AVG 9 Anti-Virus

Manuale per l'utente

Revisione documento 90.21 (3.2.2010)

Sommario

1. Introduzione

Questa guida per l'utente fornisce la documentazione completa relativa a **AVG 9 Anti-Virus**.

Complimenti per l'acquisto di AVG 9 Anti-Virus!

AVG 9 Anti-Virus è un elemento della gamma di prodotti AVG pluripremiati progettata per fornire maggiore tranquillità e la protezione completa del PC. Analogamente a tutti i prodotti AVG, **AVG 9 Anti-Virus** è stato interamente riprogettato per fornire la protezione famosa e accreditata di AVG in una nuova maniera più efficace e intuitiva.

Il nuovo prodotto **AVG 9 Anti-Virus** presenta un'interfaccia semplificata combinata con funzioni di scansione più efficaci 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 del computer e della rete. Goditi l'esperienza della protezione completa offerta da AVG.

2. Requisiti per l'installazione di AVG

2.1. Sistemi operativi supportati

AVG 9 Anti-Virus è destinato alla protezione delle workstation 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)
- Windows 7 (x86 e x64, tutte le edizioni)

(e possibilmente Service Pack successivi per sistemi operativi specifici)

2.2. Requisiti hardware minimi e consigliati

Requisiti hardware minimi per **AVG 9 Anti-Virus**:

- CPU Intel Pentium da 1,5 GHz
- 512 MB di memoria RAM
- 390 MB di spazio libero sul disco rigido (per l'installazione)

Requisiti hardware consigliati per **AVG 9 Anti-Virus**:

- CPU Intel Pentium da 1,8 GHz
- 512 MB di memoria RAM
- 510 MB di spazio libero sul disco rigido (per l'installazione)

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 (http://www.avg.com/it).

Prima di avviare l'installazione di AVG, è consigliabile visitare il sito Web di AVG (http://www.avg.com/it) per controllare che non sia disponibile un nuovo file di installazione. In questo modo si sarà certi di installare la versione più recente di AVG 9 Anti-Virus.

Si consiglia di provare il nuovo strumento AVG Download Manager che consente di individuare il file di installazione nella lingua desiderata.

Durante il processo di installazione verrà richiesto 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. AVG Download Manager

AVG Download Manager è uno strumento semplice che consente di selezionare il file di installazione corretto per la versione Trial del 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.

Attenzione: *tenere presente che AVG Download Manager non è adatto al download delle edizioni Network e SBS e supporta solo i seguenti sistemi operativi: Windows 2000 (SP4 + SRP roll-up), Windows XP, Windows Vista e Windows 7.*

AVG Download Manager è disponibile per il download nel sito Web di AVG (http://www.avg.com/it). 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

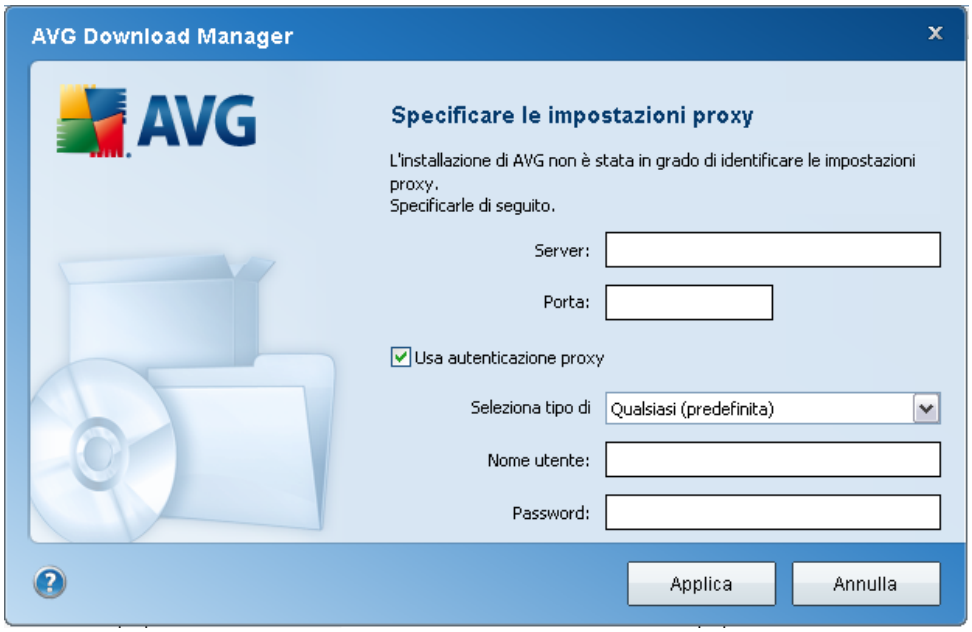
Nel passaggio successivo, **AVG Download Manager** tenterà di stabilire una connessione Internet in modo da individuare gli aggiornamenti. Non sarà possibile procedere con il processo di download finché **AVG Download Manager** non avrà completato il controllo della connettività.

