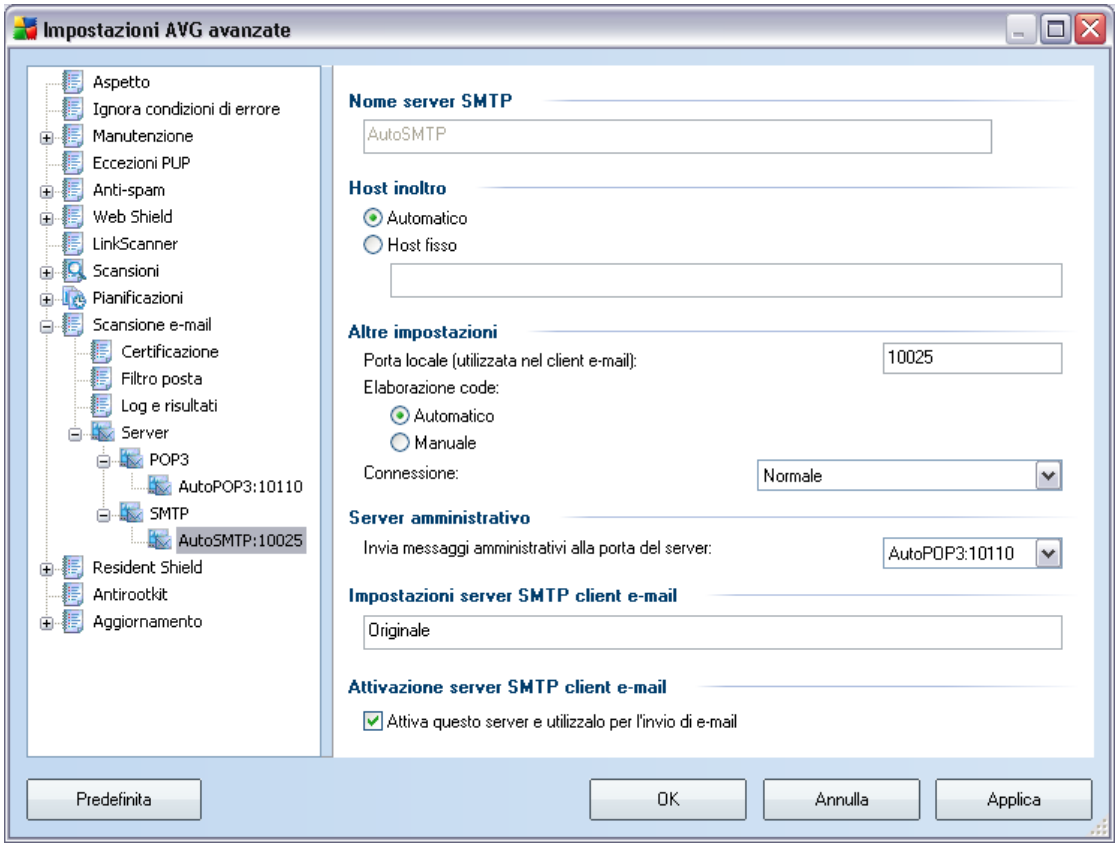
- ***Altre impostazioni***: specifica parametri più dettagliati:

  - Porta locale: specifica la porta su cui è prevista la comunicazione dall'applicazione di posta. Nell'applicazione di posta sarà quindi necessario specificare tale porta come porta per la comunicazione POP3.

  - Usa APOP se disponibile: questa opzione fornisce un accesso più protetto al server di posta. In questo modo ***Scansione e-mail*** utilizzerà un metodo alternativo per inoltrare la password di accesso dell'account utente, inviandola al server in formato crittografato utilizzando una catena di variabili ricevuta dal server. Naturalmente questa funzionalità è disponibile solo se supportata dal server di posta di destinazione.

  - Connessione: dal menu a discesa è possibile specificare il tipo di connessione da utilizzare (regolare/SSL/SSL predefinito). Se si sceglie la connessione SSL, i dati inviati verranno crittografati senza il rischio di essere rilevati o monitorati da terze parti. Questa funzionalità è disponibile solo se supportata dal server di posta di destinazione.

- ***Attivazione server POP3 client e-mail***: fornisce brevi informazioni sulle impostazioni di configurazione richieste per configurare correttamente il client e-mail (in modo tale che ***Scansione e-mail*** controlli tutta la posta in entrata). Si tratta di un riepilogo basato sui parametri corrispondenti specificati nella finestra di dialogo e in altre finestre correlate.



Questa finestra di dialogo (che si apre da ***Server / SMTP***) consente di impostare un nuovo server ***Scansione E-mail*** utilizzando il protocollo SMTP per la posta in uscita:

- ***Nome server SMTP***: digitare il nome del server o mantenere il nome predefinito AutoSMTP
- ***Host di inoltro*** : definisce il metodo per determinare il server di posta utilizzato per la posta in uscita:
  - Automatico: l'accesso verrà effettuato automaticamente, in base alle impostazioni del client e-mail.
  - Host fisso: in questo caso verrà sempre utilizzato il server specificato in questo campo. Specificare l'indirizzo o il nome del server di posta. Per il nome, è possibile utilizzare un nome di dominio (ad esempio smtp. acme.com) o un indirizzo IP (ad esempio 123.45.67.89). Se il server di

posta utilizza una porta non standard, è possibile digitare il nome della porta dopo quello del server utilizzando come separatore il segno di due punti, ad esempio smtp.acme.com:8200. La porta standard per la comunicazione SMTP è la numero 25.

- ***Altre impostazioni***: specifica parametri più dettagliati:

o Porta locale: specifica la porta su cui è prevista la comunicazione dall'applicazione di posta. Nell'applicazione di posta sarà quindi necessario specificare tale porta come porta per la comunicazione SMTP.

o Elaborazione code: determina il comportamento di ***Scansione e-mail*** durante l'elaborazione dei requisiti per l'invio di messaggi di posta:

➢ Automatico: la posta in uscita viene recapitata immediatamente al server di posta di destinazione.

➢ Manuale: il messaggio viene inserito nella coda di messaggi in uscita e inviato in seguito.

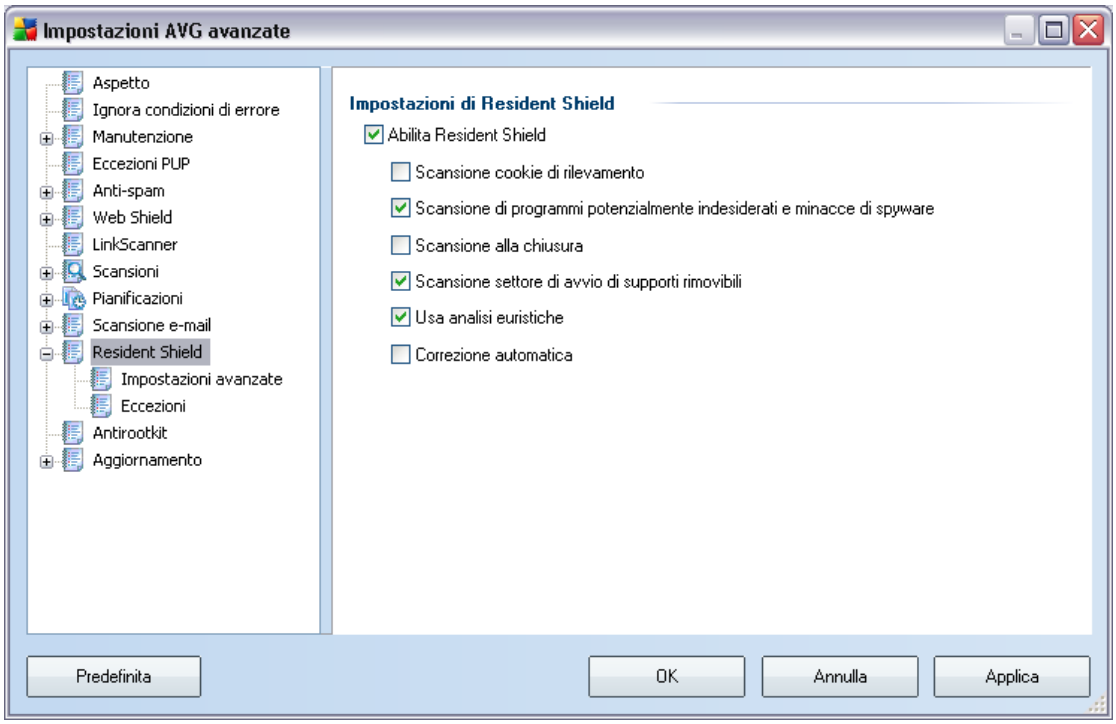
o Connessione: questo menu a discesa consente di specificare il tipo di connessione da utilizzare (normale/SSL/SSL predefinito). Se si sceglie la connessione SSL, i dati inviati verranno crittografati senza il rischio di essere rilevati o monitorati da terze parti. Questa funzionalità è disponibile solo se supportata dal server di posta di destinazione.

- ***Server amministrativo***: indica il numero della porta del server che verrà utilizzata per il recapito inverso dei rapporti amministrativi. Questi messaggi vengono generati, ad esempio, se il messaggio in entrata viene rifiutato dal server di posta di destinazione o se il server non è disponibile.

- ***Impostazioni server SMTP client e-mail***: fornisce informazioni su come configurare l'applicazione di posta client in modo che i messaggi di posta in uscita vengano controllati utilizzando il server modificato per il controllo della posta in uscita. Si tratta di un riepilogo basato sui parametri corrispondenti specificati nella finestra di dialogo e in altre finestre correlate.

12.11 Resident Shield

Il componente***Resident Shield*** fornisce una protezione attiva di file e cartelle da virus, spyware e altro malware.



Nella finestra di dialogo ***Impostazioni Resident Shield*** è possibile attivare o disattivare completamente la protezione di ***Resident Shield*** selezionando/deselezionando la voce ***Abilita Resident Shield*** (*questa opzione è attivata per impostazione predefinita*). Inoltre, è possibile selezionare quali funzionalità di ***Resident Shield*** attivare:

- ***Scansione cookie***: questo parametro definisce che i cookie devono essere rilevati durante la scansione. (*i cookie HTTP sono utilizzati per autenticare, rilevare e mantenere informazioni specifiche sugli utenti, quali le preferenze dei siti e il contenuto dei carrelli elettronici*)
- ***Scansione di programmi potenzialmente indesiderati***: (*attivata per impostazione predefinita*) esegue la scansione di programmi potenzialmente pericolosi (*applicazioni eseguibili che possono funzionare come vari tipi di spyware o adware*)

- ***Scansione alla chiusura***: la scansione alla chiusura assicura che AVG esegua la scansione di oggetti attivi (ad esempio, applicazioni, documenti …) quando vengono aperti e anche quando vengono chiusi; questa funzionalità consente di proteggere il computer da alcuni tipi di virus sofisticati

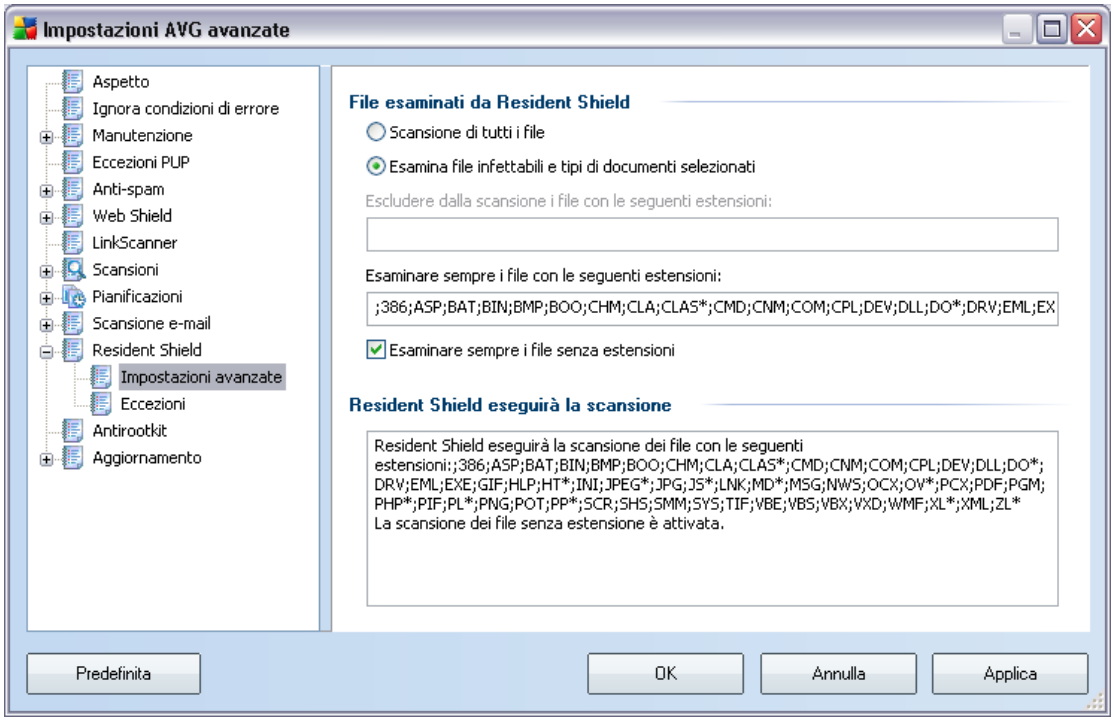
- ***Scansione settore di avvio di supporti rimovibili***: (*attivata per impostazione predefinita*)

- ***Usa analisi euristiche***- (*attivata per impostazione predefinita*) l'analisi euristica verrà utilizzata per il rilevamento (*emulazione dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale*)

- ***Correzione automatica***: le infezioni rilevate verranno corrette automaticamente se è disponibile una soluzione

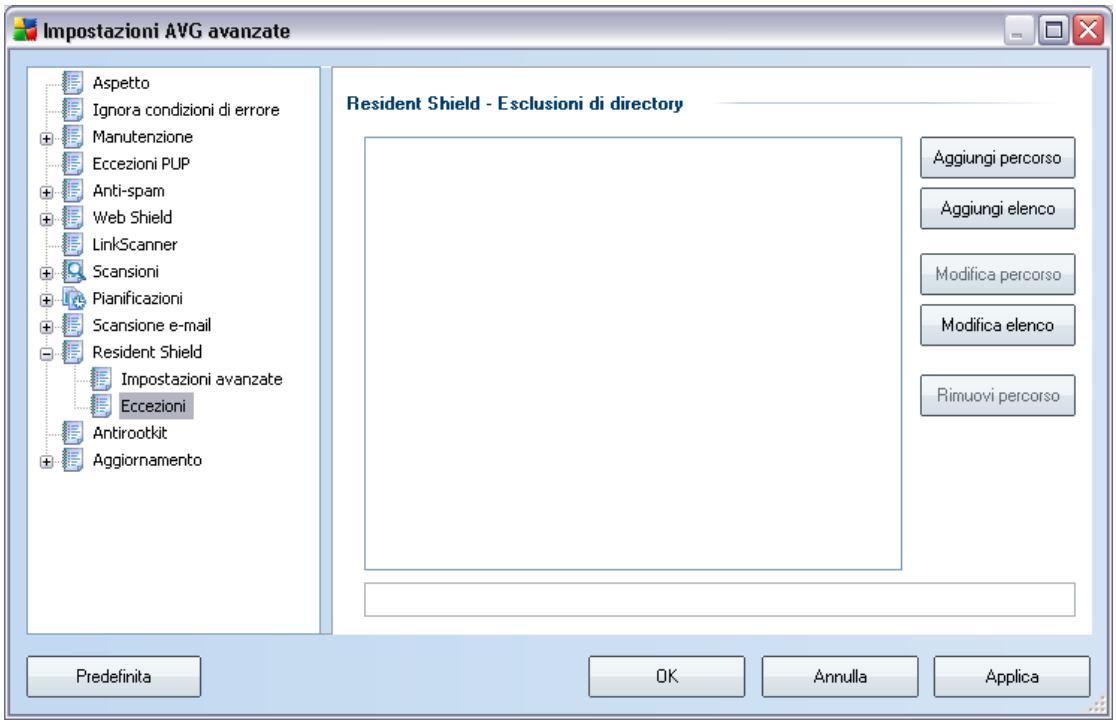
12.11. Impostazioni avanzate

Nella finestra di dialogo ***File esaminati da Resident Shield*** è possibile configurare i file che verranno sottoposti a scansione (*in base a estensioni specifiche*):



Stabilire se si desidera eseguire la scansione di tutti i file o solo dei file infettabili. In questo caso, è possibile specificare anche un elenco di estensioni definendo i file da escludere dalla scansione e un elenco di estensioni di file che devono essere sottoposti a scansione in qualsiasi circostanza.

12.11. Eccezioni



La finestra di dialogo ***Esclusioni da Resident Shield*** offre la possibilità di definire le cartelle che devono essere escluse dalla scansione di ***Resident Shield*** . Se non è essenziale, si consiglia di non escludere alcuna directory. Se si decide di escludere una cartella dalla scansione di ***Resident Shield*** , tenere presente che le nuove impostazioni saranno effettive solo dopo il riavvio del computer.

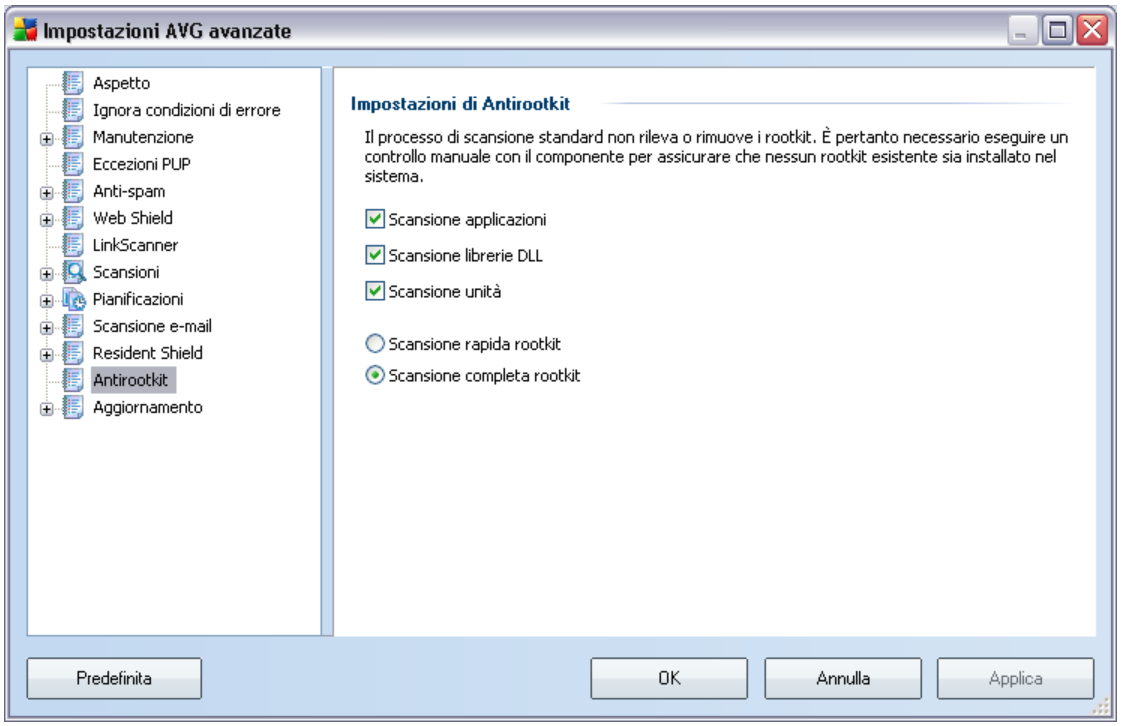
La finestra di dialogo fornisce i seguenti pulsanti di controllo:

- ***Aggiungi percorso*** : consente di specificare le directory da escludere dalla scansione selezionadole una alla volta dalla struttura di esplorazione del disco locale
- ***Aggiungi elenco*** : consente di immettere un elenco intero di directory da escludere dalla scansione di***Resident Shield***

- ***Modifica percorso*** : consente di modificare il percorso specificato di una cartella selezionata
- ***Modifica elenco*** : consente di modificare l'elenco delle cartelle
- ***Rimuovi percorso*** : consente di eliminare dall'elenco il percorso di una cartella selezionata

12.12. Anti-Rootkit

In questa finestra di dialogo è possibile modificare la configurazione del componente ***Antirootkit***:



La modifica di tutte le funzioni del componente ***Antirootkit*** presenti in questa finestra di dialogo è inoltre accessibile direttamente dall'***interfaccia del componente Antirootkit***.

Selezionare le caselle di controllo pertinenti per specificare gli oggetti da sottoporre a scansione:

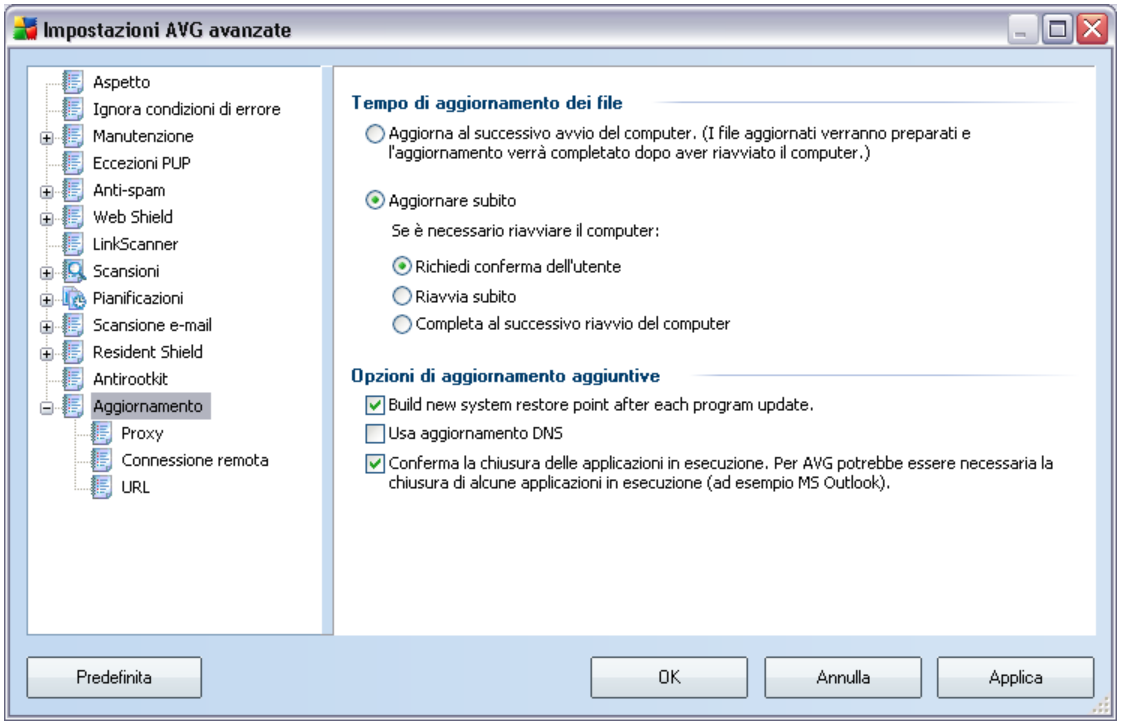
- ***Scansione applicazioni***

- ***Scansione librerie DLL***
- ***Scansione unità***

Quindi, è possibile selezionare la modalità di scansione di rootkit:

- ***Scansione rapida rootkit***: esegue la scansione della sola cartella di sistema (*in genere c:\Windows*)
- ***Scansione completa rootkit***: esegue la scansione di tutti i dischi accessibili tranne A: e B:

12.13 Aggiornamento



L'elemento di esplorazione ***Aggiorna*** consente di aprire una finestra di dialogo in cui è possibile specificare i parametri generali in relazione all'aggiornamento di AVG:

Quando eseguire l'aggiornamento dei file

In questa sezione è possibile selezionare tra due opzioni alternative: l'aggiornamento

può essere pianificato per il riavvio successivo del PC oppure è possibile avviare l' aggiornamento immediatamente. Per impostazione predefinita, è selezionata l'opzione per l'aggiornamento immediato per consentire ad AVG di garantire il livello massimo di protezione. Si consiglia la pianificazione di un aggiornamento da eseguire al riavvio successivo del PC solo se si è sicuri che il computer viene riavviato regolarmente, almeno una volta al giorno.

Se si decide di mantenere la configurazione predefinita e di avviare immediatamente il processo di installazione, è possibile specificare le circostanze in cui deve essere eseguito un possibile riavvio.

- ***Richiedi conferma dell'utente***: verrà richiesto di approvare un riavvio del PC necessario per finalizzare il processo di installazione di _
- ***Riavvia subito***: il computer verrà riavviato immediatamente in maniera automatica dopo la finalizzazione del processo di aggiornamento senza richiesta di conferma dell'utente
- ***Completa al successivo riavvio del computer***: la finalizzazione del processo di aggiornamento verrà posticipata al riavvio successivo del computer. È bene ricordarsi che questa opzione è consigliata solo se si è sicuri che il computer viene riavviato regolarmente, almeno una volta al giorno

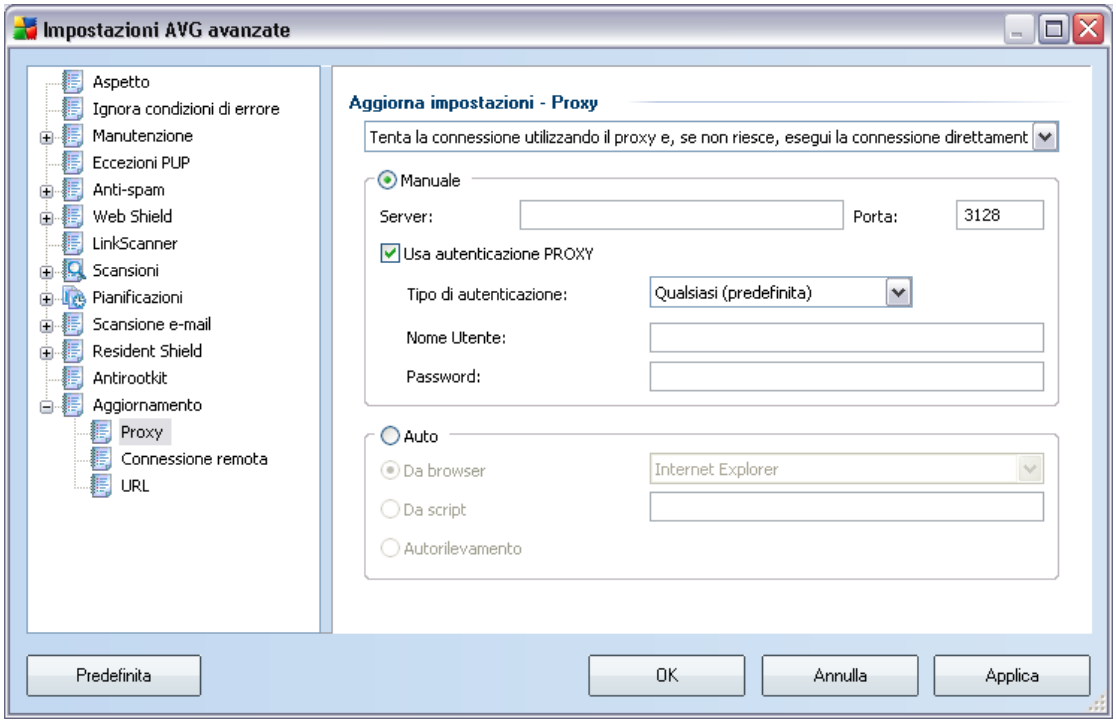
Opzioni di aggiornamento aggiuntive

- ***Crea nuovo punto di ripristino del sistema dopo ogni aggiornamento del programma***: prima dell'avvio di ciascun aggiornamento del programma AVG viene creato un punto di ripristino del sistema. Se il processo di aggiornamento non ha esito positivo e il sistema operativo si blocca, è possibile ripristinare il sistema operativo nella configurazione originale da questo punto. Questa opzione è accessibile tramite Start / Tutti i programmi / Accessori / Utilità di sistema / Ripristino configurazione di sistema, tuttavia le eventuali modifiche sono consigliate ai soli utenti esperti. Mantenere selezionata questa casella di controllo se si desidera utilizzare questa funzionalità.
- ***Usa aggiornamento DNS***: selezionare questa casella di controllo per confermare che si desidera utilizzare il metodo di rilevamento dei file di aggiornamento che elimina le quantità di dati trasferite tra il server di aggiornamento e il client AVG;
- ***La voce Conferma la chiusura delle applicazioni in esecuzione*** (*attiva per impostazione predefinita*) garantirà che nessuna applicazione in

esecuzione venga chiusa senza autorizzazione, nel caso sia necessario per la finalizzazione del processo di aggiornamento;

- ***Controlla l'ora del computer***: selezionare questa opzione per ricevere una notifica nel caso in cui l'ora del computer differisca dall'ora esatta di un valore superiore al numero di ore specificato.

12.13. Proxy



Il server proxy è un server autonomo o un servizio in esecuzione su un PC che garantisce una connessione più sicura a Internet. Secondo le regole di rete specificate è possibile accedere a Internet direttamente o tramite il server proxy. Sono anche consentite entrambe le possibilità contemporaneamente. Quindi, nella prima voce della finestra di dialogo ***Impostazioni aggiornamento – Proxy*** è necessario selezionare l'opzione desiderata dal menu della casella combinata:

- ***Utilizza proxy***
- ***Non usare server proxy***
- ***Tenta la connessione utilizzando il proxy e, se non riesce, esegui la connessione direttamente*** - impostazioni predefinite

Se si seleziona un'opzione utilizzando un server proxy, sarà necessario specificare ulteriori dati. Le impostazioni del server possono essere configurate manualmente o automaticamente.

Configurazione manuale

Se si seleziona la configurazione manuale (selezionare *l'opzione**Manuale** per attivare la sezione della finestra di dialogo corrispondente*) è necessario specificare le seguenti voci:

- ***Server*** : specifica l'indirizzo IP o il nome del server
- ***Porta*** : specifica il numero della porta che consente l'accesso a Internet (*per impostazione predefinita, il numero è impostato su 3128 ma può essere modificato – se non si è sicuri, contattare l'amministratore di rete*)

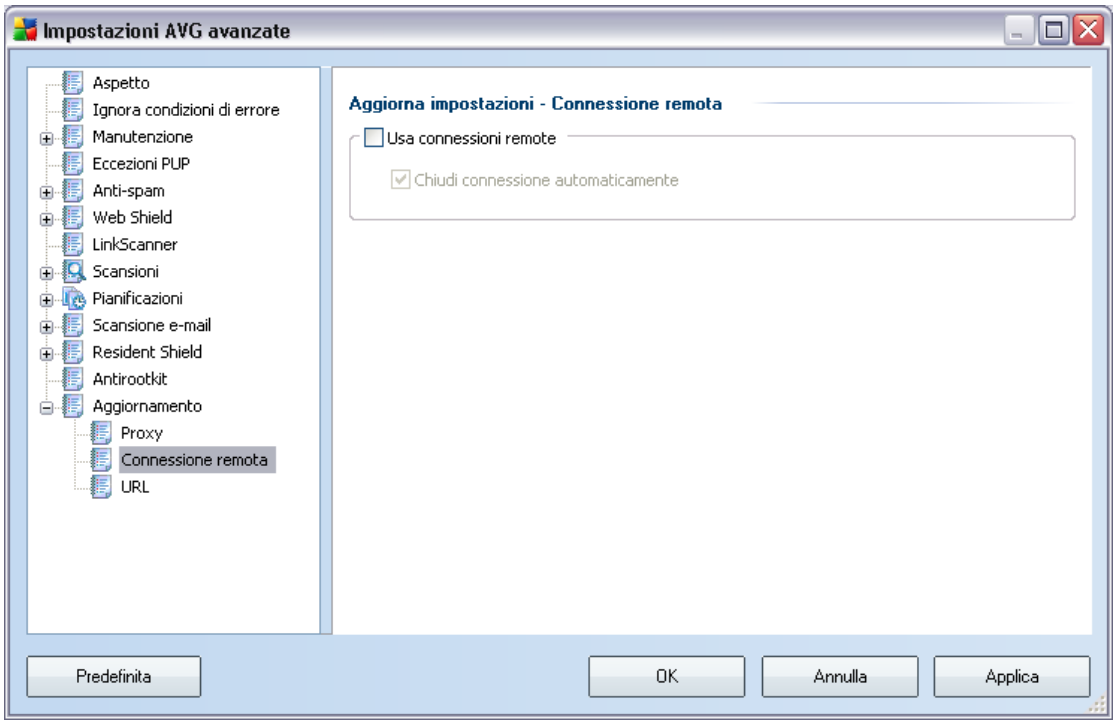
È anche possibile che sul server proxy siano state configurate regole specifiche per ciascun utente. Se il server proxy è impostato in questo modo, selezionare l'opzione ***Usa autenticazione PROXY*** per verificare che nome utente e password siano validi per la connessione a Internet tramite il server proxy.

Configurazione automatica

Se si seleziona la configurazione automatica (*selezionare l'opzione **Auto** per attivare la sezione della finestra di dialogo corrispondente*) quindi selezionare l'origine della configurazione proxy:

- ***Da browser***: la configurazione verrà letta dal browser Internet predefinito (*i browser supportati sono Internet Explorer, Firefox, Mozilla e Opera*)
- ***Da script***: la configurazione verrà letta da uno script scaricato con la funzione di restituzione dell'indirizzo proxy
- ***Autorilevamento***: la configurazione verrà rilevata automaticamente direttamente dal server proxy

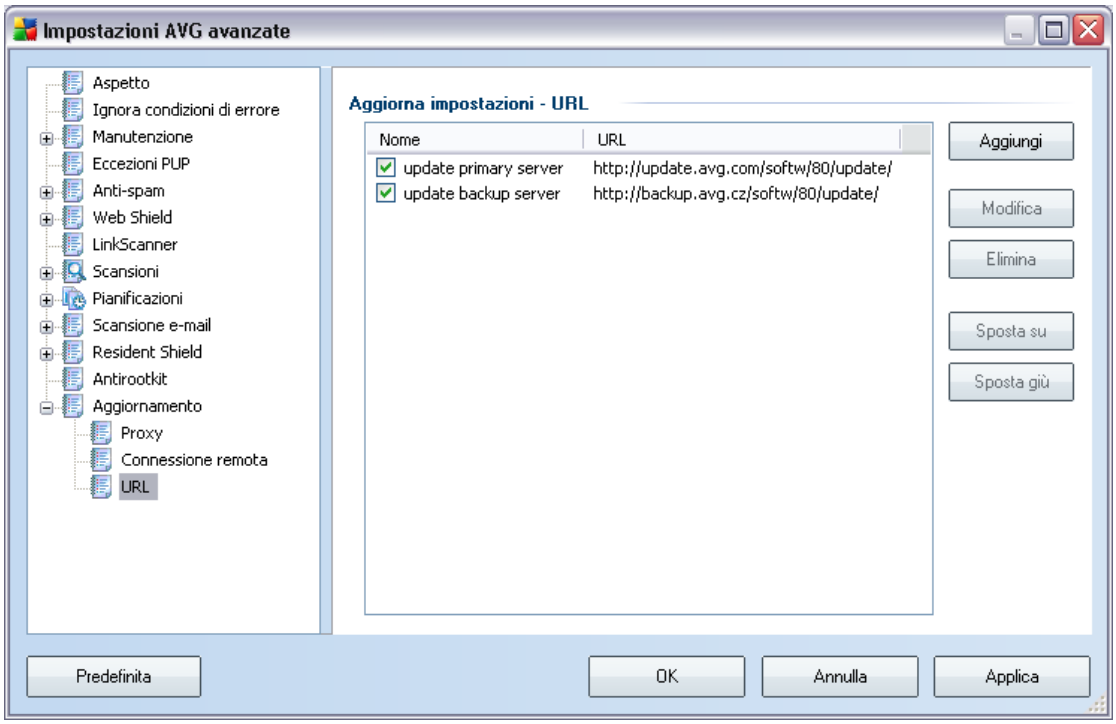
12.13.2 Connessione remota



Tutti i parametri definiti facoltativamente nella finestra di dialogo ***Aggiornamento impostazioni - Connessione remota*** fanno riferimento alla connessione remota a Internet. I campi della finestra di dialogo rimangono inattivi fino a quando non viene selezionata l'opzione ***Usa connessioni remote*** che consente l'attivazione dei campi.

Specificare se si desidera connettersi automaticamente a Internet (***Apri connessione automaticamente***) o confermare la connessione manualmente ogni volta (***Richiedi prima della connessione***). Per la connessione automatica è necessario scegliere se la connessione deve essere chiusa al termine dell'aggiornamento (***Chiudi connessione automaticamente***).

12.13. URL



Nella finestra di dialogo ***URL*** è contenuto un elenco di indirizzi Internet da cui è possibile scaricare i file di aggiornamento. È possibile modificare l'elenco e i suoi elementi utilizzando i seguenti pulsanti di controllo:

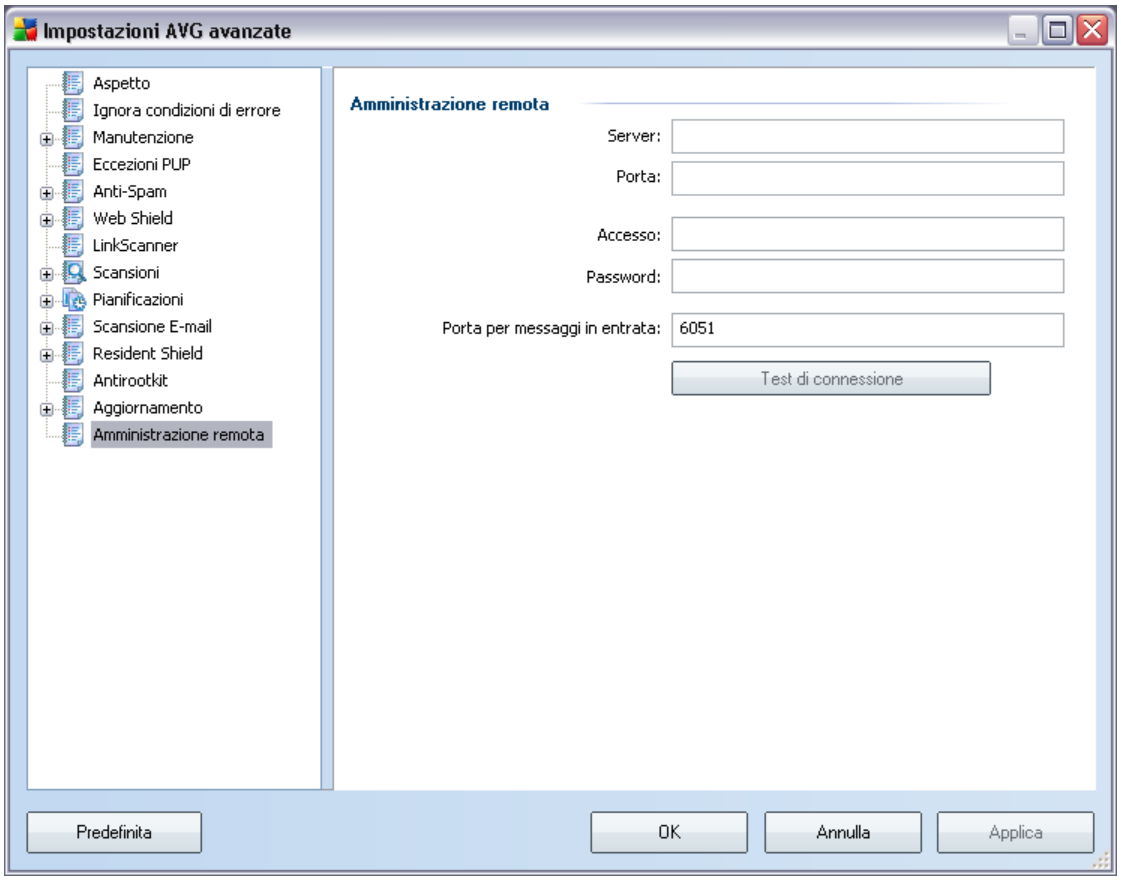
- ***Aggiungi*** :consente di aprire una finestra di dialogo in cui è possibile specificare un nuovo URL da aggiungere all'elenco
- ***Modifica***: consente di aprire una finestra di dialogo in cui è possibile modificare i parametri dell'URL selezionato
- ***Elimina*** : consente di eliminare l'URL selezionato dall'elenco
- ***Predefinito***: consente di tornare all'elenco di URL predefinito
- ***Sposta Su*** : consente di spostare l'URL selezionato di una posizione verso l'alto nell'elenco
- ***Sposta Giù***: consente di spostare l'URL selezionato di una posizione verso il basso nell'elenco

12.13. Gestione

La finestra di dialogo ***Gestione*** offre due opzioni accessibili tramite due pulsanti:

- ***Elimina file di aggiornamento temporanei***: selezionare questo pulsante per eliminare tutti i file di aggiornamento ridondanti dal disco rigido (*per impostazione predefinita, questi file restano memorizzati per 30 giorni*)
- ***Ripristina la precedente versione del database dei virus***: selezionare questo pulsante per eliminare l'ultima versione del database dei virus dal disco rigido e tornare alla precedente versione salvata (*la nuova versione del database dei virus verrà inserita nel successivo aggiornamento*)

12.14. Amministrazione remota



Le impostazioni di ***Amministrazione remota*** fanno riferimento alla connessione

della workstation client AVG al sistema di amministrazione remota. Se si programma di connettere la workstation corrispondente all'amministrazione remota, specificare i seguenti parametri:

- ***Server***: nome del server (o indirizzo IP del server) in cui è installato AVG Admin Server
- ***Porta***: fornisce il numero della porta tramite cui il client AVG comunica con AVG Admin Server (*4158 è il numero di porta predefinito: se viene utilizzato non è necessario specificarlo*)
- ***Nome utente***: se la comunicazione tra il client AVG e AVG Admin Server è protetta, fornire il proprio nome utente ...
- ***Password***:... e la password
- ***Porte per i messaggi in entrata***: numero di porta tramite cui il client AVG accetta i messaggi in entrata da AVG Admin Server

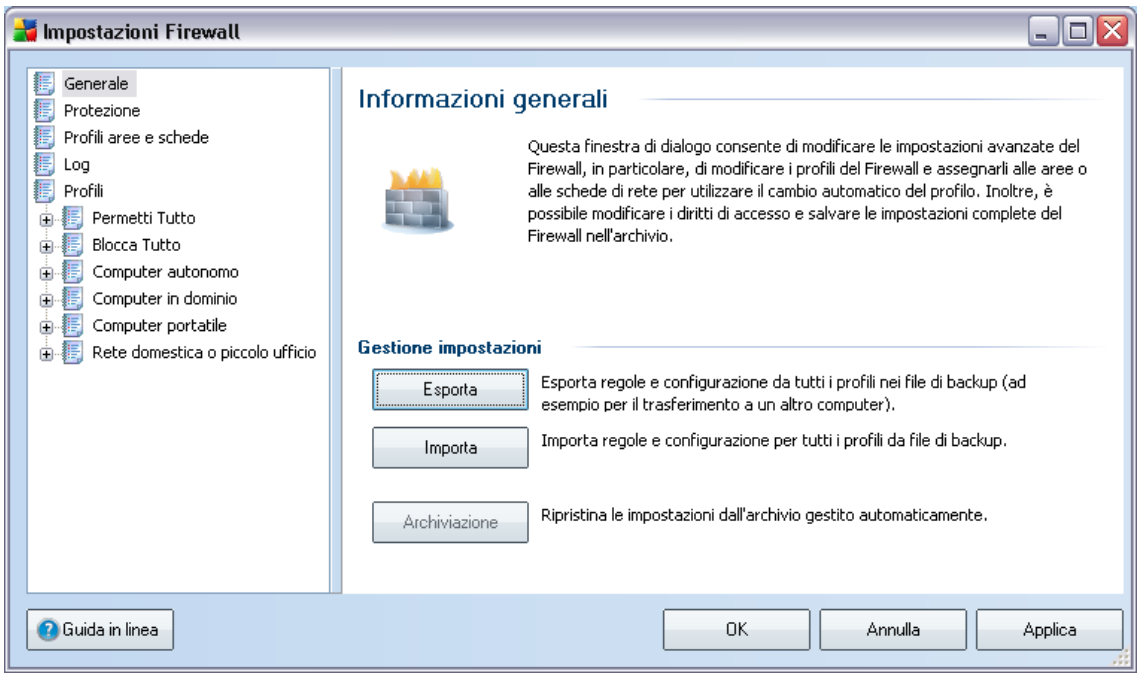
Il pulsante ***Test di connessione*** consente di verificare che tutti i dati indicati in alto sono validi e possono essere utilizzati per effettuare la connessione al DataCenter.