- 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. Download dei file di installazione

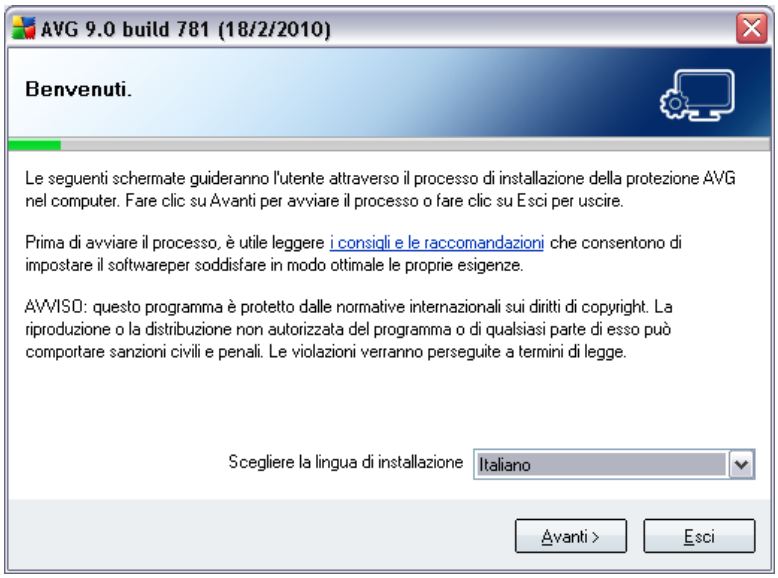
A questo punto sono state fornite tutte le informazioni necessarie a **AVG Download Manager** per avviare il download del pacchetto di installazione e avviare il processo di installazione. Accedere quindi al Processo di installazione di AVG.

5. Processo di installazione di AVG

Per installare **AVG 9 Anti-Virus** 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 di AVG (http://www.avg.com/it), sezione ***Supporto / 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 a ogni passaggio. Di seguito viene fornita una descrizione di ciascuna finestra di dialogo:

5.1. Avvio dell'installazione

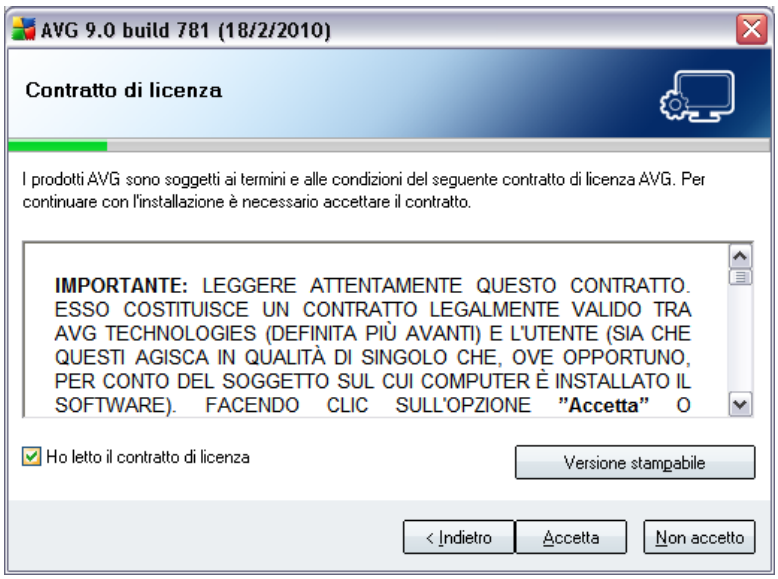


Il processo di installazione inizia con la finestra ***Benvenuti nel programma di installazione di AVG*** . Da qui è possibile selezionare la lingua utilizzata per il processo di installazione. Nella parte inferiore della finestra di dialogo, individuare la voce ***Scegliere la lingua di installazione*** 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, che può essere specificata*

successivamente durante il processo di installazione.

5.2. Contratto di licenza



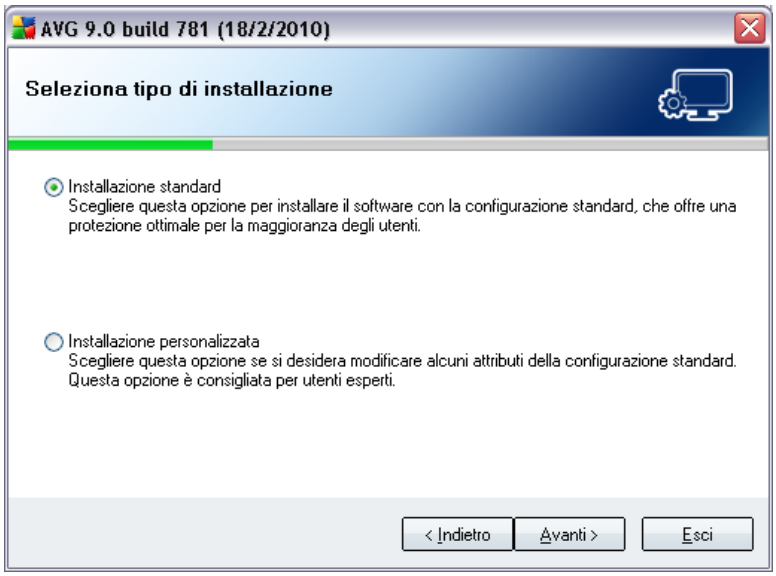
Nella finestra di dialogo ***Contratto di licenza*** è disponibile l'intero contenuto del contratto di licenza AVG. Leggere con attenzione il contratto e confermarne lettura e accettazione selezionando la casella di controllo ***Ho letto il contratto di licenza***, quindi selezionando il pulsante ***Accetta***.

Se non si accettano i termini del contratto di licenza, selezionare il pulsante ***Non accetto***. 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.

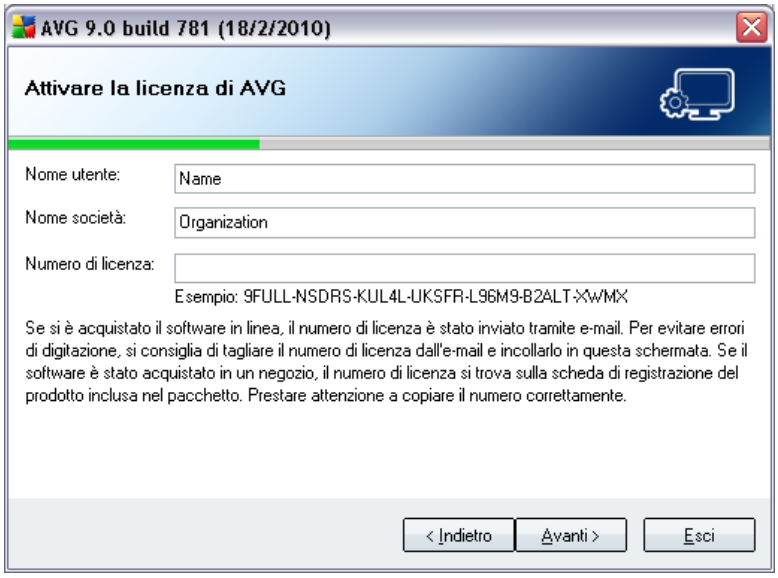
L'installazione personalizzata deve essere utilizzata solo da utenti esperti che hanno valide ragioni per installare AVG senza le impostazioni standard, ad esempio per soddisfare requisiti di sistema specifici.

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 ***Numero licenza***. Il numero di vendita è disponibile sulla custodia del CD presente nella confezione di **AVG 9 Anti-Virus** . Il numero di licenza sarà contenuto nel messaggio e-mail di conferma ricevuto

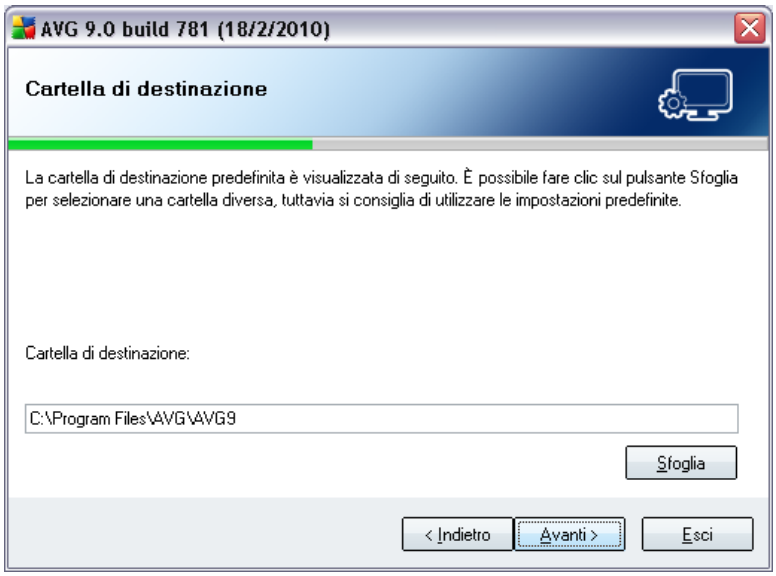
dopo l'acquisto in linea di **AVG 9 Anti-Virus**. È necessario digitare il numero esattamente come viene indicato. Se il numero di licenza è disponibile nel formato digitale (*contenuto nel messaggio e-mail*), si consiglia di utilizzare il metodo "copia e incolla" per immetterlo.



Selezionare 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 ***AVG Security Toolbar***. Se è stata selezionata l'installazione personalizzata, si proseguirà con la finestra di dialogo ***Cartella di destinazione***.