Nota: *per una descrizione dettagliata dell'amministrazione remota consultare la documentazione di AVG Network Edition.*

13. Impostazioni del firewall

La finestra di dialogo di configurazione di ***Firewall*** viene aperta in una nuova finestra dove in varie finestre di dialogo è possibile impostare parametri del componente molto avanzati. La modifica della configurazione avanzata deve essere eseguita solo da utenti esperti. A tutti gli altri utenti si consiglia di mantenere l'impostazione della configurazione tramite la ***Configurazione guidata del firewall***.

13.1.Generale

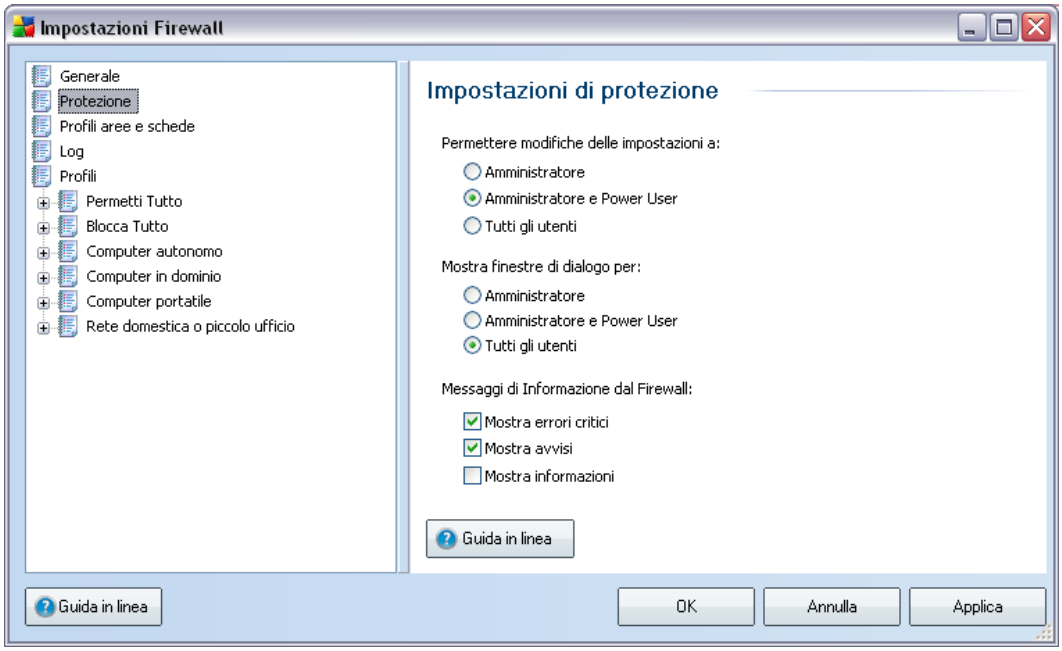


In ***Informazioni generali*** è possibile esportare/importare o memorizzare la configurazione di ***Firewall***:

- ***Esporta / Importa***: consente di esportare le regole e le impostazioni di ***Firewall*** nei file di backup o di importare l'intero file di backup.

- ***Archivio***: dopo ogni modifica apportata alla configurazione di ***Firewall*** l'intera configurazione originale viene salvata in un archivio. È possibile accedere alle configurazioni archiviate mediante il pulsante ***Archivio impostazioni***. Se l'archivio impostazioni è vuoto, significa che non sono state apportate modifiche dopo l'installazione del componente ***Firewall***. Il numero massimo di record archiviati è 10. Se si tenta di salvare un numero maggiore di record, i record meno recenti verranno sovrascritti.

13.2.Protezione



Nella finestra di dialogo ***Impostazioni di protezione*** è possibile definire regole generali del comportamento di ***Firewall***, indipendentemente dal profilo selezionato:

- ***Permettere modifiche delle impostazioni a***: consente di specificare a chi è consentito modificare la configurazione di ***Firewall***.
- ***Mostra finestre di dialogo per***: consente di specificare gli utenti per i quali devono essere visualizzate le finestre di dialogo di conferma (*finestre di dialogo in cui si chiede una decisione in una situazione che non è coperta da una regola definita di* ***Firewall***).

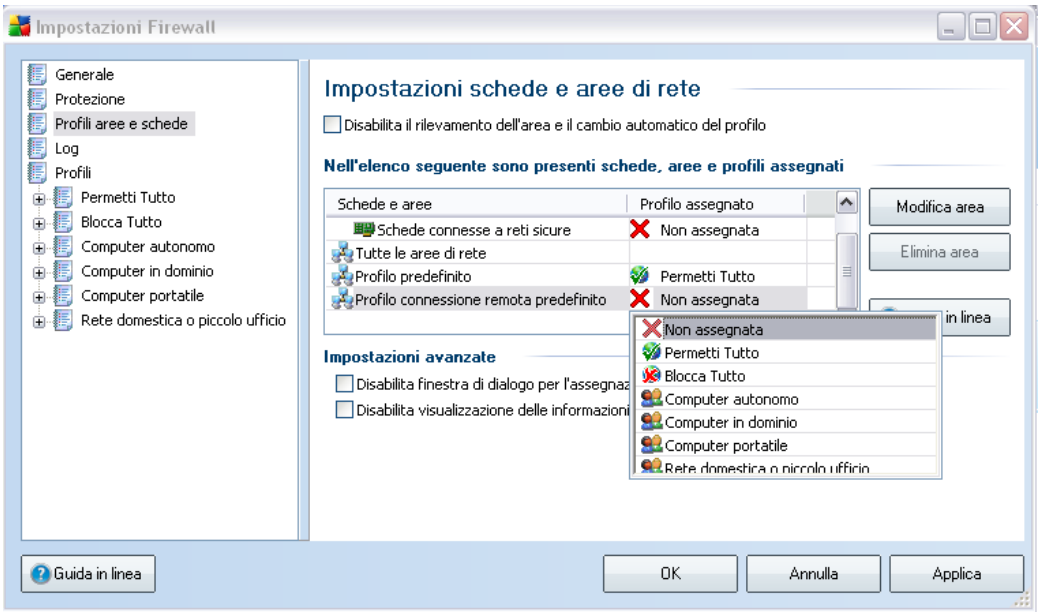
In entrambi i casi è possibile assegnare il diritto specifico a uno dei seguenti gruppi di utenti:

- ***Amministratore*** : consente di controllare completamente il PC e dispone dei diritti per assegnare ogni utente ai vari gruppi con autorità definite in modo specifico.
- ***Amministratore e Power User*** : l'amministratore può assegnare qualunque utente a un gruppo specifico (*Power User*) e definire le autorità dei membri del gruppo.

- **Tutti gli utenti** : altri utenti non assegnati a un gruppo specifico.

- ***Messaggi di Informazione dal Firewall***: consente di decidere quali messaggi di informazione di ***Firewall*** devono essere visualizzati. È consigliabile che gli errori critici e gli avvisi vengano visualizzati sempre, mentre è possibile decidere personalmente cosa fare con i messaggi di informazione.

13.3.Profili di aree e schede



Nella finestra di dialogo ***Impostazioni delle aree di rete e delle schede*** è possibile modificare impostazioni correlate all'assegnazione di profili definiti a schede specifiche con riferimento alle rispettive reti:

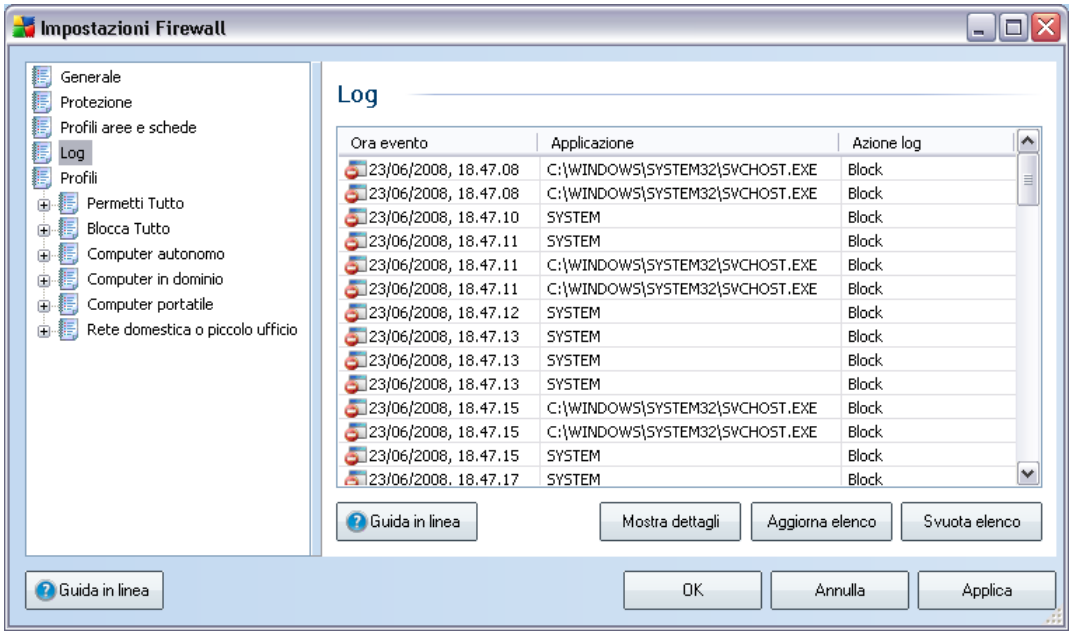
- ***Disabilita rilevamento delle aree e attivazione dei profili***: uno dei profili definiti può essere assegnato a ciascun tipo di interfaccia di rete, rispettivamente a ciascun'area. Se non si desidera definire profili specifici, verrà utilizzato un profilo comune definito durante la ***Configurazione guidata del firewall***. Tuttavia, se si decide di distinguere profili e assegnarli a schede e aree specifiche e in seguito si desidera, per qualsiasi motivo, cambiare temporaneamente questa impostazione, selezionare l'opzione ***Disabilita rilevamento delle aree e attivazione dei profili***.

- ***Elenco di schede, aree e profili assegnati***: in questo elenco è possibile

trovare una panoramica delle schede e delle aree rilevate. A ciascuna di esse è possibile assegnare un profilo specifico dal menu dei profili definiti (*tutti i profili vengono principalmente definiti nella* ***Configurazione guidata del firewall*** *oppure , in un secondo momento, è possibile creare nuovi profili nella finestra di dialogo* ***Profili*** *di Impostazioni del firewall*). Per aprire questo menu, fare clic sul rispettivo elemento nell'elenco delle schede e selezionare il profilo.

- ***Impostazioni avanzate***: se si seleziona la relativa opzione, la funzione di visualizzazione di un messaggio informativo verrà disattivata

13.4.Log



La finestra di dialogo ***Registro*** consente di visualizzare l'elenco di tutte le azioni e gli eventi registrati di ***Firewall*** con una descrizione dettagliata dei parametri rilevanti.

- ***Ora evento*** : la data e l'ora esatte in cui è stato rilevato l'evento.
- ***Applicazione*** : nome del processo a cui fa riferimento l'evento registrato.
- ***Azione*** : tipo di azione eseguita.

Sono disponibili i seguenti pulsanti di controllo:

- ***Guida in linea***: consente di aprire i file della guida correlati alla finestra di dialogo.

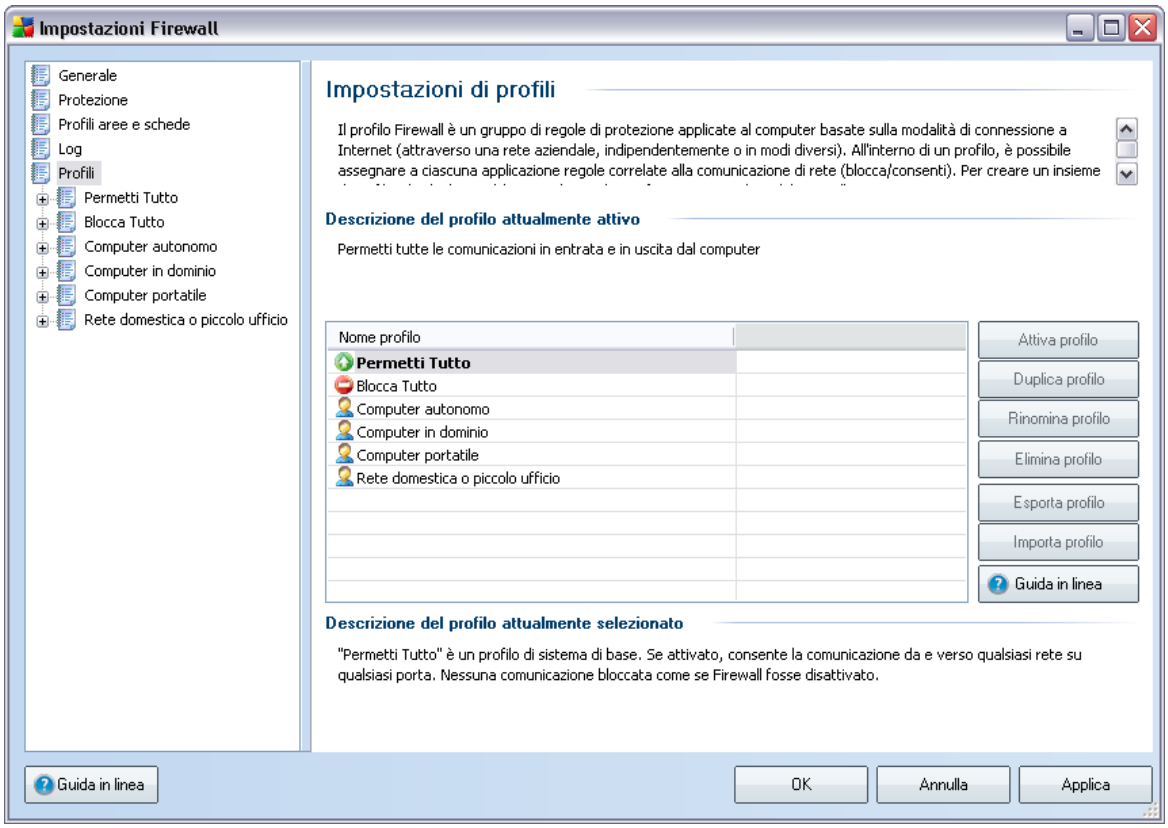
- ***Mostra dettagli***: se si ritiene che i parametri forniti non siano sufficienti e si desidera visualizzare più informazioni, utilizzare questo pulsante per passare alla panoramica avanzata del file di registro contenente ulteriori informazioni (su utente, PID, direzione, protocollo, porta remota/locale e indirizzo IP remoto/locale).

- ***Aggiorna elenco***: tutti i parametri registrati possono essere ordinati in base all'attributo selezionato: cronologicamente (*date*) o alfabeticamente (*altre colonne*). È sufficiente fare clic sull'intestazione di colonna pertinente. Utilizzare il pulsante ***Aggiorna elenco*** per aggiornare le informazioni visualizzate.

- ***Svuota elenco***: consente di eliminare tutte le voci contenute nell'elenco.

13.5.Profili

Nella finestra di dialogo ***Impostazioni di profili*** è possibile trovare un elenco di tutti i profili disponibili.



Tutti gli altri profili di sistema possono essere modificati direttamente da questa finestra di dialogo utilizzando i pulsanti di controllo seguenti:

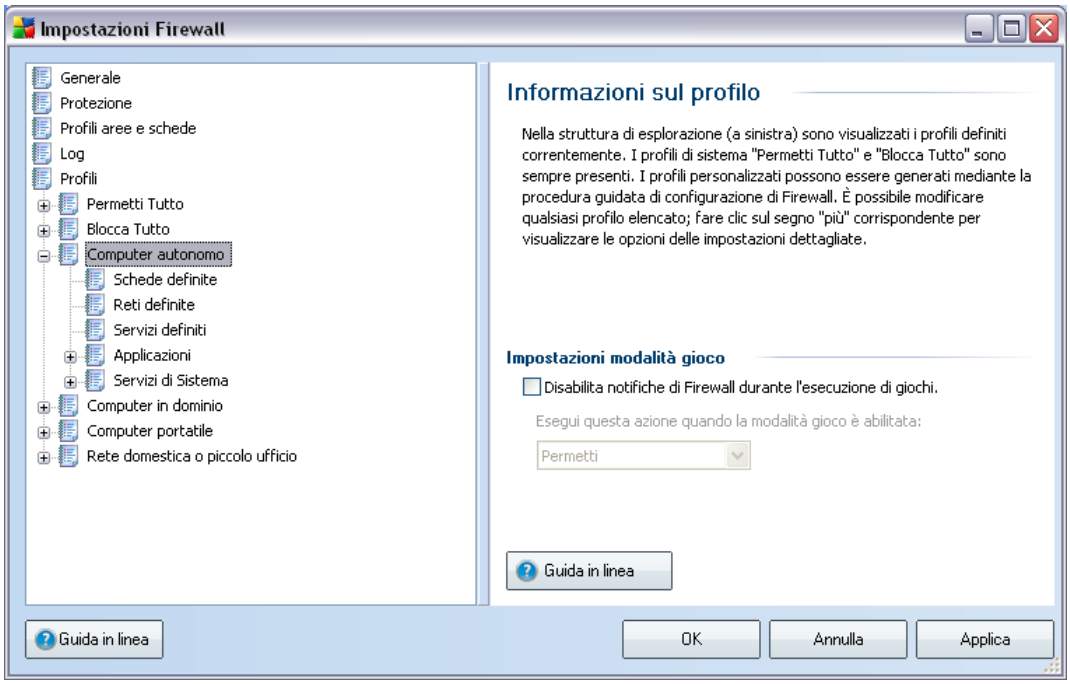
- ***Attiva profilo***: questo pulsante consente di impostare il profilo selezionato come attivo. Significa che il profilo selezionato verrà utilizzato da ***Firewall*** per controllare il traffico di rete.
- ***Duplica profilo***: consente di creare una copia identica del profilo selezionato. In seguito sarà possibile modificare e rinominare la copia per creare un nuovo profilo basato sull'originale duplicato.
- ***Rinomina profilo***: consente di definire un nuovo nome per il profilo selezionato.

- ***Elimina profilo***: consente di eliminare dall'elenco il profilo selezionato.
- ***Esporta profilo***: consente di registrare la configurazione del profilo selezionato in un file che verrà salvato per un possibile ulteriore utilizzo.
- ***Importa profilo***: consente di configurare le impostazioni del profilo selezionato in base ai dati esportati dal file di configurazione di backup.
- ***Guida in linea***: consente di aprire la finestra di dialogo del file della guida

Nella sezione inferiore della finestra di dialogo si trova la descrizione del profilo attualmente selezionato nell'elenco.

Il menu di esplorazione visualizzato a sinistra cambierà in base al numero di profili definiti elencati nella finestra di dialogo ***Profilo***. Ogni profilo definito crea un ramo specifico nell'elemento ***Profilo***. È quindi possibile modificare specifici profili nelle seguenti finestre di dialogo (*che sono identiche per tutti i profili*):

13.5.1.Informazioni sui profili



La finestra di dialogo ***Informazioni sui profili*** è la prima di una sezione in cui è possibile modificare la configurazione di ogni profilo all'interno di diverse finestre separate relative a specifici parametri del profilo.

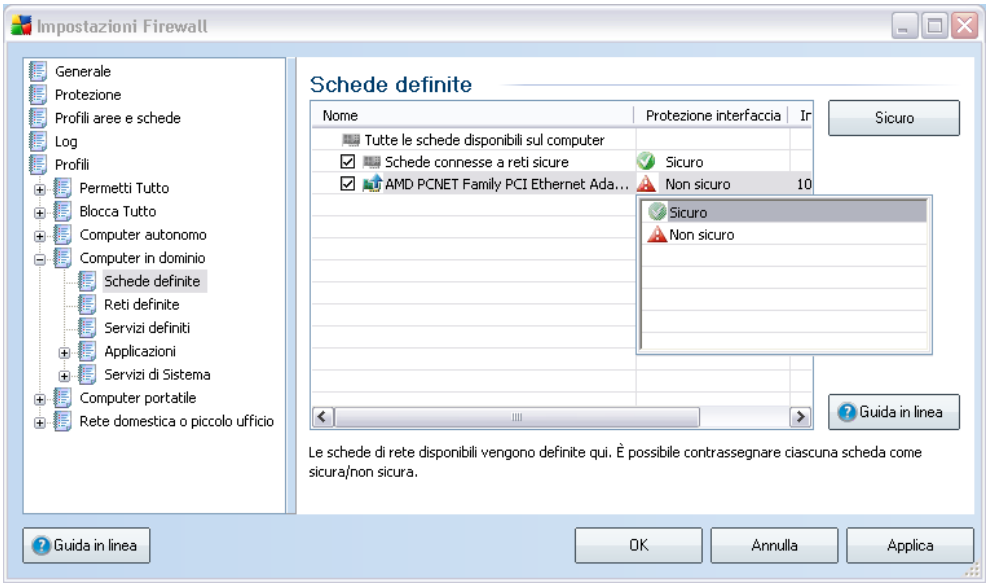
Attiva il bridging di rete delle macchine virtuali: selezionare questa voce per consentire alle macchine virtuali in WMware di connettersi direttamente alla rete

Impostazioni modalità gioco

Nella sezione ***Impostazioni modalità gioco*** è possibile decidere e confermare se si desidera che vengano visualizzati messaggi informativi del ***Firewall*** anche quando è in esecuzione un'applicazione a schermo intero sul computer (*in genere si tratta di giochi, ma l'impostazione si applica a qualunque applicazione a schermo intero, ad esempio, presentazioni in formato PPT*). per eseguire l'operazione è sufficiente selezionare il relativo elemento. Poiché i messaggi informativi possono in qualche modo essere dannosi, per impostazione predefinita la funzionalità è disattivata.

Se si seleziona l'elemento ***Abilita notifica Firewall durante l'esecuzione di giochi***, è necessario selezionare nel menu a discesa quale azione deve essere eseguita qualora una nuova applicazione ancora priva di regole specificate tenti di comunicare in rete (*applicazioni che normalmente visualizzerebbero una finestra di richiesta di conferma*). Tutte queste applicazioni possono essere consentite o bloccate.

13.5.2.Schede definite

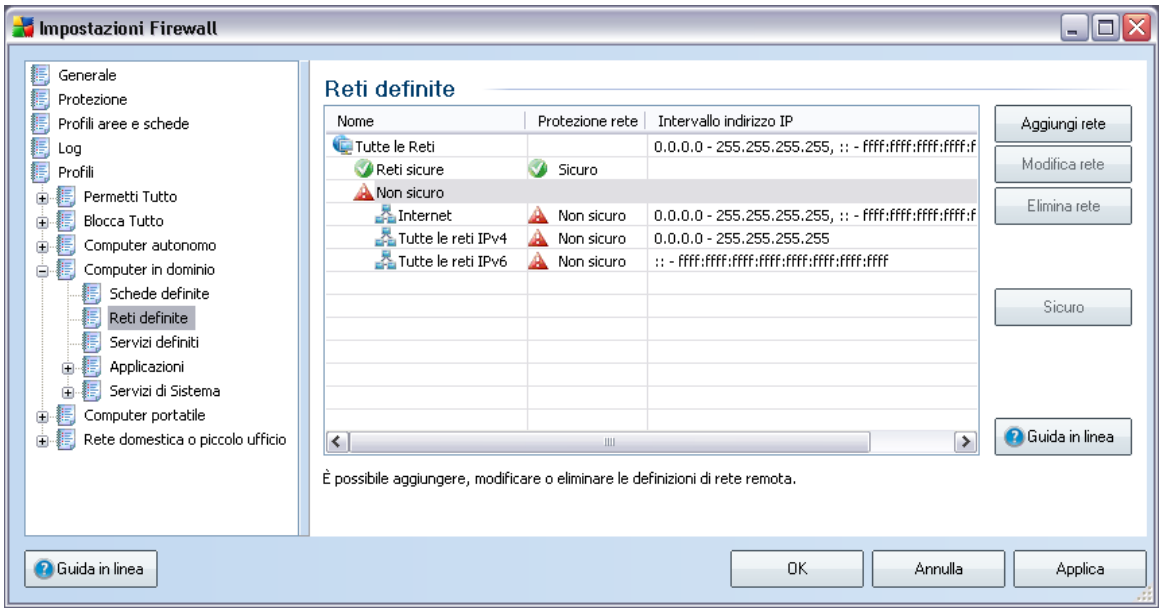


Nella finestra di dialogo ***Schede definite*** è visualizzato un elenco di tutte le schede rilevate sul computer. Una rete specifica fa riferimento a ciascuna scheda. Per l'elenco di tutte le reti, consultare la finestra di dialogo ***Reti definite***.

Per ogni scheda rilevata vengono fornite le informazioni indicate di seguito:

- ***Schede***: elenco di tutte le schede rilevate, utilizzate dal computer per la connessione a reti specifiche
- ***Protezione interfaccia***: per impostazione predefinita, tutte le schede vengono ritenute non sicure e solo se si è certi che la rispettiva scheda (e la rispettiva rete) sia sicura, è possibile assegnarla in questo modo (*fare clic sulla voce dell'elenco che si riferisce alla rispettiva scheda e scegliere Sicuro dal menu di scelta rapida oppure utilizzare il pulsante* ***Segna come sicuro***). Tutte le schede sicure e le rispettive reti verranno incluse nel gruppo delle schede e delle reti mediante le quali l'applicazione può comunicare con la regola dell'applicazione impostata su ***Consenti protette***
- ***Intervallo indirizzi IP*** : ogni rete (che fa riferimento a una scheda specifica) verrà rilevata automaticamente e specificata sotto forma di intervallo degli indirizzi IP

13.5.3.Reti definite



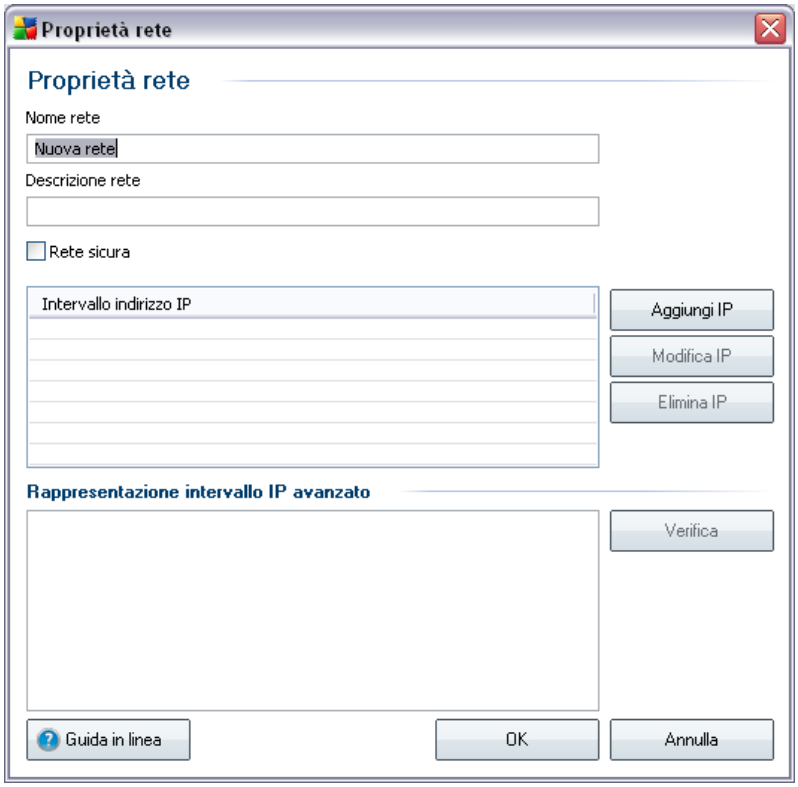
Nella finestra di dialogo ***Reti Definite*** è disponibile un elenco di tutte le reti a cui è connesso il computer. Ogni rete fa riferimento a una scheda specifica. Per un elenco di tutte le schede, vedere la finestra di dialogo ***Reti definite***.

Per ogni rete rilevata vengono fornite le informazioni indicate di seguito:

- ***Reti*** : elenco dei nomi di tutte le reti a cui è connesso il computer.
- ***Protezione rete*** : per impostazione predefinita, tutte le reti vengono considerate non sicure e solo se si è certi che una rete sia sicura è possibile assegnarla così (*fare clic sulla voce di elenco relativa alla rete desiderata e selezionare Sicuro dal menu di scelta rapida*). Tutte le reti sicure verranno incluse nel gruppo delle reti attraverso le quali l'applicazione potrà comunicare con la regola dell'applicazione impostata su ***Consenti protette.***
- ***Intervallo indirizzi IP*** : ogni rete verrà rilevata automaticamente e specificata sotto forma di intervallo degli indirizzi IP.

Pulsanti di controllo

- ***Aggiungi rete*** : consente di aprire la finestra di dialogo ***Proprietà rete*** dove è possibile modificare parametri della rete appena definita:



In questa finestra di dialogo è possibile specificare il ***Nome rete***, fornire

la ***Descrizione rete*** e possibilmente assegnare la rete come sicura. La nuova rete può essere definita manualmente in una finestra di dialogo autonoma aperta mediante il pulsante ***Aggiungi IP*** (in alternativa ***Modifica IP*** / ***Elimina IP***). In questa finestra di dialogo è possibile specificare la rete mediante il relativo intervallo IP o la relativa maschera IP.

Per un grande numero di reti da definire come parte della rete appena creata è possibile utilizzare l'opzione ***Rappresentazione intervallo IP avanzato***: immettere l'elenco di tutte el reti nel relativo campo di testo (*è supportato qualunque formato standard*) e premere il pulsante ***Verifica*** per assicurarsi che il formato possa essere riconosciuto. Quindi premere ***OK*** per confermare e salvare i dati.

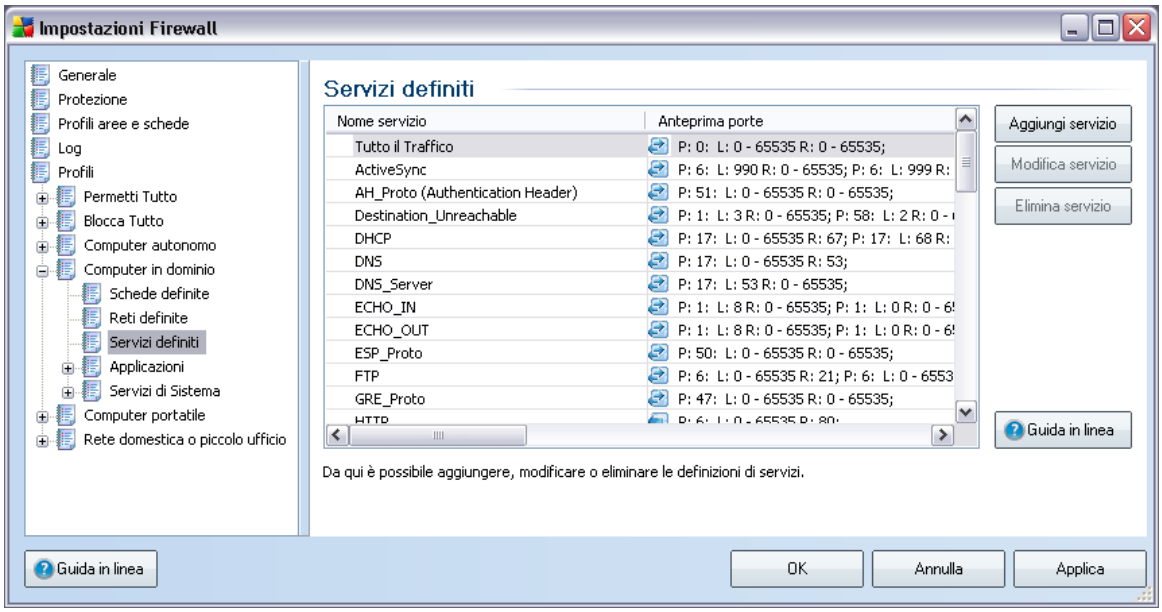
- ***Modifica rete*** : consente di aprire la finestra di dialogo ***Proprietà rete*** (*vedere sopra*) dove è possibile modificare i parametri di una rete già definita (*questa finestra di dialogo è identica alla finestra di dialogo per l'aggiunta di nuove reti, vedere la descrizione nel paragrafo precedente*)

- ***Elimina rete*** : consente di rimuovere il nodo di una rete selezionata dall'elenco delle reti.

- ***Segna come sicuro*** : per impostazione predefinita, tutte le reti vengono considerate non sicure e solo se si è certi che la rete desiderata sia sicura è consigliabile utilizzare questo pulsante per assegnarla così.

- ***Guida in linea***: consente di aprire la finestra di dialogo del file della guida

13.5.4.Servizi definiti



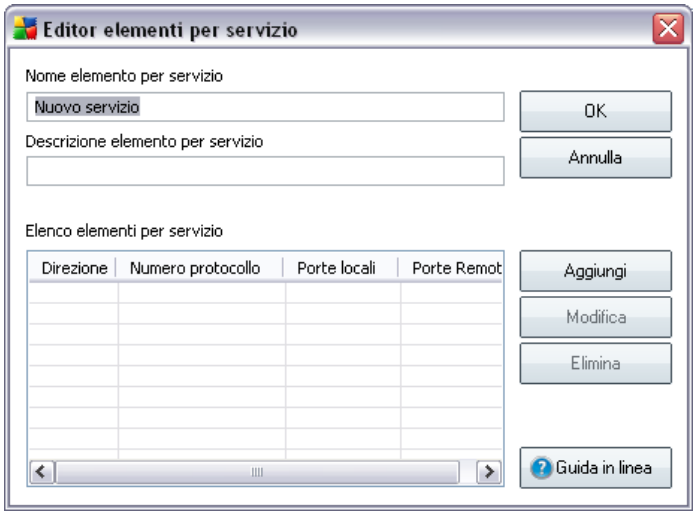
La finestra di dialogo ***Servizi definiti*** consente di aprire un elenco di tutti i servizi definiti per l'applicazione nella configurazione predefinita e dei servizi già definiti dall'utente. La finestra di dialogo è suddivisa in due colonne:

- ***Nome servizio:*** fornisce il nome del servizio
- ***Anteprima porte***: le frecce indicano la comunicazione in entrata/in uscita; inoltre viene fornito il numero o il nome del protocollo utilizzato (P) e il numero o l'intervallo delle porte locali (L) / remote (R) utilizzate

Da qui è possibile aggiungere, modificare e/o eliminare servizi specifici.

Pulsanti di controllo

- ***Aggiungi servizio*** : consente di aprire una nuova finestra di dialogo ***Editor elementi per servizio*** in cui vengono definiti i parametri del servizio aggiunto:

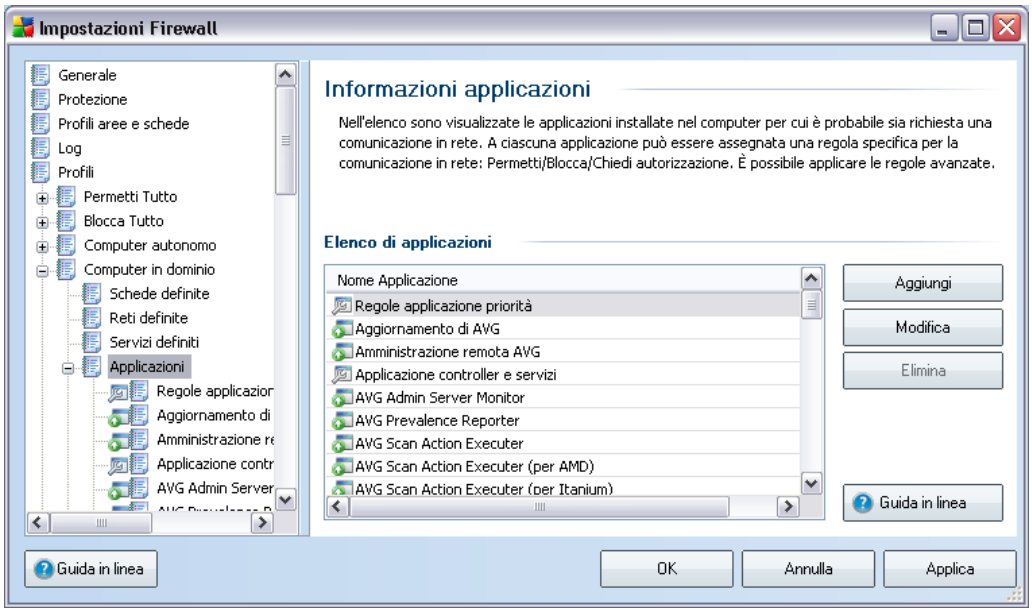


In questa finestra è possibile specificare il ***Nome elemento per servizio*** e fornire una breve ***Descrizione elemento per servizio***. Nella sezione ***Elenco elementi per servizio*** è quindi possibile aggiungere (*e anche modificare o eliminare*) elementi per il servizio specificando i seguenti parametri:

- ***Direzione*** : in entrata, in uscita o in entrambe le direzioni.
- ***Numero protocollo*** : il tipo di protocollo (*selezionarne uno dal menu*)
- ***Porte locali*** : l'elenco di intervalli di porte locali.
- ***Porte remote*** : l'elenco di intervalli di porte remote.

- ***Modifica servizio*** : consente di aprire la finestra di dialogo ***Editor elementi per servizio***(*vedere sopra*) dove è possibile modificare i parametri di un servizio già definito (*questa finestra di dialogo è identica alla finestra di dialogo per l'aggiunta di un nuovo servizio, vedere la descrizione nel paragrafo precedente*)
- ***Elimina servizio*** : consente di rimuovere il nodo di un servizio selezionato dall'elenco.
- ***Guida in linea***: consente di aprire la finestra di dialogo del file della guida

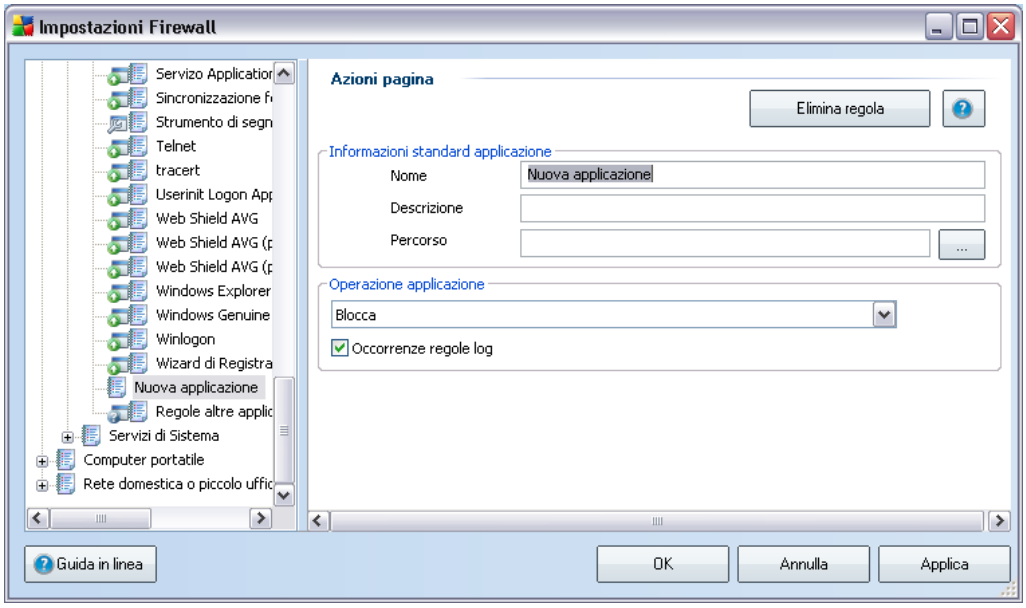
13.5.5.Applicazioni



Nella finestra di dialogo ***Informazioni applicazioni*** è possibile trovare una panoramica di tutte le applicazioni che comunicano in rete e che vengono rilevate sul computer durante la ricerca della ***Configurazione guidata del firewall*** nella finestra di dialogo ***Scansione di applicazioni Internet*** o successivamente, in qualsiasi altro momento. Per modificare l'elenco, utilizzare i seguenti pulsanti di controllo:

- ***Aggiungi***: consente di aprire la finestra di dialogo per definire un nuovo insieme di regole dell'applicazione
- ***Modifica***: consente di aprire la finestra di dialogo per modificare un insieme di regole esistenti per l'applicazione
- ***Elimina***: consente di rimuovere dall'elenco l'applicazione selezionata
- ***Guida in linea***: consente di aprire la finestra di dialogo del file della guida

Per aprire la finestra di dialogo per la definizione di un nuovo insieme di regole dell'applicazione utilizzare il pulsante ***Aggiungi*** nella finestra di dialogo ***Applicazioni*** in ***Impostazioni del firewall***:



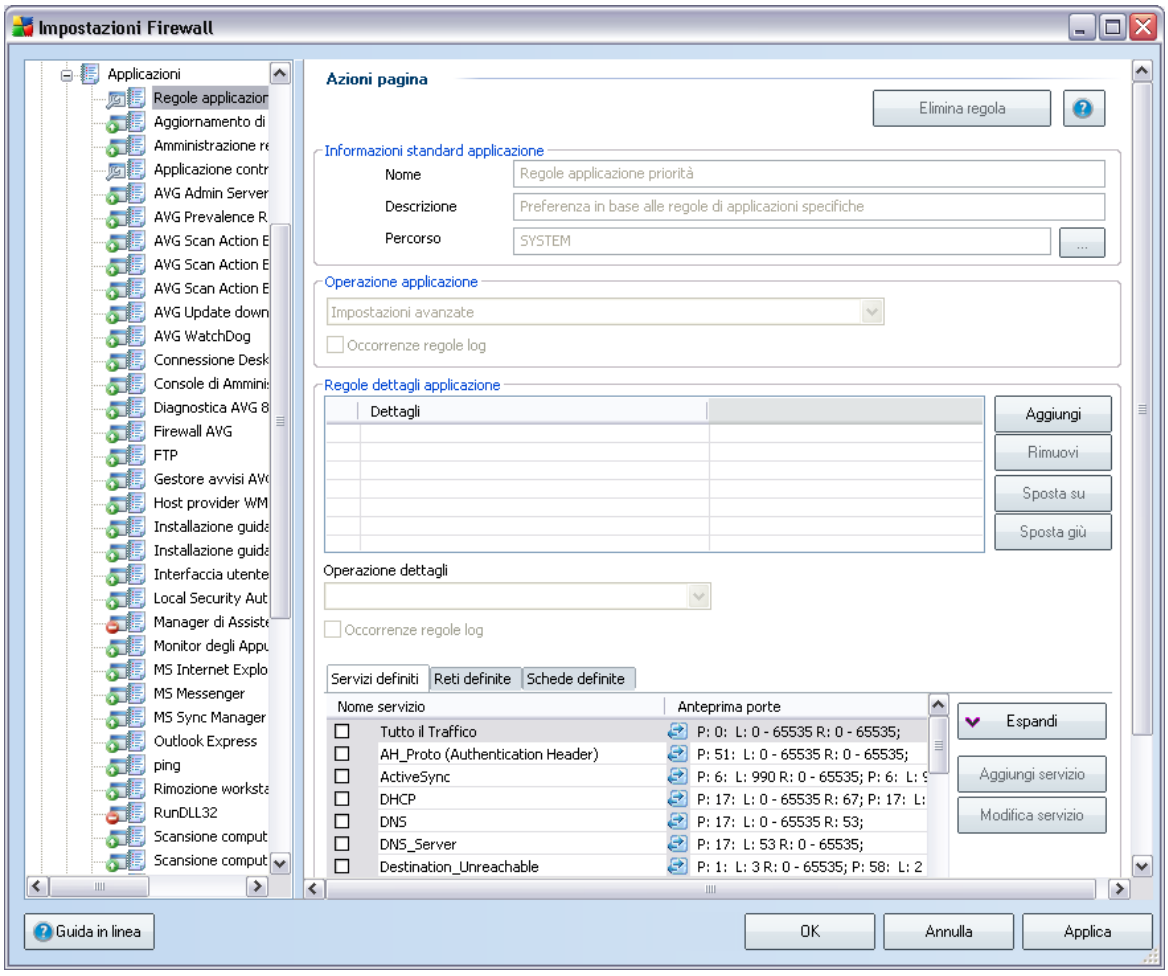
Questa finestra di dialogo consente di definire quanto segue:

- ***Informazioni standard applicazione***: nome dell'applicazione, relativa descrizione breve e percorso sul disco
- ***Azione applicazione***: dal menu a discesa scegliere una regola che deve essere applicata all'applicazione:
  - ***Impostazioni avanzate:*** questa opzione consente di modificare l'insieme di regole descritto in dettaglio nella parte inferiore di questa finestra di dialogo; *per la descrizione di questa sezione vedere il capitolo* ***Modifica applicazione***
  - ***Consenti tutte:*** verranno consentiti tutti i tentativi di comunicazione dell'applicazione
  - ***Consenti protette:*** l'applicazione potrà comunicare solo in reti protette (*ad esempio, la comunicazione sulla rete aziendale protetta verrà consentita mentre la comunicazione mediante Internet verrà bloccata*); per una panoramica e una descrizione di reti protette, vedere la finestra di dialogo ***Reti***
  - ***Chiedi:*** ogni volta che l'applicazione tenta di comunicare in rete, verrà chiesto di scegliere se consentire o bloccare la comunicazione

- ***Blocca:*** qualsiasi tentativo di comunicazione da parte dell'applicazione viene bloccato

- ***Registra occorrenze regole***: selezionare questa opzione per confermare che si desidera registrare tutte le operazioni del ***Firewall*** relative all'applicazione per la quale si configura l'insieme di regole. Le varie voci del registro si portanno ritrovare nella finestra di dialogo ***Registri***.