5.6. Installazione personalizzata - Cartella di destinazione

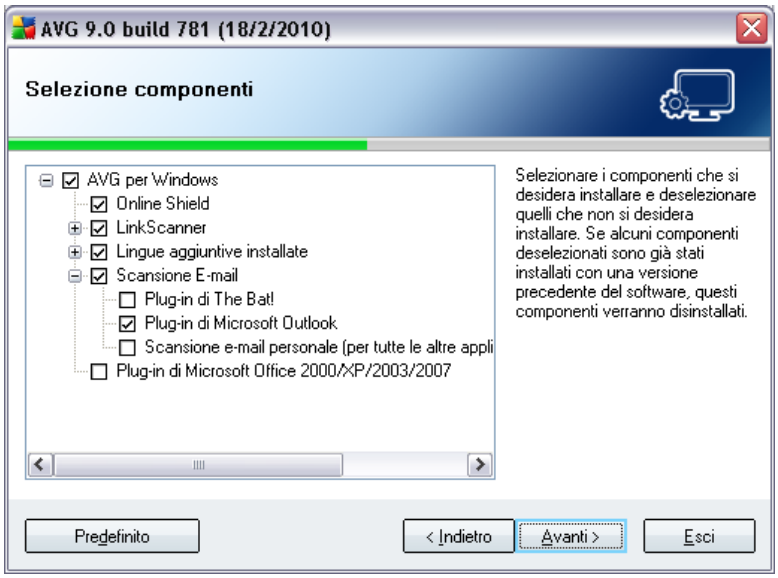


La finestra di dialogo ***Cartella di destinazione*** consente di specificare la posizione in cui **AVG 9 Anti-Virus** sarà installato. Per impostazione predefinita, AVG viene installato nella cartella dei programmi che si trova nell'unità C:. Se la cartella non esiste, in una nuova finestra di dialogo verrà richiesto di confermare che si consente a AVG di creare tale cartella.

Se si desidera modificare questa posizione, utilizzare il pulsante ***Sfoglia*** per visualizzare la struttura dell'unità e selezionare la cartella pertinente.

Fare clic sul pulsante ***Avanti*** per confermare.

5.7. Installazione personalizzata - Selezione dei componenti



La finestra di dialogo ***Selezione dei componenti*** visualizza una panoramica di tutti i componenti di **AVG 9 Anti-Virus** che è possibile installare. Se le impostazioni predefinite non sono adeguate alle esigenze specifiche, è possibile rimuovere/aggiungere determinati componenti.

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

- ***Selezione lingua***

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

- ***Plug-in per Scansione E-mail***

  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.

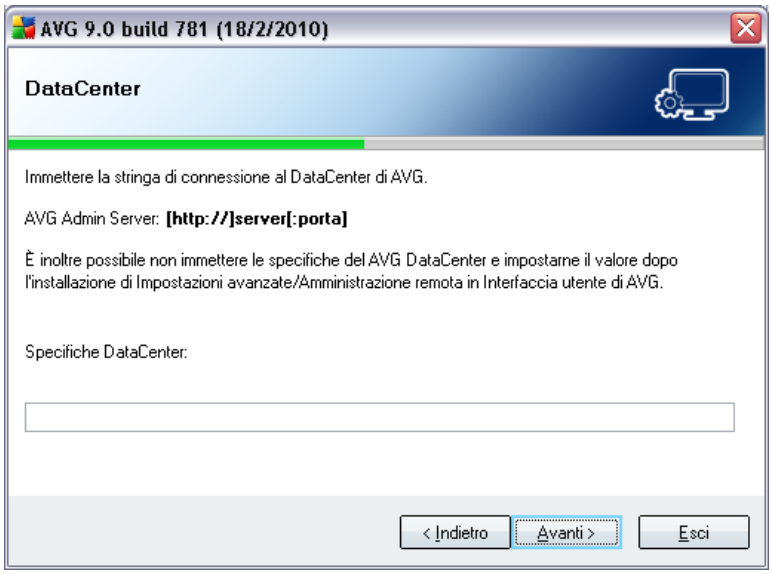
- ***Amministrazione remota***

  Se si prevede di collegare il computer ad Amministrazione remota di AVG successivamente, selezionare la relativa voce per installare anche questo componente.

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

5.8. AVG DataCenter

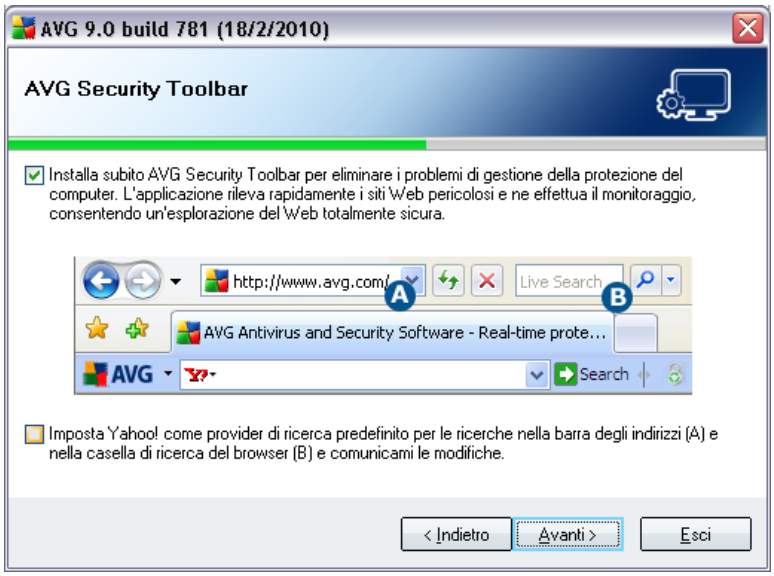
Se è in uso una licenza di rete di AVG e nella precedente finestra di dialogo ***Installazione personalizzata - Selezione componenti*** la voce ***Amministrazione remota*** è stata selezionata per l'installazione, è necessario specificare i parametri di ***AVG DataCenter***:



Nel campo di testo delle ***specifiche di AVG DataCenter*** immettere la stringa di connessione a ***AVG DataCenter*** nel formato *server:porta*. Se questa informazione al momento non è disponibile, lasciare vuoto il campo. È possibile completare la configurazione successivamente nella finestra di dialogo ***Impostazioni avanzate / Amministrazione remota***.

Nota: *per informazioni dettagliate su Amministrazione remota di AVG, consultare il Manuale per l'utente di AVG Network Edition disponibile per il download sul sito Web di AVG (http://www.avg.com/it).*

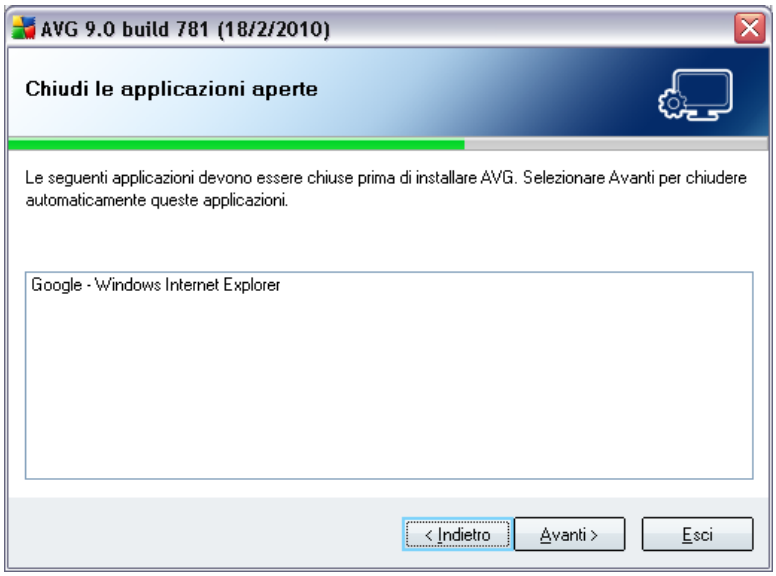
5.9. AVG Security Toolbar



Nella finestra di dialogo ***AVG Security Toolbar*** specificare se si desidera installare ***AVG Security Toolbar*** (*per la verifica dei risultati di ricerca forniti dai motori di ricerca Internet supportati*). Se non si modificano le impostazioni predefinite, questo componente verrà installato automaticamente nel browser Web (*i browser al momento supportati sono Microsoft Internet Explorer v. 6.0 o successiva e Mozilla Firefox v. 2.0 o successiva*) per offrire la protezione in linea completa durante l'esplorazione di Internet.

Inoltre, è possibile decidere se utilizzare Yahoo! come provider di ricerca predefinito. In caso affermativo, selezionare la relativa casella di controllo.

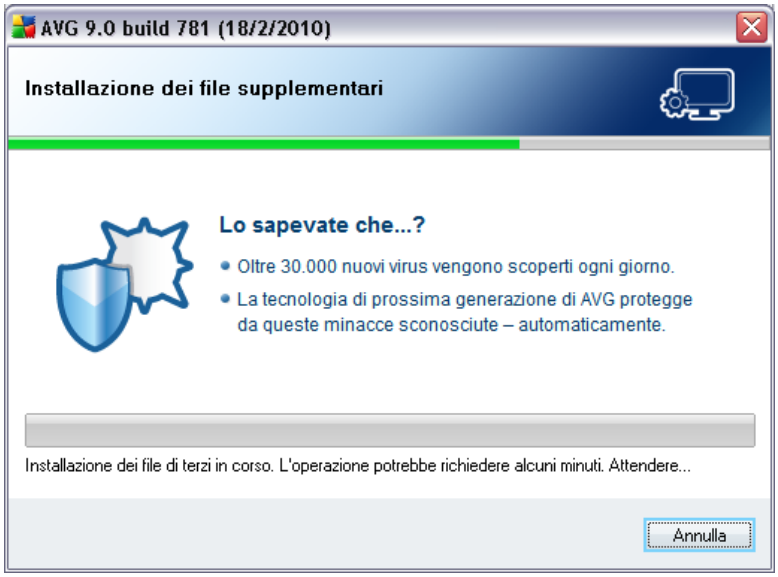
5.10. Chiudi le applicazioni aperte



La finestra di dialogo ***Chiudi le applicazioni aperte*** viene visualizzata durante il processo di installazione solo se al momento sul computer sono in esecuzione programmi in conflitto. Viene quindi fornito l'elenco dei programmi che devono essere chiusi per poter completare il processo di installazione. Selezionare il pulsante ***Avanti*** per confermare la chiusura delle rispettive applicazioni e procedere al passaggio successivo.