Per aprire la finestra di dialogo per la modifica di un insieme di regole esistenti per l'applicazione utilizzare il pulsante ***Modifica*** nella finestra di dialogo ***Applicazioni*** di ***Impostazioni del firewall***:



In questa finestra di dialogo è possibile modificare tutti i parametri dell'applicazione:

- ***Informazioni standard applicazione***: nome dell'applicazione, relativa descrizione breve e percorso sul disco
- ***Azione applicazione***: dal menu a discesa scegliere una regola che deve essere applicata all'applicazione:
  - ***Impostazioni avanzate:*** questa opzione consente di modificare l'insieme di regole in modo dettagliato nella parte inferiore della finestra di dialogo.
  - ***Consenti tutte:*** verranno consentiti tutti i tentativi di comunicazione dell'applicazione
  - ***Consenti protette:*** l'applicazione potrà comunicare solo in reti protette (*ad esempio, la comunicazione sulla rete aziendale protetta verrà consentita mentre la comunicazione mediante Internet verrà bloccata*); per una panoramica e una descrizione di reti protette, vedere la finestra di dialogo ***Reti***
  - ***Chiedi:*** ogni volta che l'applicazione tenta di comunicare in rete, verrà chiesto di scegliere se consentire o bloccare la comunicazione
  - ***Blocca:*** qualsiasi tentativo di comunicazione da parte dell'applicazione viene bloccato
- ***Registra occorrenze regole***: selezionare questa opzione per confermare che si desidera registrare tutte le operazioni del ***Firewall*** relative all'applicazione per la quale si configura l'insieme di regole. Le varie voci del registro si portanno ritrovare nella finestra di dialogo ***Registri***.
- ***Regole dettagliate applicazione***: è possibile aprire questa sezione per la modifica solo se prima è stata selezionata l'opzione ***Impostazioni avanzate*** dal menu a discesa ***Azione applicazione***. È possibile modificare tutte le impostazioni dettagliate (elencate nella colonna ***Dettagli***) mediante questi pulsanti di controllo:
  - ***Aggiungi***: utilizzare il pulsante per creare una nuova regola dettagliata per un'applicazione specifica. Nella scheda ***Dettagli*** viene visualizzata una nuova voce e sarà necessario specificare i parametri relativi selezionando le reti corrispondenti per la comunicazione con l'applicazione (scheda ***Reti***), le schede che possono essere utilizzate dall'applicazione (scheda ***Schede***) e i servizi utilizzabili dall'applicazione (scheda ***Nome servizio***).

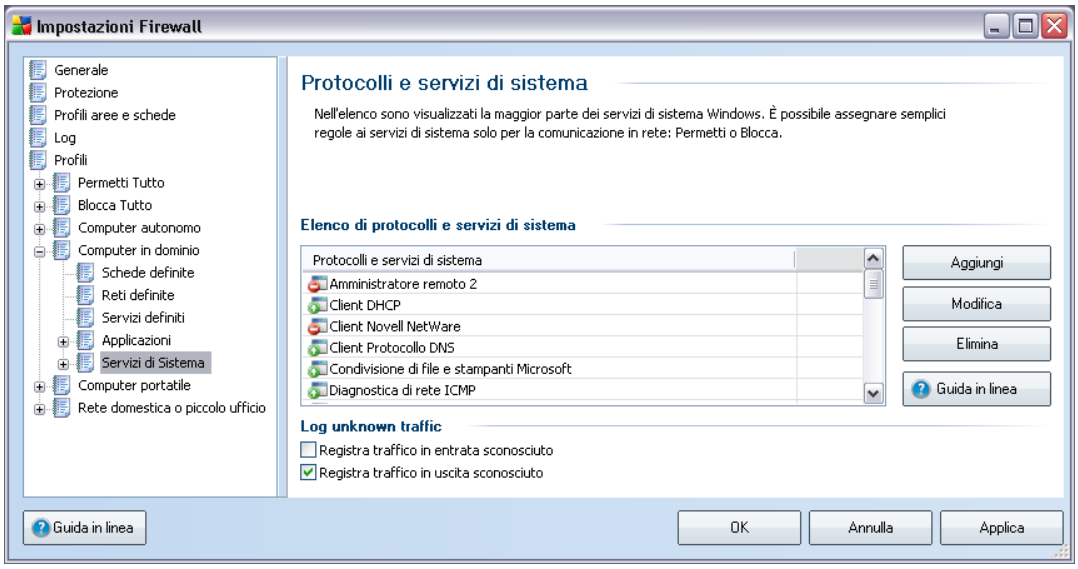
- ***Rimuovi***: consente di rimuovere la voce selezionata su una regola dettagliata dall'elenco

- ***Sposta su / Sposta giù*** : le regole dettagliate vengono ordinate in base alla priorità. Se si desidera modificare la priorità delle regole, utilizzare i pulsanti ***Sposta su*** e ***Sposta giù*** per modificare le impostazioni dettagliate in base alle necessità.

Ciascuna impostazione dettagliata specifica inoltre quali ***Servizi definiti / Reti definite / Schede definite*** verranno utilizzati.

13.5.6.Servizi di sistema

Si consiglia di apportare modifiche alla finestra di dialogo Protocolli e servizi di sistema solo se si è utenti esperti.

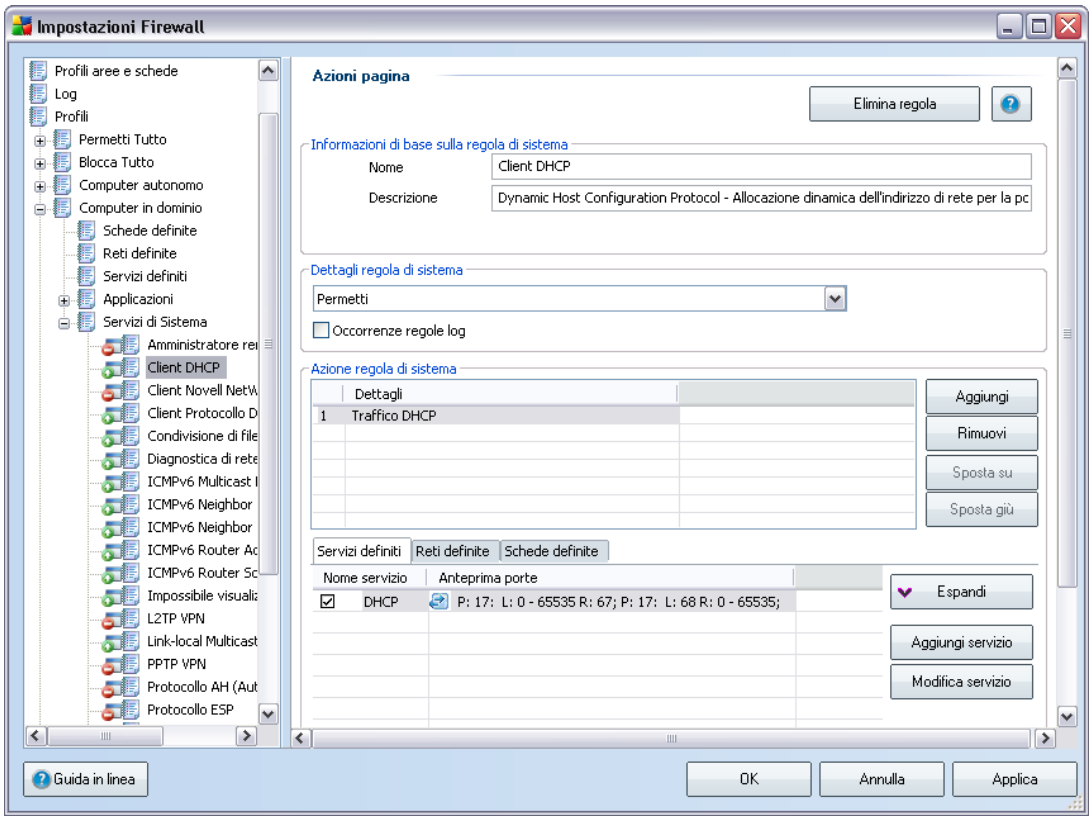


Nella finestra di dialogo ***Protocolli e servizi di sistema*** è visualizzata una panoramica dei protocolli e dei servizi di sistema che stabiliscono comunicazioni in rete. Sotto l'elenco è possibile trovare due opzioni: selezionarle/deselezionarle per confermare che si desidera registrare tutto il traffico sconosciuto in entrambe le direzioni (*in entrata o in uscita*).

Pulsanti di controllo

- ***Aggiungi/Modifica***: entrambi i pulsanti consentono di aprire la stessa

finestra di dialogo nella quale è possibile modificare i parametri del servizio di sistema. Il pulsante ***Aggiungi*** consente di aprire una finestra di dialogo vuota in modalità di base (*nessuna sezione delle opzioni avanzate; tuttavia questa sezione può essere aperta selezionando le impostazioni avanzate per l'azione dell'applicazione*); il pulsante ***Modifica*** consente di aprire la stessa finestra di dialogo con i dati già immessi riferiti al servizio di sistema selezionato:



- **Informazioni standard applicazione**: nome dell'applicazione e breve descrizione

- **Azione applicazione**: dal menu a discesa scegliere una regola da applicare al funzionamento del servizio di sistema (*rispetto alle applicazioni, sono disponibili solo tre azioni per i servizi di sistema*):

  - ***Blocca***: qualsiasi tentativo di comunicazione da parte del servizio di sistema viene bloccato

  - ***Consenti protette***: il servizio di sistema potrà comunicare solo

tramite reti sicure (*ad esempio, le comunicazioni alla rete aziendale protetta saranno consentite, mentre le comunicazioni in Internet verranno bloccate*). Per una panoramica e una descrizione delle reti sicure, vedere la finestra di dialogo ***Reti***

- ***Consenti tutte*** - verranno consentiti tutti i tentativi di comunicazione del servizio di sistema

o ***Registra occorrenze regole***: selezionare questa opzione per confermare che si desidera registrare tutte le azioni del componente ***Firewall*** relative al servizio di sistema per il quale si configura l'insieme di regole. Le varie voci del registro si potranno ritrovare nella finestra di dialogo ***Registri***.

o ***Regole dettagli applicazione*** - per ciascun servizio di sistema è possibile specificare ulteriormente le regole dettagliate nella sezione ***Regole dettagli applicazione***. Tutte le impostazioni dettagliate (elencate nella scheda ***Dettagli***) possono essere modificate utilizzando questi pulsanti di controllo:

- ***Aggiungi***: utilizzare il pulsante per creare una nuova regola dettagliata per un servizio di sistema specifico. Nella scheda ***Dettagli*** viene visualizzata una nuova voce e sarà necessario specificare i parametri relativi selezionando le reti corrispondenti per consentire la comunicazione del servizio di sistema (scheda ***Reti***), le schede che possono essere utilizzate dal servizio di sistema (***Schede***) e i servizi che possono essere utilizzati dal servizio di sistema (scheda ***Nome servizio***).

- ***Rimuovi***: consente di rimuovere la voce selezionata su una regola dettagliata dall'elenco

- ***Sposta su / Sposta giù*** : le regole dettagliate vengono ordinate in base alla priorità. Se si desidera modificare la priorità delle regole, utilizzare i pulsanti ***Sposta su*** e ***Sposta giù*** per modificare le impostazioni dettagliate in base alle necessità.

Ciascuna impostazione dettagliata specifica inoltre quali ***Servizi definiti / Reti definite / Schede definite*** verranno utilizzati.

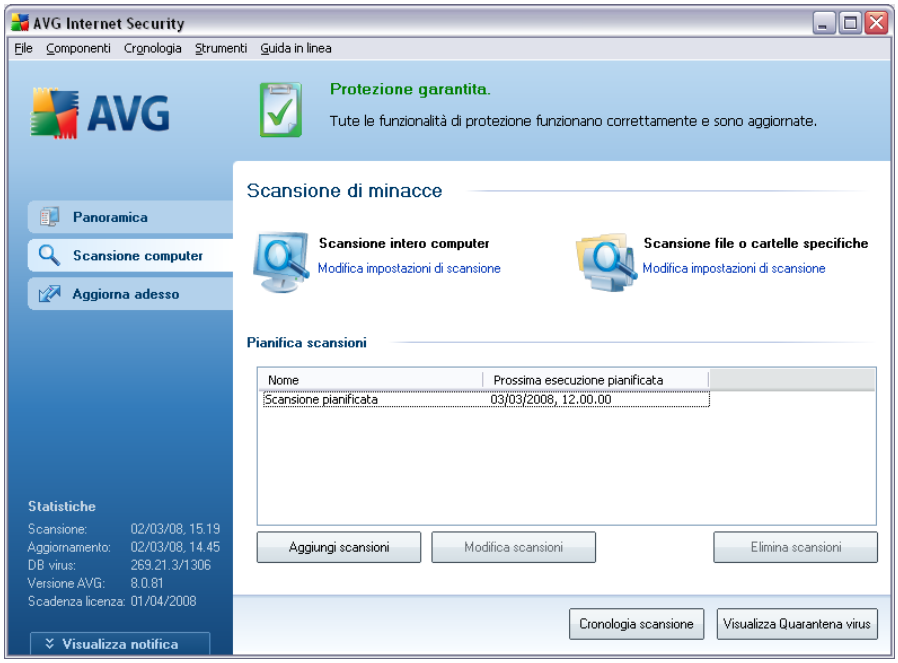
- ***Elimina***: consente di rimuovere la voce selezionata su un servizio di sistema selezionato dall'elenco precedente.

- ***Guida in linea***: consente di aprire la finestra di dialogo del file della guida

14. Scansione AVG

La scansione è una parte fondamentale del funzionamento di **AVG 8.5 Internet Security** . È possibile eseguire verifiche su richiesta o pianificarle affinché vengano eseguite su base giornaliera in un orario specifico.

14.1.Interfaccia di scansione



L'interfaccia di scansione di AVG è accessibile tramite il collegamento rapido ***Scansione computer***. Fare clic sul collegamento per accedere alla finestra di dialogo ***Scansione di minacce***. Nella finestra di dialogo è contenuto quanto segue:

- panoramica delle scansioni predefinite: sono disponibili due tipi di controlli (definiti dal fornitore di software) che possono essere utilizzati immediatamente su richiesta oppure pianificati;
- sezione della pianificazione delle scansioni, dove si possono definire nuovi controlli e creare nuove pianificazioni in base alle esigenze.

Pulsanti di controllo

I pulsanti di controllo disponibili nell'interfaccia di controllo sono i seguenti:

- ***Cronologia scansione*** : consente di visualizzare la finestra di dialogo Panoramica risultati di scansione insieme alla cronologia completa della scansione

- ***Visualizza Quarantena virus***: consente di aprire una nuova finestra con Quarantena virus, lo spazio in cui le infezioni rilevate vengono messe in quarantena

14.2.Scansioni predefinite

Una delle principali funzionalità di AVG è la scansione su richiesta. I controlli su richiesta sono progettati per eseguire la scansione di varie parti del computer quando si sospetta una possibile infezione da virus. Comunque, si consiglia di eseguire regolarmente tali verifiche anche se non si ritiene che siano presenti virus nel computer.

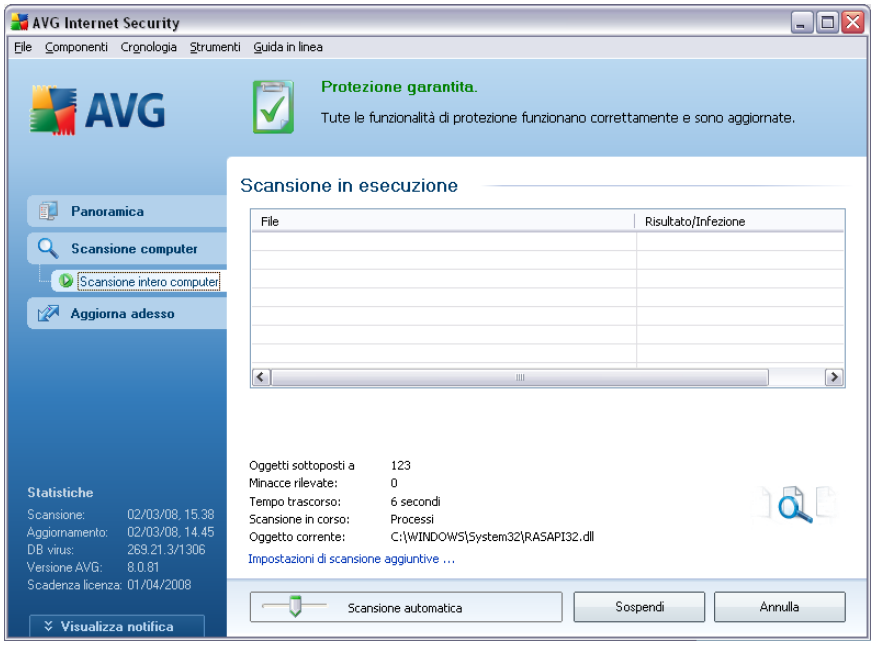
In **AVG 8.5 Internet Security** sono disponibili due tipi di scansione predefiniti dal fornitore di software:

14.2.1.Scansione intero computer

Scansione intero computer : consente di eseguire le scansioni dell'intero computer per il rilevamento di possibili infezioni e/o di programmi potenzialmente indesiderati. Questo controllo eseguirà la scansione di tutti i dischi rigidi del computer, rileverà e correggerà i virus trovati oppure rimuoverà l'infezione rilevata in ***Quarantena virus***. È necessario pianificare la scansione dell'intero computer in una workstation almeno una volta la settimana.

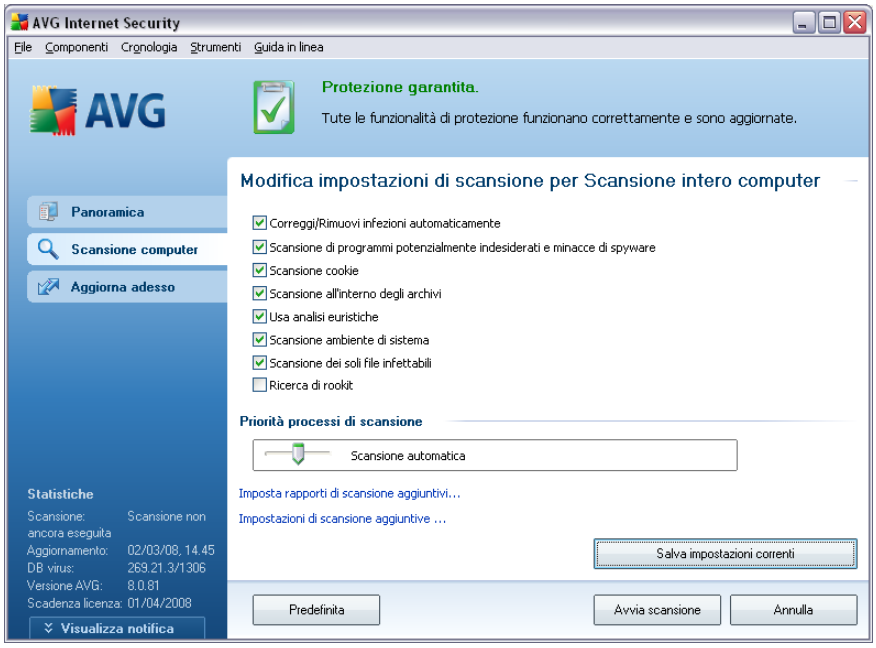
Avvia scansione

È possibile avviare ***Scansione intero computer*** direttamente dall'interfaccia di scansione facendo clic sull'icona di scansione. Non è necessario configurare ulteriori impostazioni specifiche per questo tipo di scansione, la scansione verrà avviata immediatamente nella finestra di dialogo ***Scansione in esecuzione*** (*vedere la schermata*). La scansione può essere temporaneamente interrotta (***Sospendi***) oppure annullata (***Annulla***), se necessario.



Modifica della configurazione di scansione

È possibile modificare le impostazioni predefinite di ***Scansione intero computer***. Premere il collegamento ***Modifica impostazioni di scansione*** per accedere alla finestra di dialogo ***Modifica impostazioni di scansione per Scansione intero computer***. ***Si consiglia di mantenere le impostazioni predefinite e di modificarle solo se esiste un reale motivo per farlo.***

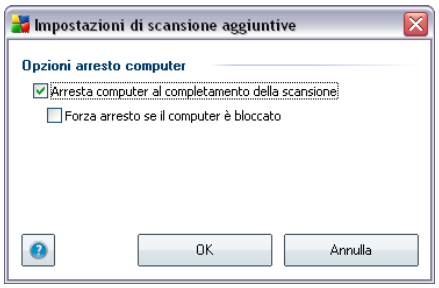


- ***Parametri scansione***: dall'elenco dei parametri di scansione è possibile attivare/disattivare parametri specifici in base alle esigenze. Per impostazione predefinita, la maggior parte dei parametri sono attivati e verranno utilizzati automaticamente durante la scansione.

- ***Priorità processi di scansione***: è possibile utilizzare il dispositivo di scorrimento per modificare la priorità del processo di scansione. Per impostazione predefinita, la priorità è impostata sul livello medio (*Scansione automatica*) per ottimizzare la velocità del processo di scansione e l'utilizzo delle risorse di sistema. In alternativa, è possibile eseguire il processo di scansione in maniera più lenta così da ridurre al minimo il carico delle risorse di sistema (*utile quando si necessita di lavorare al computer ma durata della scansione non influisce*) o più velocemente con maggiori requisiti di risorse di sistema (*ad esempio quando il computer rimane temporaneamente inattivo*).

- ***Imposta rapporti di scansione aggiuntivi***: il collegamento consente di aprire una nuova finestra di dialogo ***Rapporti di scansione*** in cui è possibile selezionare quali tipi di rilevamenti segnalare:

- ***Impostazioni di scansione aggiuntive***: il collegamento consente di aprire una nuova finestra di dialogo ***Opzioni arresto computer*** in cui è possibile decidere se il computer deve essere arrestato automaticamente al termine dell'esecuzione del processo di scansione. Dopo aver confermato questa opzione (***Arresta computer al completamento della scansione***), viene attivata una nuova opzione che consente l'arresto del computer anche se è correntemente bloccato (***Forza arresto se il computer è bloccato***).