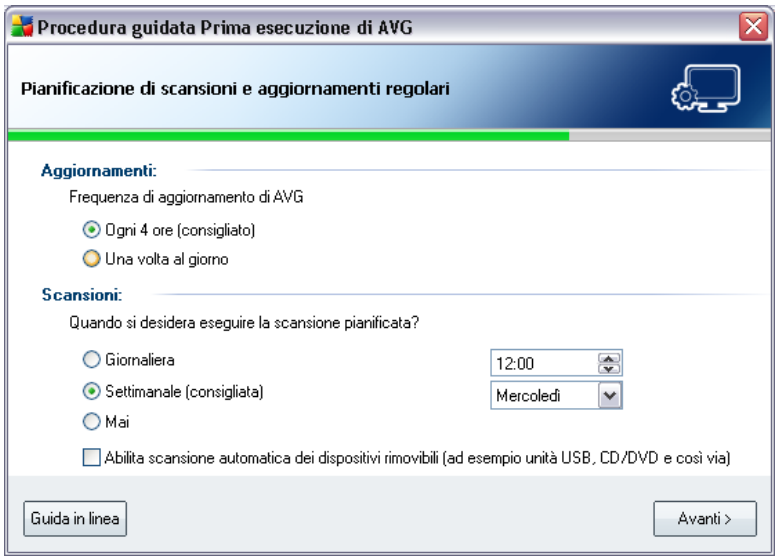
5.11. Installazione di AVG

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



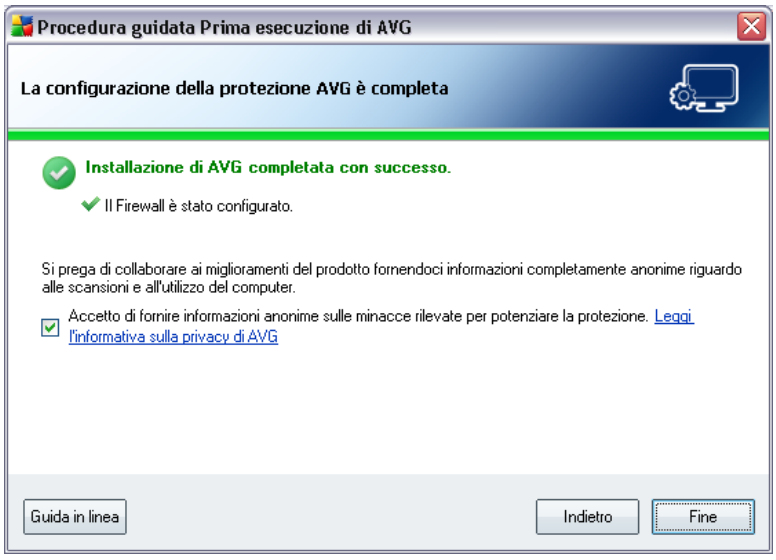
Al termine dell'installazione, si verrà reindirizzati automaticamente alla seguente finestra di dialogo.

5.12. 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. Fare clic sul pulsante ***Avanti*** per continuare.

5.13. La configurazione della protezione AVG è completa



AVG 9 Anti-Virus è stato configurato.

In questa finestra di dialogo è possibile decidere se attivare l'opzione di segnalazione anonima di exploit e siti pericolosi a AVG Virus Lab. In caso affermativo, selezionare l'opzione ***Accetto di fornire informazioni ANONIME sulle minacce rilevate per potenziare la protezione***.

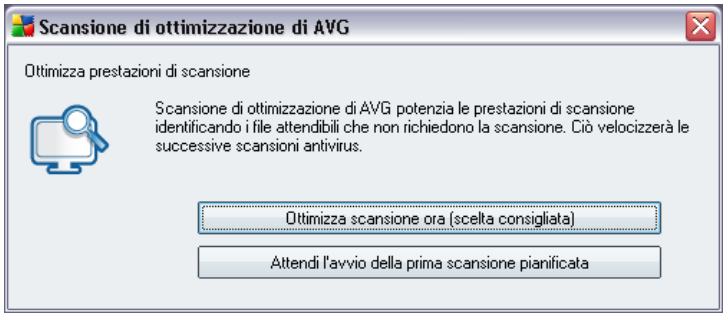
Per concludere, selezionare il pulsante ***Fine.***

6. Dopo l'installazione

6.1. Ottimizzazione scansione

La funzionalità di ottimizzazione della scansione esegue la ricerca nelle cartelle *Windows* e *Programmi* in cui rileva i file appropriati (*al momento si tratta dei file *.exe, *.dll e *.sys*) e salva le informazioni su questi file. Al successivo accesso questi file non verranno nuovamente sottoposti a scansione e ciò ridurrà notevolmente i tempi di scansione.