Avviso: *queste impostazioni di scansione sono identiche ai parametri di una nuova scansione definita, come descritto nel capitolo* ***Scansione AVG / Pianificazione di scansioni/ Scansione da eseguire****.*

Se si decide di modificare la configurazione predefinita di ***Scansione intero computer*** , è possibile salvare le nuove impostazioni come configurazione predefinita da utilizzare per tutte le altre scansioni dell'intero computer.

14.2.2.Scansione file o cartelle specifiche

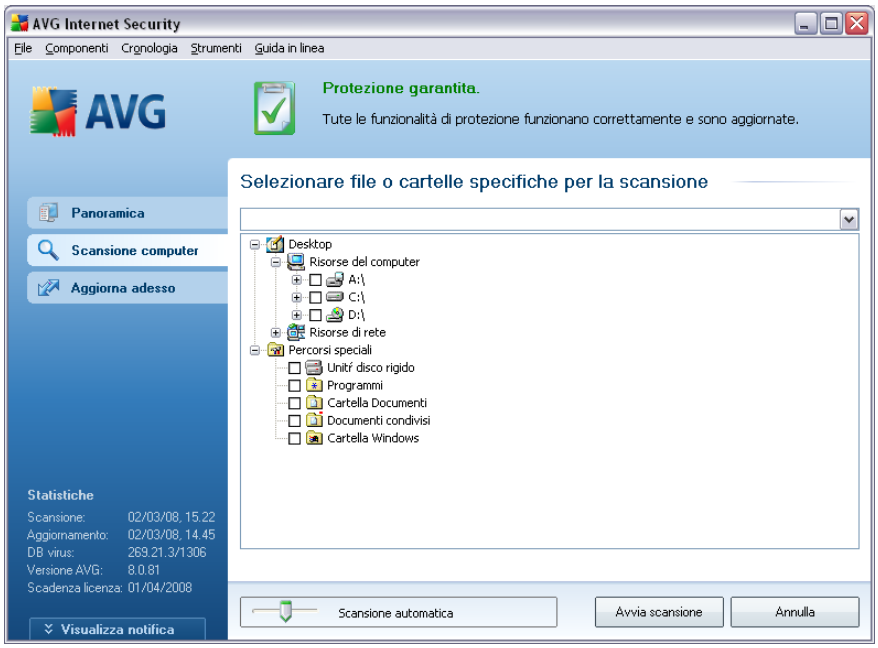
Scansione file o cartelle specifiche: consente di eseguire la scansione solo delle aree del computer selezionate per la scansione (cartelle, dischi rigidi, dischi floppy, CD selezionati e così via). L'avanzamento della scansione nel caso di rilevamento di virus e il relativo trattamento sono gli stessi della scansione dell'intero computer: gli eventuali virus rilevati vengono corretti o rimossi in ***Quarantena virus***. La scansione di file o cartelle specifiche può essere utilizzata per impostare controlli personalizzati e la relativa pianificazione in base alle proprie esigenze.

Avvia scansione

È possibile avviare ***Scansione file o cartelle specifiche*** direttamente dall'interfaccia di scansione facendo clic sull'icona di scansione. Viene aperta una nuova finestra di dialogo ***Selezionare file o cartelle specifiche per la scansione***. Nella struttura del computer selezionare le cartelle che si desidera sottoporre a scansione. Il percorso di ciascuna cartella selezionata verrà generato automaticamente e visualizzato nella casella di testo nella parte superiore della finestra di dialogo.

È possibile sottoporre a scansione una specifica cartella escludendo tutte le sottocartelle relative; a questo scopo scrivere un segno meno "**-**" davanti al percorso generato automaticamente (*vedere la schermata*). Per escludere l'intera cartella dalla scansione, utilizzare il parametro "!".

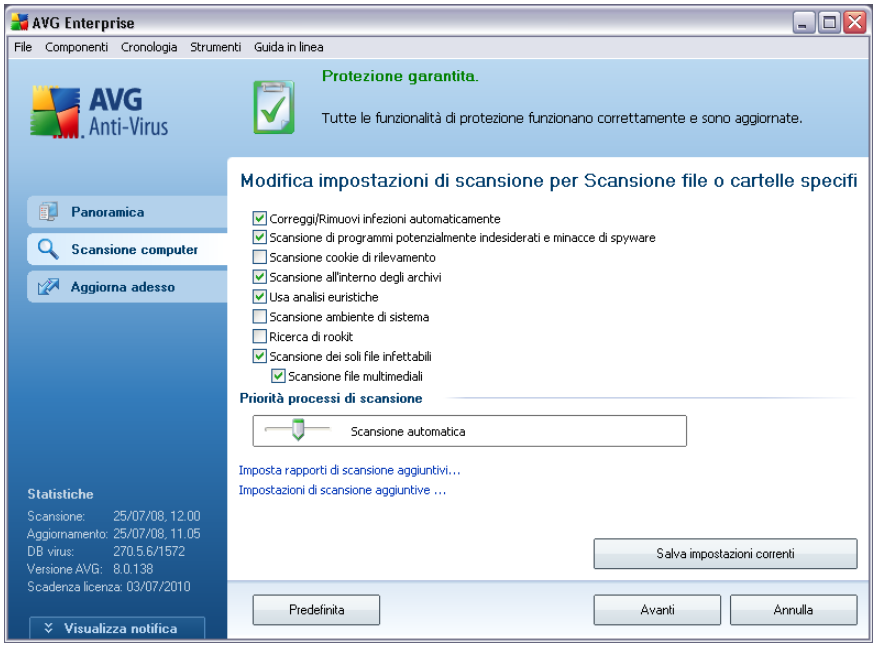
Infine, per avviare la scansione, premere il pulsante ***Avvia scansione*** ; il processo di scansione è praticamente identico a quello della scansione dell'intero computer.



Modifica della configurazione di scansione

È possibile modificare le impostazioni predefinite di ***Scansione file o cartelle specifiche***. Premere il collegamento ***Modifica impostazioni di scansione*** per

accedere alla finestra di dialogo ***Modifica impostazioni di scansione per Scansione file o cartelle specifiche*** . ***Si consiglia di mantenere le impostazioni predefinite e di modificarle solo se esiste un reale motivo per farlo.***

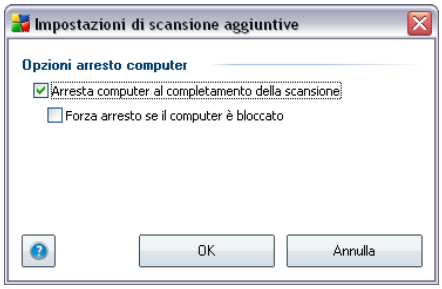


- ***Parametri scansione***: nell'elenco dei parametri di scansione è possibile attivare o disattivare parametri specifici in base alle esigenze (*per una descrizione dettagliata di queste impostazioni, consultare il capitolo Impostazioni AVG avanzate / Scansioni / Scansione file o cartelle specifiche*).

- ***Priorità processi di scansione***: è possibile utilizzare il dispositivo di scorrimento per modificare la priorità del processo di scansione. Per impostazione predefinita, la priorità è impostata sul livello medio (*Scansione automatica*) per ottimizzare la velocità del processo di scansione e l'utilizzo delle risorse di sistema. In alternativa, è possibile eseguire il processo di scansione in maniera più lenta così da ridurre al minimo il carico delle risorse di sistema (*utile quando si necessita di lavorare al computer ma durata della scansione non influisce*) o più velocemente con maggiori requisiti di risorse di sistema (*ad esempio quando il computer rimane temporaneamente inattivo*).

- ***Imposta rapporti di scansione aggiuntivi***: il collegamento consente di aprire una nuova finestra di dialogo ***Rapporti di scansione*** in cui è possibile selezionare quali tipi di rilevamenti segnalare:

- ***Impostazioni di scansione aggiuntive***: il collegamento consente di aprire una nuova finestra di dialogo ***Opzioni arresto computer*** in cui è possibile decidere se il computer deve essere arrestato automaticamente al termine dell'esecuzione del processo di scansione. Dopo aver confermato questa opzione (***Arresta computer al completamento della scansione***), viene attivata una nuova opzione che consente l'arresto del computer anche se è correntemente bloccato (***Forza arresto se il computer è bloccato***).



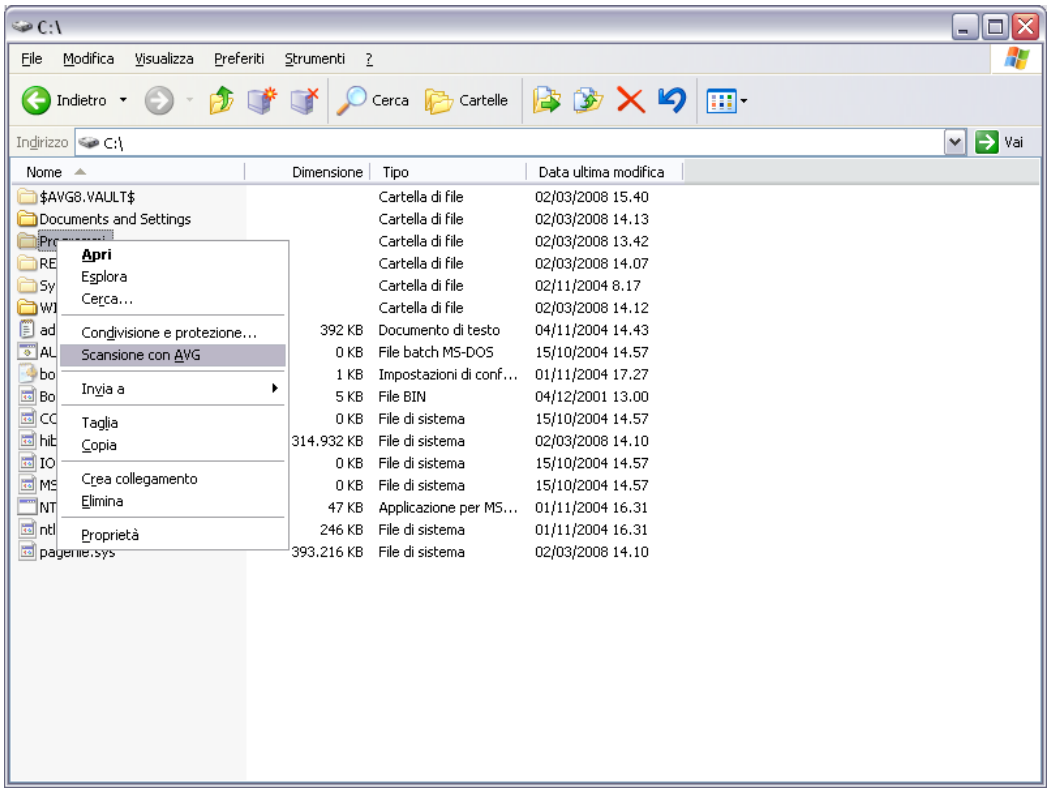
Avviso: *queste impostazioni di scansione sono identiche ai parametri di una nuova scansione definita, come descritto nel capitolo* ***Scansione AVG / Pianificazione di scansioni/ Scansione da eseguire****.*

Se si decide di modificare la configurazione predefinita di ***Scansione file o cartelle specifiche*** è possibile salvare la nuova impostazione come configurazione predefinita da utilizzare per tutte le altre scansioni di file o cartelle specifiche. Inoltre, questa configurazione verrà utilizzata come modello per tutte le nuove scansioni pianificate (*tutte le scansioni personalizzate si basano sulla configurazione corrente di Scansione file o cartelle specifiche*).

14.3.Scansione in Esplora risorse

Oltre alle scansioni predefinite avviate per l'intero computer o per le aree selezionate, AVG offre l'opzione di una scansione rapida di un oggetto specifico direttamente nell'ambiente Esplora risorse. Se si desidera aprire un file sconosciuto e non si è sicuri del contenuto, è possibile decidere di eseguire un controllo su richiesta. Procedere

come segue:



- In Esplora risorse evidenziare il file o la cartella che si desidera verificare
- Fare clic con il pulsante destro del mouse sull'oggetto per aprire il menu di scelta rapida
- Selezionare l'opzione ***Scansione con AVG*** per eseguire la scansione con AVG

14.4.Scansione riga di comando

In **AVG 8.5 Internet Security** è disponibile un'opzione che consente di eseguire la scansione dalla riga di comando. Ad esempio, è possibile utilizzare questa opzione su server oppure durante la creazione di uno script batch da avviare automaticamente dopo l'avvio del computer. Dalla riga di comando, è possibile avviare la scansione mentre nell'interfaccia grafica di AVG viene fornita la maggior parte dei parametri.

Per avviare la scansione di AVG dalla riga di comando, eseguire il seguente comando dalla cartella in cui è stato installato AVG:

- ***avgscanx*** per sistemi operativi a 32 bit
- ***avgscana*** per sistemi operativi a 64 bit

Sintassi del comando

La sintassi del comando è la seguente:

- ***avgscanx /parameter*** ... ad esempio ***avgscanx /comp*** per la scansione dell'intero computer
- ***avgscanx /parameter /parameter*** .. nel caso di più parametri, questi dovrebbero essere allineati in una riga e separati da uno spazio e dal carattere della barra (/)
- se per un parametro è necessario fornire un valore specifico (ad esempio, il parametro ***/scan*** richiede informazioni relative alle aree nel computer delle quali eseguire la scansione ed è necessario fornire il percorso esatto della sezione selezionata), i valori vengono separati da virgole. Ad esempio: ***avgscanx /scan=C:\,D:***

Parametri scansione

Per visualizzare una panoramica completa dei parametri disponibili, digitare il rispettivo comando insieme al parametro /? o /HELP (ad esempio ***avgscanx /?***). Nota: l'unico parametro obbligatorio è /SCAN, che consente di specificare quali aree del computer devono essere sottoposte a scansione. Per spiegazioni più dettagliate delle opzioni, vedere panoramica parametri riga di comando.

Per eseguire la scansione, premere ***INVIO***. Durante la scansione è possibile arrestare il processo premendo ***CTRL+C*** oppure ***CTRL+PAUSA***.

Scansione CMD avviata dall'interfaccia grafica

Quando viene eseguita la modalità provvisoria di Windows, è inoltre possibile avviare la scansione da riga di comando dall'interfaccia utente grafica. La scansione verrà avviata dalla riga di comando. La finestra di dialogo ***Compositore riga di comando*** consente solo di specificare la maggior parte dei parametri di scansione nella comoda interfaccia grafica.

Poiché questa finestra di dialogo è accessibile solo nella modalità provvisoria di

Windows, per ulteriori informazioni consultare il file della Guida aperto direttamente dalla finestra di dialogo.

14.4.1.Parametri scansione CMD

Di seguito viene fornito un elenco di tutti i parametri disponibili per la scansione dalla riga di comando:

- ***/SCAN*** Scansione file o cartelle specifiche /SCAN=percorso; percorso (ad esempio /SCAN=C:\;D:\)
- ***/COMP*** Scansione computer intero
- ***/HEUR*** Usa analisi euristica
- ***/EXCLUDE*** Escludi percorso o file dalla scansione
- ***/@*** File di comando /nome file/
- ***/EXT*** Esegui scansione su queste estensioni /ad esempio EXT=EXE,DLL/
- ***/NOEXT*** Non eseguire scansione su queste estensioni /ad esempio NOEXT=JPG/
- ***/ARC*** Esegui scansione su archivi
- ***/CLEAN*** Pulisci automaticamente
- ***/TRASH*** Sposta file infetti in Quarantena virus
- ***/QT*** Controllo rapido
- ***/MACROW*** Segnala macro
- ***/PWDW*** Rapporto sui file protetti da password
- ***/IGNLOCKED*** Ignora file bloccati
- ***/REPORT*** Rapporto sul file /nome file/
- ***/REPAPPEND*** Allega al file rapporto
- ***/REPOK*** Segnala file non infetti come OK

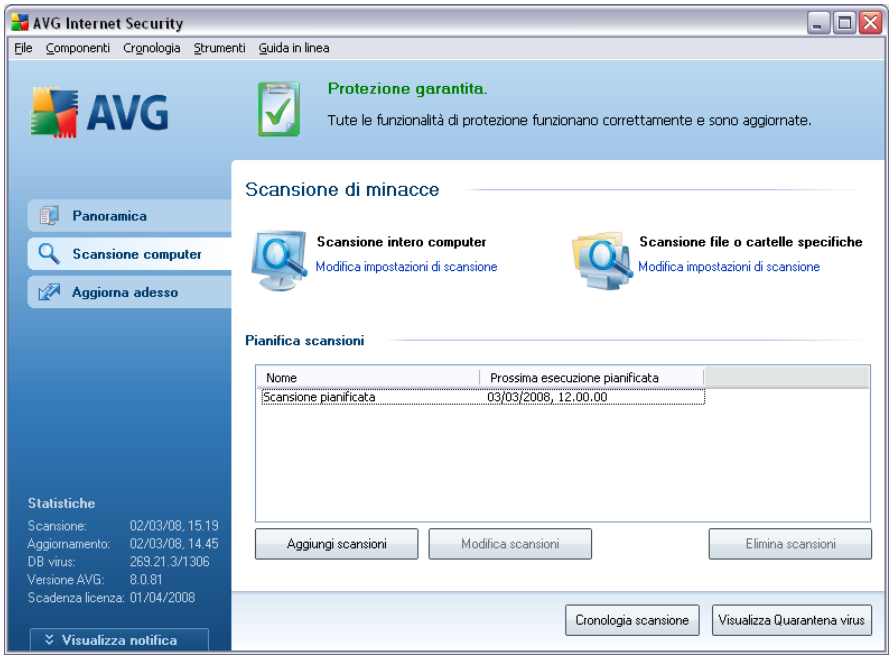
- ***/NOBREAK*** Non consentire interruzione CTRL-BREAK
- ***/BOOT*** Abilita controllo MBR/BOOT
- ***/PROC*** Scansione dei processi attivi
- ***/PUP*** Segnala "Programmi potenzialmente indesiderati"
- ***/REG*** Scansione Registro di sistema
- ***/COO*** Esegui scansione dei cookie
- ***/?*** Visualizza la Guida sull'argomento
- ***/HELP*** Visualizza la Guida sull'argomento
- ***/PRIORITY*** Imposta priorità scansione /Bassa, Automatica, Elevata/ (vedere Impostazioni avanzate / Scansioni)
- ***/SHUTDOWN*** Arresta computer al completamento della scansione
- ***/FORCESHUTDOWN*** Forza arresto del computer al completamento della scansione
- ***/ADS*** Esegui scansione flussi di dati alternativi (solo NTFS)

14.5.Pianificazione di scansioni

AVG 8.5 Internet Security consente di eseguire una scansione su richiesta (ad esempio quando si sospetta che un'infezione sia stata trasferita nel computer) oppure in base a una pianificazione. Si consiglia di eseguire le scansioni in base a una pianificazione: in questo modo ci si assicura che il computer rimane protetto da possibili infezioni e non è necessario preoccuparsi dell'avvio della scansione.

Si consiglia di avviare ***Scansione intero computer*** su base regolare, almeno una volta alla settimana. Tuttavia, se possibile, avviare la scansione dell'intero computer ogni giorno, come impostato nella configurazione predefinita della pianificazione della scansione. Se il computer è sempre acceso, è possibile pianificare le scansioni fuori dagli orari di lavoro. Se il computer rimane a volte spento, è possibile pianificare l'esecuzione delle scansioni all'avvio del computer, nel caso in cui l'attività non sia stata eseguita.

Per creare nuove pianificazioni di scansioni, vedere l'interfaccia di scansione di AVG e individuare la sezione inferiore denominata ***Pianificazione scansioni***:



Pulsanti di controllo per la pianificazione delle scansioni

All'interno della sezione di modifica sono disponibili i seguenti pulsanti di controllo:

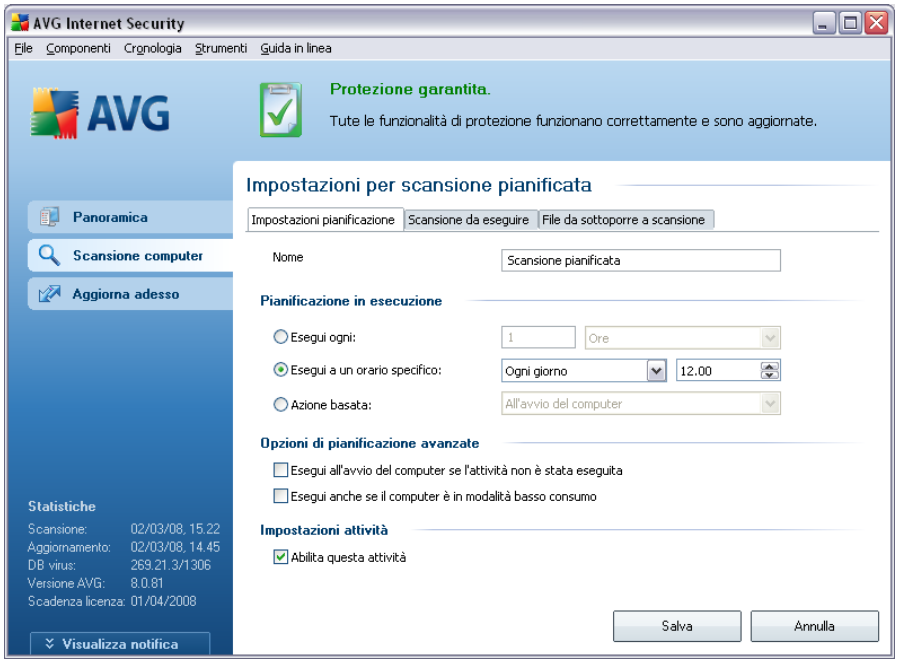
- ***Aggiungi pianificazione scansione***: il pulsante consente di aprire la finestra di dialogo ***Impostazioni per scansione pianificata*** , scheda ***Impostazioni pianificazione***. In questa finestra di dialogo è possibile specificare i parametri del nuovo controllo definito.

- ***Modifica pianificazione scansione***: il pulsante può essere utilizzato solo se è stato selezionato in precedenza un controllo esistente dall'elenco dei controlli pianificati. In tal caso il pulsante è visualizzato come attivo e, premendolo, si passa alla finestra di dialogo ***Impostazioni per scansione pianificata*** , scheda ***Impostazioni pianificazione***. I parametri del controllo selezionato sono già specificati in questa sezione e possono essere modificati.

- ***Elimina pianificazione scansione***: questo pulsante è attivo anche se è stato selezionato in precedenza un controllo esistente dall'elenco dei controlli pianificati. È possibile eliminare il controllo dall'elenco premendo il pulsante di controllo. Tuttavia, è possibile rimuovere solo i controlli personali; non è possibile eliminare ***Pianificazione scansione intero computer*** predefinita all'interno delle impostazioni predefinite.

14.5.1.Impostazioni pianificazione

Se si desidera pianificare un nuovo controllo e il relativo avvio regolare, accedere alla finestra di dialogo ***Impostazioni per il controllo pianificato***. La finestra di dialogo è suddivisa in tre schede: ***Impostazioni pianificazione*** - *vedere l'immagine in basso* (la scheda predefinita cui si viene automaticamente reindirizzati), ***Scansione da eseguire*** e ***File da sottoporre a scansione***.



Nella scheda ***Impostazioni attività*** è possibile selezionare/deselezionare la voce ***Abilita questa attività*** per disattivare temporaneamente il controllo pianificato e riattivarlo secondo le necessità.

Quindi, assegnare un nome alla scansione da creare e pianificare. Digitare il nome nel campo di testo dalla voce ***Nome***. Provare a denominare le scansioni assegnando nomi brevi, descrittivi e appropriati per poterle riconoscere più facilmente in futuro.

Esempio: *non è appropriato denominare una scansione "Nuova scansione" o "Scansione personale" poiché questi nomi non fanno riferimento agli elementi sottoposti a scansione. Un esempio di un buon nome descrittivo potrebbe essere "Scansione aree di sistema" e così via. Inoltre, non è necessario specificare nel nome della scansione se si tratta di una scansione dell'intero computer oppure relativa solo ai file o alle cartelle selezionati. Le scansioni saranno sempre una versione specifica della scansione dei file e delle cartelle sellezionati.*

In questa finestra di dialogo è possibile definire ulteriormente i seguenti parametri della scansione:

- ***Pianificazione in esecuzione***: consente di specificare gli intervalli di tempo per l'avvio della nuova scansione pianificata. È possibile definire l'ora dall'avvio ripetuto della scansione dopo un certo periodo di tempo (***Esegui ogni...***) o definendo data e ora esatte (***Esegui a un orario specifico...***) oppure definendo un evento a cui dovrà essere associato l'avvio della scansione (***Azione in base all'avvio del computer***).

- ***Opzioni di pianificazione avanzate***: questa sezione consente di definire le circostanze in cui deve essere avviata o non avviata la scansione se il computer si trova in modalità basso consumo oppure se è completamente spento.

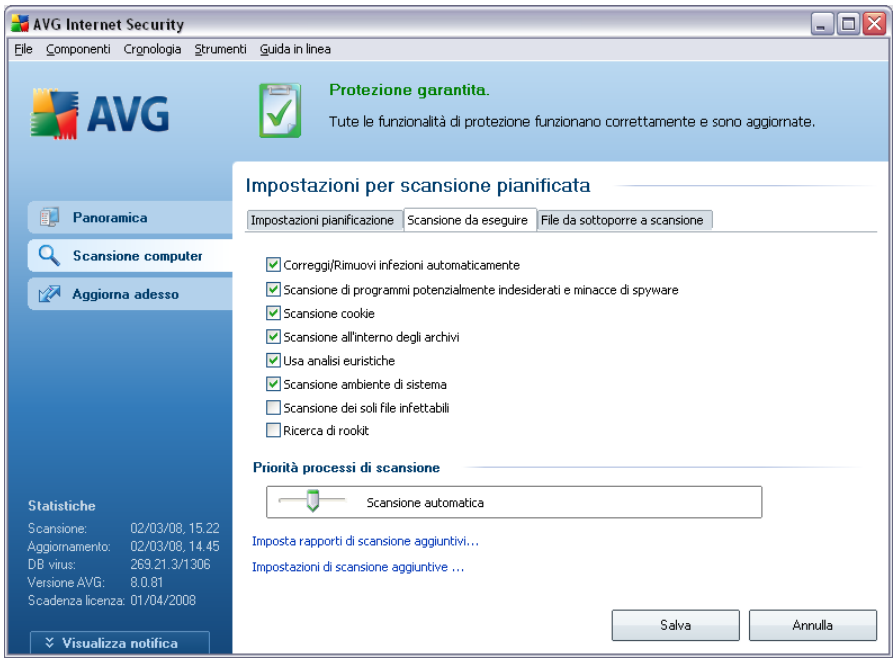
Pulsanti di controllo delle impostazioni per la finestra di dialogo della scansione pianificata

Sono disponibili due pulsanti di controllo sulle tre schede della finestra di dialogo ***Impostazioni per scansione pianificata*** (***Impostazioni pianificazione***, ***Scansione da eseguire*** e ***File da sottoporre a scansione***) e tutte hanno la stessa funzionalità indipendentemente dalla scheda visualizzata:

- ***Salva***: consente di salvare tutte le modifiche eseguite su questa scheda o su un'altra scheda della finestra di dialogo e di tornare alla finestra di dialogo predefinita dell'interfaccia di scansione di AVG. Pertanto, se si desidera configurare i parametri di controllo di tutte le schede, premere il pulsante per salvarli solo dopo aver specificato tutti i requisiti desiderati.

- ***Annulla***: consente di annullare le eventuali modifiche eseguite sulla scheda o su un'altra scheda della finestra di dialogo e di tornare alla finestra di dialogo predefinita dell'interfaccia di scansione di AVG.

14.5.2.Scansione da eseguire



Nella scheda ***Scansione da eseguire*** è presente un elenco di parametri che possono essere attivati o disattivati facoltativamente. Per impostazione predefinita, la maggior parte dei parametri è attivata e la funzionalità verrà applicata durante la scansione. A meno che ci sia una ragione valida per modificare le impostazioni, si consiglia di mantenere la configurazione predefinita:

- ***Correggi/Rimuovi infezioni automaticamente*** : (*attivata per impostazione predefinita*) se viene identificato un virus durante la scansione, può essere corretto automaticamente, se è disponibile una soluzione. Se il file infetto non può essere corretto automaticamente o se si decide di disattivare questa opzione, si riceverà un messaggio di notifica sulla presenza di un virus e si dovrà decidere l'azione da intraprendere sull'infezione rilevata. L'azione consigliata è quella di rimuovere il file infetto in Quarantena virus.

- ***Scansione di programmi potenzialmente indesiderati*** : (*attivata per impostazione predefinita*): questo parametro controlla la funzionalità Antivirus che consente il rilevamento di programmi potenzialmente indesiderati (*file eseguibili che possono essere eseguiti come spyware o adware*) e che possono essere bloccati o rimossi;

- ***Scansione cookie di rilevamento*** (*attivata per impostazione predefinita*): questo parametro del componente Anti-Spyware stabilisce che i cookie devono

essere rilevati durante la scansione (*i cookie HTTP vengono utilizzati per autenticare, rilevare e mantenere informazioni specifiche sugli utenti, quali le preferenze dei siti e il contenuto dei carrelli elettronici*);

- ***Scansione all'interno degli archivi*** : (*attivata per impostazione predefinita*): questo parametro stabilisce che la scansione deve controllare tutti i file anche se inclusi all'interno di un tipo di archivio, quale ZIP, RAR e così via.

- ***Usa analisi euristiche*** : (*attivata per impostazione predefinita*): analisi euristica (*emulazione dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale*) che sarà uno dei metodi utilizzati per il rilevamento di virus durante la scansione;

- ***Scansione ambiente di sistema*** : (*attivata per impostazione predefinita*): la scansione verrà eseguita anche sulle aree di sistema del computer;

- ***Ricerca di rootkit***: selezionare questa voce per includere il rilevamento dei rootkit nella scansione dell'intero computer. Il rilevamento dei rootkit è disponibile anche da solo all'interno del componente ***Anti-Rootkit***;

    - ***Scansione dei soli file infettabili*** : (*disattivata per impostazione predefinita*): se l'opzione è attivata, la scansione non verrà applicata ai file che non possono essere infettabili. Può trattarsi ad esempio di alcuni file di testo normale o di altri file non eseguibili.

All'interno della sezione ***Priorità processi di scansione*** è inoltre possibile specificare la velocità di scansione desiderata in base all'utilizzo delle risorse di sistema. Per impostazione predefinita, il valore di questa opzione è impostato sul livello medio di utilizzo automatico delle risorse. Se si desidera aumentare la velocità della scansione, il tempo che impiegherà sarà inferiore ma l'utilizzo delle risorse di sistema aumenterà notevolmente durante l'esecuzione e rallenterà le altre attività sul PC (*questa opzione può essere utilizzata quando il computer è acceso ma non è utilizzato*). Tuttavia, è possibile diminuire l'utilizzo delle risorse di sistema aumentando la durata della scansione.

Nota: *per impostazione predefinita, la configurazione della scansione è impostata per garantire prestazioni ottimali. A meno che non ci sia una ragione valida per modificare l'impostazione della scansione, si consiglia di mantenere la configurazione predefinita. Solo gli utenti esperti dovrebbero apportare eventuali modifiche alla configurazione. Per ulteriori opzioni sulla configurazione della scansione vedere la finestra di dialogo* ***Impostazioni avanzate*** *accessibile dalla voce di menu di sistema* ***File / Impostazioni avanzate****.*

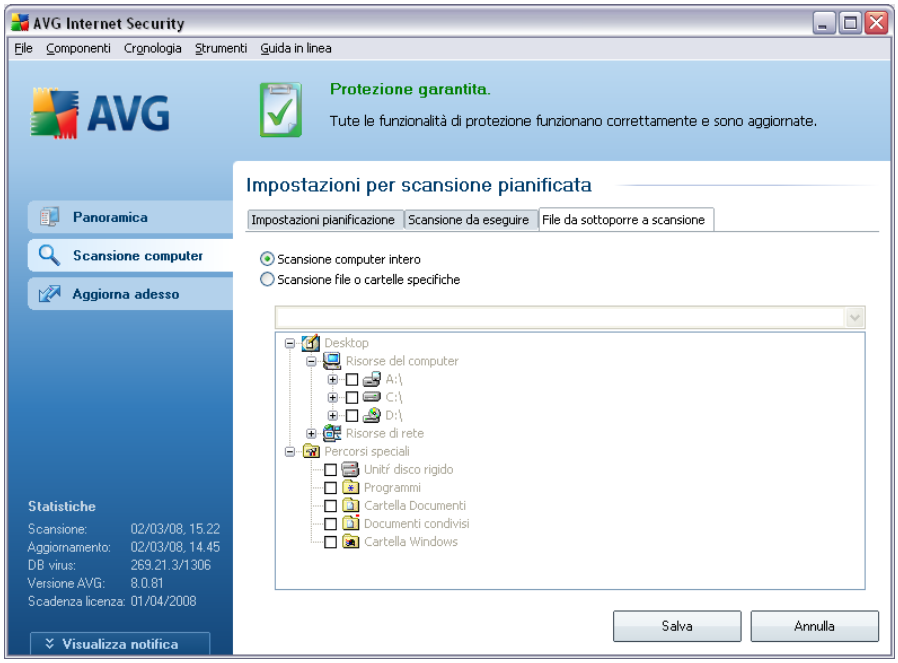
Pulsanti di controllo delle impostazioni per la finestra di dialogo della scansione pianificata

Sono disponibili due pulsanti di controllo sulle tre schede della finestra di dialogo ***Impostazioni per scansione pianificata*** (***Impostazioni pianificazione***, ***Scansione da eseguire*** e ***File da sottoporre a scansione***) e tutte hanno la stessa funzionalità indipendentemente dalla scheda visualizzata:

- ***Salva***: consente di salvare tutte le modifiche eseguite su questa scheda o su un'altra scheda della finestra di dialogo e di tornare alla finestra di dialogo predefinita dell'interfaccia di scansione di AVG. Pertanto, se si desidera configurare i parametri di controllo di tutte le schede, premere il pulsante per salvarli solo dopo aver specificato tutti i requisiti desiderati.

- ***Annulla***: consente di annullare le eventuali modifiche eseguite sulla scheda o su un'altra scheda della finestra di dialogo e di tornare alla finestra di dialogo predefinita dell'interfaccia di scansione di AVG.

14.5.3.File da sottoporre a scansione



Nella scheda ***File da sottoporre a scansione*** è possibile definire se si desidera pianificare la scansione dell'intero computer o la scansione di file o cartelle specifiche.

Se si seleziona la scansione di file o cartelle specifiche, nella parte inferiore di questa finestra di dialogo viene attivata la struttura visualizzata che consente di specificare le cartelle da sottoporre a scansione.

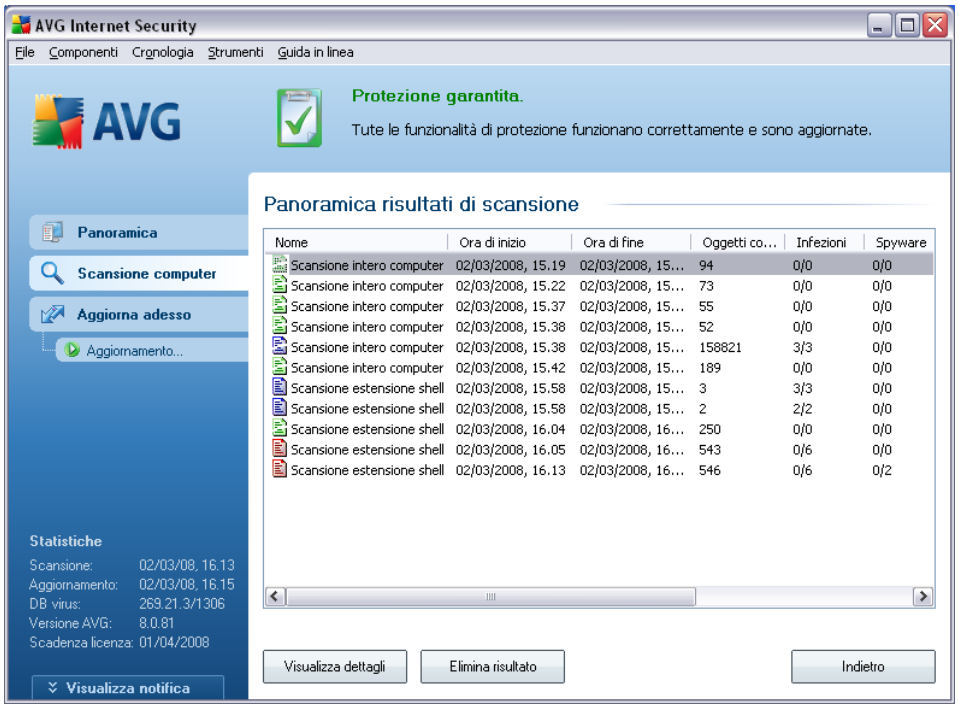
Pulsanti di controllo delle impostazioni per la finestra di dialogo della scansione pianificata

Sono disponibili due pulsanti di controllo sulle tre schede della finestra di dialogo ***Impostazioni per scansione pianificata*** (***Impostazioni pianificazione***, ***Scansione da eseguire*** e ***File da sottoporre a scansione***) e tutte hanno la stessa funzionalità indipendentemente dalla scheda visualizzata:

- ***Salva***: consente di salvare tutte le modifiche eseguite su questa scheda o su un'altra scheda della finestra di dialogo e di tornare alla finestra di dialogo predefinita dell'interfaccia di scansione di AVG. Pertanto, se si desidera configurare i parametri di controllo di tutte le schede, premere il pulsante per salvarli solo dopo aver specificato tutti i requisiti desiderati.

- ***Annulla***: consente di annullare le eventuali modifiche eseguite sulla scheda o su un'altra scheda della finestra di dialogo e di tornare alla finestra di dialogo predefinita dell'interfaccia di scansione di AVG.

14.6.Panoramica di Risultati scansione



La finestra di dialogo ***Panoramica risultati di scansione*** è accessibile dall' interfaccia di scansione di AVG tramite il pulsante ***Cronologia scansione***. Nella finestra di dialogo è contenuto l'elenco di tutte le scansioni avviate in precedenza e le informazoni dei risultati relativi:

- ***Nome***: nome della scansione; può essere il nome di una delle scansioni predefinite o il nome assegnato alla propria scansione pianificata. Ciascun nome include un'icona che indica i risultati della scansione:

  - il colore verde indica che non è stata rilevata alcuna infezione durante la scansione

  - il colore blu indica che è stata rilevata un'infezione durante la scansione ma l'oggetto infetto è stato rimosso automaticamente

  - il colore rosso indica che è stata rilevata un'infezione durante la scansione ma non è stato possibile rimuoverla.

  Ciascuna icona può essere intera o suddivisa in due parti: l'icona intera

indica una scansione completata correttamente, l'icona suddivisa in due indica una scansione annullata o interrotta.

Nota: *per informazioni dettagliate su ciascuna icona vedere la finestra di dialogo* ***Risultati scansione*** *accessibile tramite il pulsante* ***Visualizza dettagli*** *(nella parte inferiore della finestra di dialogo).*

- ***Ora di inizio***: data e ora di avvio della scansione
- ***Ora di fine***: data e ora del completamento della scansione
- ***Oggetti controllati***: numero di oggetti controllati durante la scansione
- ***Infezioni***: numero delle infezioni da virus rilevate / rimosse
- ***Spyware*** : numero di spyware rilevato / rimosso
- ***Informazioni registro di scansione***: informazioni relative all'andamento e al risultato della scansione (in genere in relazione alla finalizzazione o all'interruzione)

Pulsanti di controllo

I pulsanti di controllo per la finestra di dialogo ***Panoramica risultati di scansione*** sono i seguenti:

- ***Visualizza dettagli***: questo pulsante è attivo solo se è stata selezionata una scansione specifica nella panoramica in alto; premere il pulsante per passare alla finestra di dialogo ***Risultati scansione*** per visualizzare i dati dettagliati sulla scansione selezionata
- ***Elimina risultati***: questo pulsante è attivo solo se è stata selezionata una scansione specifica nella panoramica in alto; premere il pulsante per rimuovere la voce selezionata per la panoramica deir isultati di scansione
- ***Indietro***: consente di tornare alla finestra di dialogo predefinita dell'interfaccia di scansione di AVG

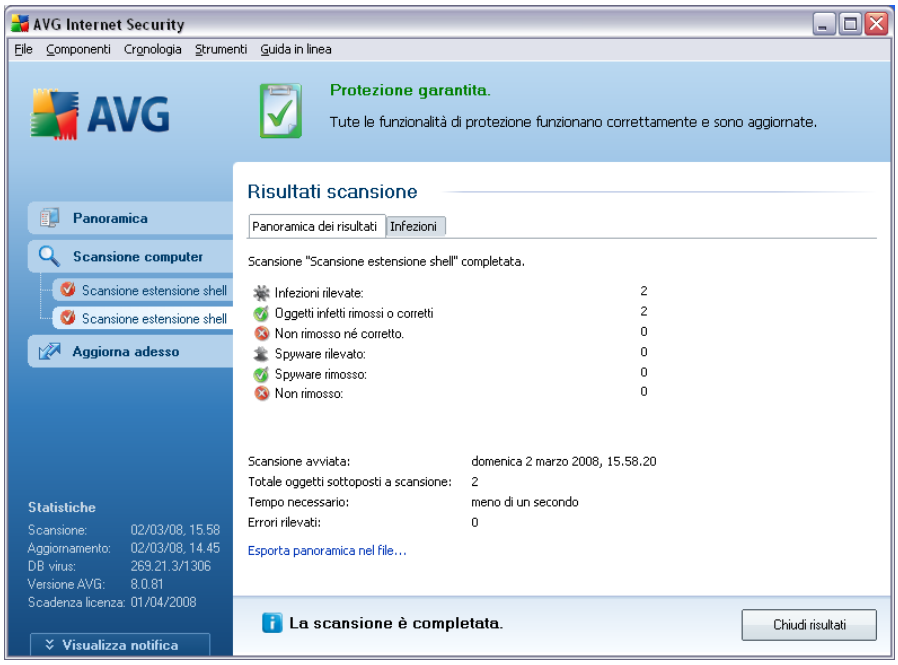
14.7.Dettagli di Risultati scansione

Se nella finestra di dialogo ***Panoramica risultati di scansione*** è selezionata una scansione specifica, è possibile fare clic sul pulsante ***Visualizza dettagli*** per passare alla finestra di dialogo ***Risultati scansione*** che contiene i dati dettagliati sul corso e sui risultati della scansione selezionata.

La finestra di dialogo è suddivisa in altre schede:

- ***Panoramica dei risultati***: questa scheda viene visualizzata tutte le volte e fornisce i dati statistici che descrivono l'avanzamento della scansione
- ***Infezioni***: questa scheda viene visualizzata solo se durante la scansione è stata rilevata un'infezione da virus
- ***Spyware***: questa scheda viene visualizzata solo se durante la scansione è stato rilevato spyware
- ***Avvisi***: questa scheda viene visualizzata solo se durante la scansione sono stati rilevati oggetti che è stato possibile sottoporre a scansione
- ***Rootkit***: questa scheda viene visualizzata solo se durante la scansione sono stati rilevati rootkit
- ***Informazioni:*** questa scheda viene visualizzata solo se sono state rilevate alcune potenziali minacce non classificabili in nessuna delle categorie suddette; nella scheda viene visualizzato un messaggio di avviso sul rilevamento

14.7.1.Scheda Panoramica dei risultati



Nella scheda ***Risultati scansione*** sono contenuti i dettagli delle statistiche con informazioni in relazione a:

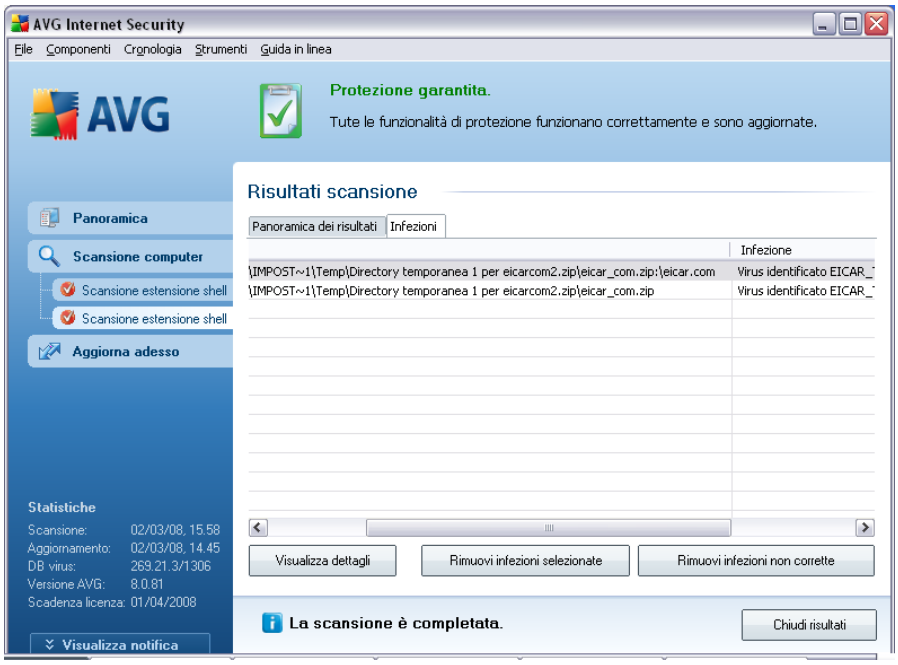
- infezioni da virus / spyware rilevate
- infezioni da virus / spyware rimosse
- numero di infezioni da virus / spyware che non è possibile rimuovere o correggere

Inoltre, sono contenute informazioni sulla data e sull'ora esatte di avvio della scansione, sul numero totale di oggetti sottoposti a scansione, sulla durata della scansione e sul numero di errori che si sono verificati durante la scansione.