Al termine del processo di installazione verrà proposta l'ottimizzazione della scansione in una nuova finestra di dialogo:



Si consiglia di utilizzare questa opzione ed eseguire il processo di ottimizzazione della scansione selezionando il pulsante ***Ottimizza scansione ora***.

6.2. Registrazione del prodotto

Una volta completata l'installazione di **AVG 9 Anti-Virus**, registrare il prodotto in linea sul sito Web di AVG (http://www.avg.com/it), alla 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.

6.3. Accesso all'interfaccia utente

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

- tramite doppio clic sull'icona di AVG sulla barra delle applicazioni
- tramite doppio clic sull'icona di AVG sul desktop

- dal menu ***Start/Programmi/AVG 9.0/Interfaccia utente di AVG***

6.4. Scansione dell'intero computer

Esiste il rischio potenziale che un virus sia stato trasmesso al computer dell'utente prima dell'installazione di **AVG 9 Anti-Virus**. 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***.

6.5. Controllo Eicar

Per confermare che **AVG 9 Anti-Virus** è stato installato correttamente 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 a salvarlo sul disco locale. Subito dopo aver confermato il download del file di controllo, il componente ***Online Shield*** visualizzerà un avviso. Questo avviso dimostra che AVG è stato installato correttamente nel computer.

Dal sito Web http://www.eicar.com è inoltre possibile scaricare la versione compressa del "virus" EICAR (*ad esempio nel formato eicar_com.zip*). ***Online Shield*** consente di scaricare questo file e di salvarlo sul disco locale, ma ***Resident Shield*** rileva il 'virus' quando si tenta di decomprimere il file. **Se AVG non identifica il file di controllo EICAR come un virus, è necessario controllare nuovamente la configurazione del programma.**

6.6. Configurazione predefinita di AVG

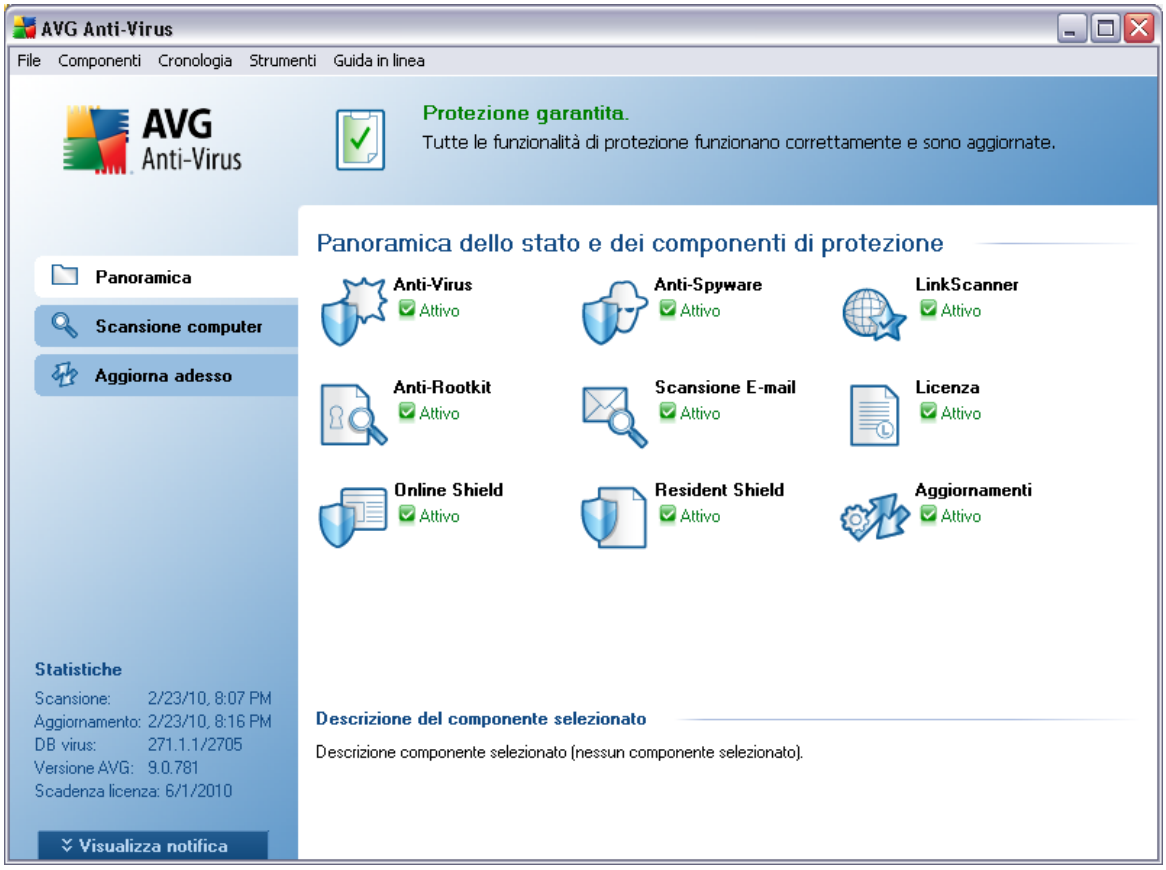
La configurazione predefinita (*ovvero la modalità di impostazione dell'applicazione dopo l'installazione*) di **AVG 9 Anti-Virus** è impostata dal fornitore del software in modo tale che tutti i componenti e le funzioni offrano un'ottimizzazione massima delle prestazioni.