Pulsanti di controllo

In questa finestra di dialogo è disponibile solo un pulsante di controllo. Il pulsante ***Chiudi risultati*** consente di tornare alla finestra di dialogo ***Panoramica risultati di scansione***.

14.7.2.Scheda Infezioni



La scheda ***Infezioni*** viene visualizzata solo nella finestra di dialogo ***Risultati scansione*** se è stata rilevata un'infezione da virus durante la scansione. La scheda è suddivisa in tre sezioni in cui sono contenute le seguenti informazioni:

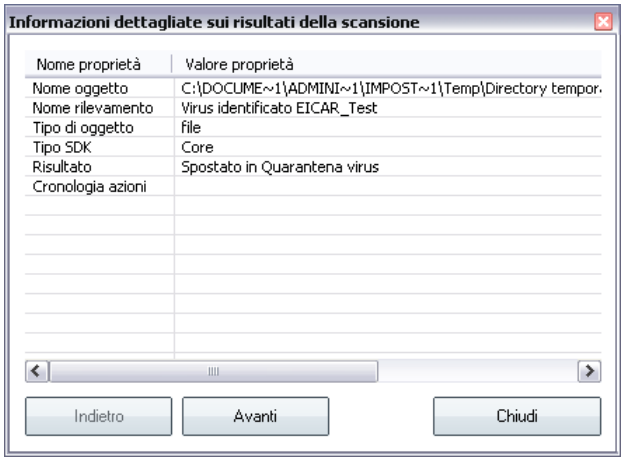
- ***File***: percorso completo della posizione originale dell'oggetto infetto
- ***Infezioni***: nome del virus rilevato (*per informazioni dettagliate su virus specifici, consultare l'Enciclopedia dei virus in linea*)
- ***Risultato***: definisce lo stato corrente dell'oggetto infetto rilevato durante la scansione:
    - ***Infetto***: l'oggetto infetto è stato rilevato e lasciato nella sua posizione originale (*ad esempio, se è stata disattivata l'opzione di correzione automatica nelle impostazioni di una scansione specifica*)
    - ***Corretto***: l'oggetto infetto è stato corretto automaticamente e lasciato nella sua posizione originale
    - ***Spostato/i in Quarantena virus***: l'oggetto infetto è stato spostato in ***Quarantena virus***

- ***Eliminato***: l'oggetto infetto è stato eliminato
- ***Aggiunto alle eccezioni PUP***: l'oggetto rilevato è stato classificato come eccezione ed è stato aggiunto all'elenco delle eccezioni PUP (*configurato nella finestra di dialogo* ***Eccezioni PUP*** *delle impostazioni avanzate*)
- ***File bloccato: non verificato*** - l'oggetto corrispondente è stato bloccato ma AVG non è in grado di sottoporlo a scansione
- ***Oggetto potenzialmente pericoloso***: l'oggetto è stato rilevato come potenzialmente pericoloso ma non infetto (*potrebbe contenere macro, ad esempio*); l'informazione deve essere considerata solo come un avviso
- ***È necessario riavviare il computer per concludere l'operazione***: non è possibile rimuovere l'oggetto infetto. Per rimuoverlo definitivamente, è necessario riavviare il computer

Pulsanti di controllo

Sono disponibili tre pulsanti di controllo in questa finestra di dialogo:

- ***Visualizza dettagli*** : il pulsante consente di aprire una nuova finestra di dialogo denominata ***Informazioni dettagliate sui risultati della scansione*** :

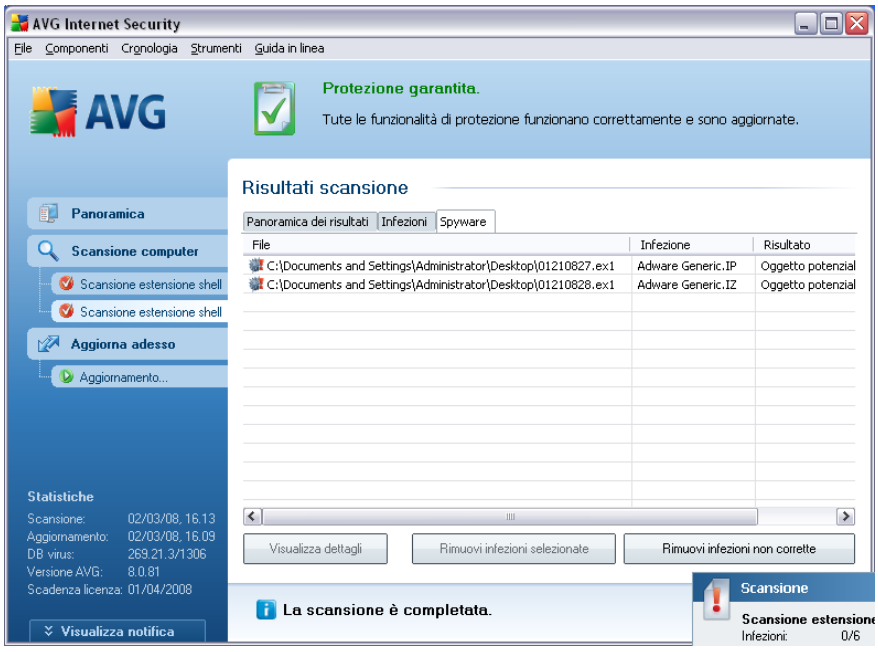


In questa finestra di dialogo sono contenute informazioni relative alla posizione dell'oggetto infetto rilevato (***Nome proprietà***). I pulsanti

Indietro / ***Avanti*** consentono di visualizzare le informazioni su specifici oggetti rilevati. Utilizzare il pulsante ***Chiudi*** per chiudere questa finestra di dialogo.

- ***Rimuovi infezioni selezionate***: utilizzare il pulsante per spostare l'oggetto rilevato selezionato in ***Quarantena virus***
- ***Rimuovi tutte le infezioni non corrette***: questo pulsante consente di eliminare tutti gli oggetti rilevati che non possono essere corretti o spostati in ***Quarantena virus***
- ***Chiudi risultati***: consente di uscire dalla panoramica delle informazioni dettagliate e di tornare alla finestra di dialogo ***Panoramica risultati di scansione***

14.7.3.Scheda Spyware



La scheda ***Spyware*** è visualizzata nella finestra di dialogo ***Risultati scansione*** solo se durante la scansione è stato rilevato spyware. La scheda è suddivisa in tre sezioni in cui sono contenute le seguenti informazioni:

- ***File***: percorso completo della posizione originale dell'oggetto infetto
- ***Infezioni*** : nome dello spyware rilevato (*per informazioni dettagliate su virus*

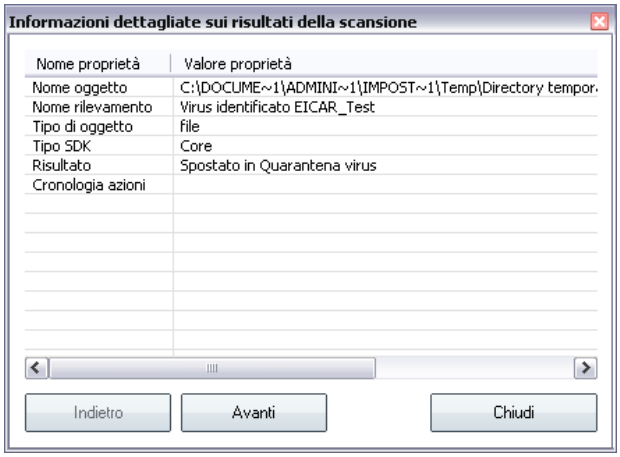
*specifici, consultare l'**Enciclopedia dei virus** in linea*)

- ***Risultato***: definisce lo stato corrente dell'oggetto infetto rilevato durante la scansione:
    - ***Infetto***: l'oggetto infetto è stato rilevato e lasciato nella sua posizione originale (ad esempio, se è stata disattivata l'opzione di correzione automatica nelle impostazioni di una scansione specifica)
    - ***Corretto***: l'oggetto infetto è stato corretto automaticamente e lasciato nella sua posizione originale
    - ***Spostato in Quarantena virus***: l'oggetto infetto è stato spostato in ***Quarantena virus***
    - ***Eliminato***: l'oggetto infetto è stato eliminato
    - ***Aggiunto alle eccezioni PUP***: l'oggetto rilevato è stato classificato come eccezione ed è stato aggiunto all'elenco delle eccezioni PUP (*configurato nella finestra di dialogo **Eccezioni PUP** delle impostazioni avanzate*).
    - ***File bloccato: non verificato*** : l'oggetto corrispondente è stato bloccato ma AVG non è in grado di sottoporlo a scansione
    - ***Oggetto potenzialmente pericoloso***: l'oggetto è stato rilevato come potenzialmente pericoloso ma non infetto (potrebbe contenere macro, ad esempio); l'informazione deve essere considerata solo come un avviso
    - ***È necessario riavviare il computer per concludere l'operazione***: non è possibile rimuovere l'oggetto infetto. Per rimuoverlo definitivamente, è necessario riavviare il computer

Pulsanti di controllo

Sono disponibili tre pulsanti di controllo in questa finestra di dialogo:

- ***Visualizza dettagli***: il pulsante consente di aprire una nuova finestra di dialogo denominata ***Informazioni dettagliate sui risultati della scansione*** :



In questa finestra di dialogo sono contenute informazioni relative alla posizione dell'oggetto infetto rilevato (***Nome proprietà***). I pulsanti ***Indietro*** / ***Avanti*** consentono di visualizzare le informazioni su specifici oggetti rilevati. Utilizzare il pulsante ***Chiudi*** per uscire da questa finestra di dialogo.

- ***Rimuovi infezioni selezionate***: utilizzare il pulsante per spostare l'oggetto rilevato selezionato in ***Quarantena virus***
- ***Rimuovi tutte le infezioni non corrette***: questo pulsante consente di eliminare tutti gli oggetti rilevati che non possono essere corretti o spostati in ***Quarantena virus***
- ***Chiudi risultati***: consente di uscire dalla panoramica delle informazioni dettagliate e di tornare alla finestra di dialogo ***Panoramica risultati di scansione***

14.7.4.Scheda Avvisi

La scheda ***Avvisi*** consente di visualizzare le informazioni relative agli oggetti "sospetti" (*file, generalmente*) rilevati durante la scansione. Quando vengono rilevati da ***Resident Shield***, viene bloccato l'accesso a questi file. Esempi tipici di questo tipo di rilevamenti sono: file nascosti, cookie, chiavi del Registro di sistema sospette, archivi o documenti protetti da password e così via.

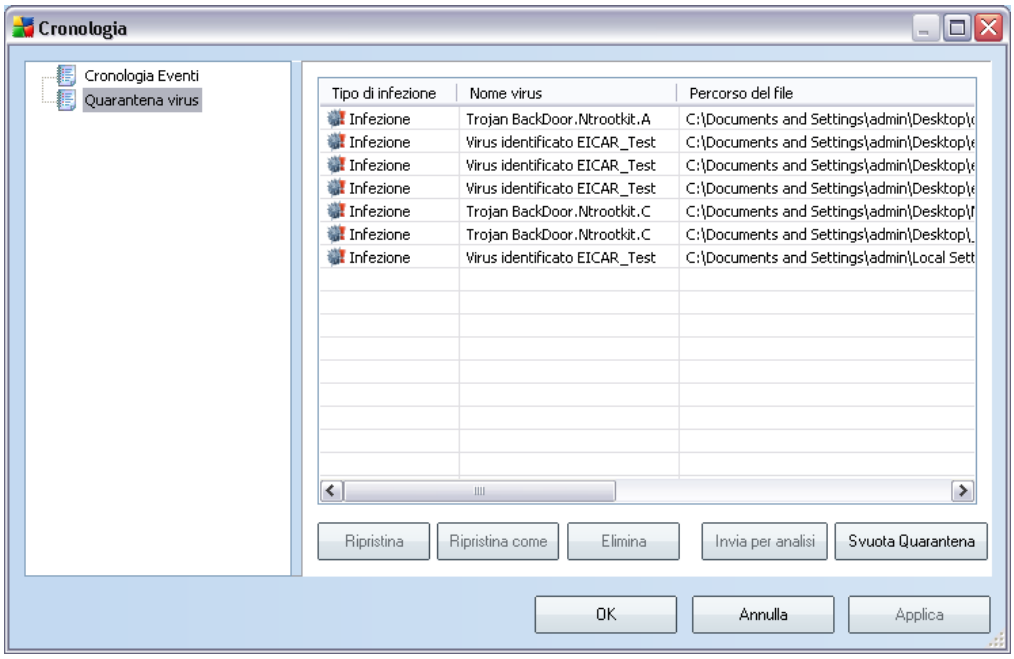
14.7.5.Scheda Rootkit

La scheda ***Rootkit*** visualizza informazioni sui rootkit rilevati durante la scansione. La relativa struttura corrisponde sostanzialmente a quella della ***scheda Infezioni*** o della ***scheda Spyware***.

14.7.6.Scheda Informazioni

Nella scheda ***Informazioni*** sono contenuti i dati sui rilevamenti che non possono essere classificati come infezioni, spyware e così via. Non possono essere etichettati come pericolosi anche se vanno considerati attentamente. Tutti i dati in questa scheda sono puramente informativi.

14.8.Quarantena virus



L'applicazione Quarantena virus è un ambiente protetto per la gestione degli oggetti sospetti o infetti rilevati durante i controlli AVG. Se durante la scansione viene rilevato un oggetto infetto e AVG non è in grado di ripararlo automaticamente, viene richiesto quale operazione eseguire sull'oggetto sospetto. La soluzione consigliata è spostare l'oggetto in ***Quarantena virus*** per un'ulteriore gestione.

L'interfaccia ***Quarantena virus*** viene aperta in una finestra separata e offre una panoramica delle informazioni relative agli oggetti infetti messi in quarantena:

- ***Tipo di infezione***: distingue i tipi di rilevamenti in base al livello di infezione (*tutti gli oggetti elencati possono essere infetti o potenzialmente infettati*)
- ***Nome virus***: specifica il nome dell'infezione rilevata in base all'Enciclopedia dei virus (in linea)

- ***Percorso del file***: percorso completo della posizione originale del file infetto rilevato
- ***Nome oggetto originale***: tutti gli oggetti rilevati inseriti nell'elenco sono stati denominati con un nome standard assegnato da AVG durante il processo di scansione. Se un oggetto aveva uno specifico nome originale conosciuto dal sistema (*ad esempio il nome di un allegato e-mail che non corrisponde al contenuto effettivo dell'allegato*), tale nome verrà visualizzato in questa colonna.
- ***Data di archiviazione***: data e ora del rilevamento e della rimozione in ***Quarantena virus del file sospetto***

Pulsanti di controllo

I seguenti pulsanti di controllo sono accessibili dall'interfaccia ***Quarantena virus***:

- ***Ripristina***: consente di ripristinare il file infetto nella posizione originale sul disco
- ***Ripristina come***: se si decide di spostare un oggetto infetto rilevato da ***Quarantena virus*** in una cartella selezionata, utilizzare questo pulsante. L'oggetto sospetto rilevato verrà salvato con il nome originale. Se il nome originale è sconosciuto, verrà utilizzato il nome standard.
- ***Elimina***: consente di rimuovere definitivamente il file infetto da ***Quarantena virus***
- ***Invia per analisi***: consente di inviare il file sospetto ai laboratori virus AVG per un'analisi approfondita
- ***Svuota Quarantena*** - elimina tutto il contenuto della ***Quarantena Virus*** completamente.

15. Aggiornamenti di AVG

15.1. Livelli di aggiornamento

AVG fornisce due livelli di aggiornamento che è possibile selezionare:

- ***In Aggiornamento definizioni*** sono contenute le modifiche necessarie per una protezione antivirus, anti-spam e anti-malware affidabile. In genere, non include eventuali modifiche del codice e consente di aggiornare solo il database delle definizioni. Questo aggiornamento deve essere applicato non appena è disponibile.

- ***In Aggiornamento programma*** sono contenuti le modifiche, le correzioni e i miglioramenti ai vari programmi.

Quando si pianifica un aggiornamento, è possibile selezionare il livello di priorità da scaricare e applicare.

15.2. Tipi di aggiornamento

Sono disponibili due tipi di aggiornamento:

- ***Aggiornamento su richiesta*** è un aggiornamento di AVG immediato che può essere eseguito in ogni momento secondo la necessità.

- ***Aggiornamento pianificato***: all'interno di AVG è inoltre possibile preimpostare un piano di aggiornamento. L'aggiornamento pianificato viene quindi eseguito periodicamente in base alla configurazione impostata. Ogni volta che sono presenti nuovi file di aggiornamento nella posizione specificata, questi vengono scaricati direttamente dal Web oppure dalla directory di rete. Quando non sono disponibili nuovi aggiornamenti, non avviene niente.

15.3. Processo di aggiornamento

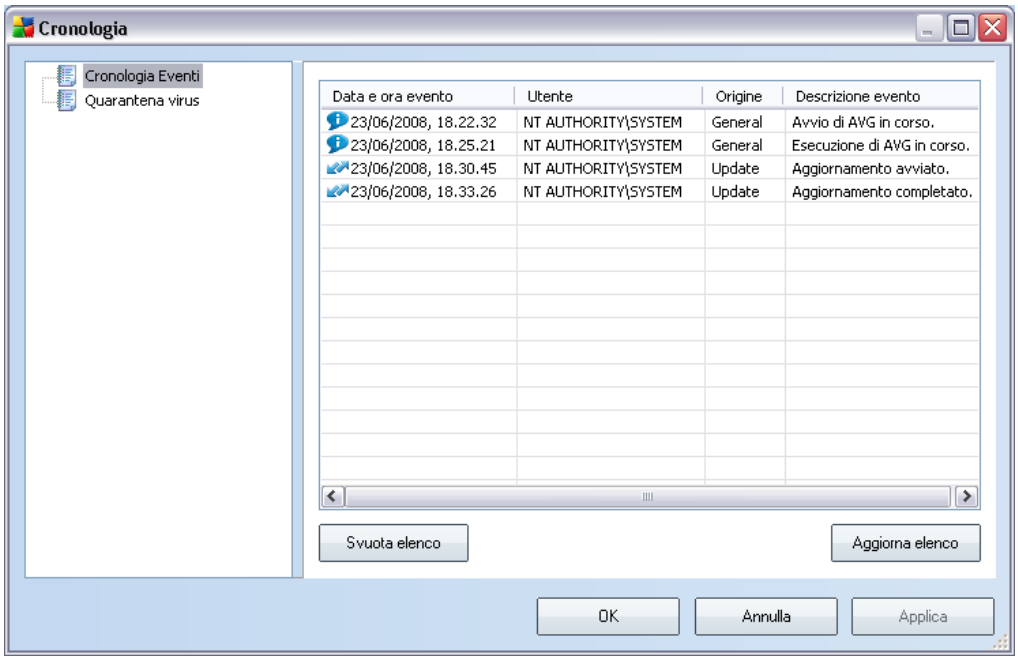
Il processo di aggiornamento può essere avviato immediatamente in base alle necessità dal collegamento rapido ***Aggiorna subito***. Questo collegamento è sempre disponibile da tutte le finestre di dialogo dell'interfaccia utente di AVG. Tuttavia, si consiglia di eseguire questi aggiornamenti a cadenza regolare come indicato nella pianificazione dell'aggiornamento modificabile nel componente Gestore aggiornamenti .

Una volta avviato l'aggiornamento, AVG verificherà innanziutto se sono presenti nuovi file di aggiornamento. In tal caso, AVG inizierà il download e avvierà il processo di

aggiornamento. Durante il processo di aggiornamento si verrà reindirizzati all'interfaccia ***Aggiorna*** da cui è possibile visualizzare la rappresentazione grafica e la panoramica dei parametri statistici rilevanti dell'avanzamento del processo (*dimensione file di aggiornamento, dati ricevuti, velocità di download, tempo trascorso e così via*).

Nota*: prima dell'avvo dell'aggiornamento di AVG viene creato un punto di ripristino del sistema. Se il processo di aggiornamento non ha esito positivo e il sistema operativo si blocca, è possibile ripristinare il sistema operativo nella configurazione originale da questo punto. Questa opzione è accessibile tramite Start / Tutti i programmi / Accessori / Utilità di sistema / Ripristino configurazione di sistema. Consigliato ai soli utenti esperti*

16. Cronologia Eventi



La finestra di dialogo ***Cronologia eventi*** è accessibile dal menu di sistema tramite la voce ***Cronologia/Log della Cronologia Eventi***. In questa finestra di dialogo è possibile trovare un riepilogo di importanti eventi che si sono verificati durante l'attività di **AVG 8.5 Internet Security** . In ***Cronologia eventi*** vengono registrati i seguenti tipi di evento:

- Informazioni sugli aggiornamenti dell'applicazione AVG
- Inizio, fine o arresto della scansione (inclusi i controlli eseguiti automaticamente)
- Eventi connessi al rilevamento di virus (da parte di Protezione permanente o scansione) inclusa la posizione in cui si sono verificati
- Altri eventi importanti

Pulsanti di controllo

- ***Svuota elenco***: consente di eliminare tutte le voci contenute nell'elenco degli eventi

- ***Aggiorna elenco***: consente di aggiornare tutte le voci contenute nell'elenco degli eventi

17. FAQ e assistenza tecnica

Se si verificano problemi con AVG, di tipo commerciale o tecnico, consultare la sezione ***FAQ*** del sito Web di AVG all'indirizzo www.avg.com.

Se non si riesce a risolvere il problema in questo modo, contattare il reparto dell'Assistenza tecnica via e-mail. Utilizzare il modulo di contatto accessibile dal menu di sistema tramite ***Guida / Utilizza Guida in linea***.