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 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 nella finestra di dialogo ***Impostazioni AVG avanzate*** visualizzata.

7. Interfaccia utente di AVG

AVG 9 Anti-Virus si apre visualizzando la finestra 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 >>

7.1. Menu di sistema

Menu di sistema è l'esplorazione standard utilizzata in tutte le applicazioni Windows. È posizionato orizzontalmente nella parte superiore della finestra principale di **AVG 9 Anti-Virus**. 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:

7.1.1. File

- ***Esci***: consente di chiudere l'interfaccia utente di **AVG 9 Anti-Virus**. Tuttavia, l'applicazione AVG continuerà a essere eseguita in background e il computer sarà comunque protetto.

7.1.2. 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***

- ***Link Scanner***: consente di aprire la pagina predefinita del componente ***Link Scanner***

- ***Scansione E-mail***: consente di aprire la pagina predefinita del componente

Scansione E-mail

- ***Licenza***: consente di aprire la pagina predefinita del componente ***Licenza***
- ***Online Shield***: consente di aprire la pagina predefinita del componente ***Online Shield***
- ***Resident Shield***: consente di aprire la pagina predefinita del componente ***Resident Shield***
- ***Gestore aggiornamenti***: consente di aprire la pagina predefinita del componente ***Gestore aggiornamenti***

7.1.3. Cronologia

- ***Risultati scansione***: consente di visualizzare l'interfaccia di controllo di AVG, in particolare la finestra di dialogo ***Panoramica risultati di scansione***
- ***Rilevamento 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 degli allegati e-mail rilevati come pericolosi dal componente ***Scansione E-mail***
- ***Rilevamenti di Online Shield***: consente di aprire una finestra di dialogo con una panoramica delle minacce rilevate da ***Online 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 9 Anti-Virus** registrate.

7.1.4. 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 9 Anti-Virus**

- ***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 9 Anti-Virus** . In genere è consigliabile mantenere le impostazioni predefinite dell'applicazione definite dal fornitore di software.

7.1.5. 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 (http://www.avg.com/it) alla pagina del centro di assistenza clienti

- ***AVG Web personale***: consente di aprire il sito Web di AVG (http://www.avg.com/it)

- ***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 aprire la pagina relativa alla registrazione del sito Web di AVG (http://www.avg.com/it). Immettere i dati di registrazione; solo i

clienti che registrano il proprio prodotto AVG possono ricevere assistenza tecnica gratuita.

***Nota**: se è in uso la versione Trial di **AVG 9 Anti-Virus**, le ultime due voci appaiono come **Acquista ora** e **Attiva**, consentendo di acquistare subito la versione completa del programma. Per **AVG 9 Anti-Virus** installato con un numero di vendita, le voci vengono visualizzate come **Registra** e **Attiva**. Per ulteriori informazioni, consultare la sezione Licenza di questa documentazione.*

- ***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***.

7.2. 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 9 Anti-Virus**. 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.

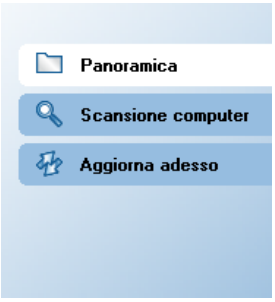

L'icona rossa indica che lo stato di AVG è critico. Uno o più componenti non funzionano correttamente e AVG non è in grado di proteggere il computer. Intervenire immediatamente per risolvere il problema segnalato. Se non si è in grado di correggere l'errore, contattare il team di assistenza tecnica di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

7.3. 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 i controlli, pianificare le scansioni oppure modificare i parametri: vedere il capitolo ***Scansione 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.

7.4. 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

In **AVG 9 Anti-Virus** la sezione ***Panoramica dei componenti*** contiene informazioni sui seguenti componenti:

- ***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 >>
- ***Link Scanner*** controlla i risultati della ricerca visualizzati nel browser Internet - dettagli >>
- ***Anti-Rootkit*** rileva i programmi e le tecnologie che tentano di camuffare i malware - dettagli >>
- ***Scansione E-mail*** controlla la posta in entrata e in uscita per rilevare virus - dettagli >>
- ***Licenza*** visualizza numero, tipo e data di scadenza della licenza - dettagli >>
- ***Online 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 questi vengono copiati, aperti o salvati - dettagli >>
- ***Gestore 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 attuale e non si desidera ricevere notifiche tramite l'icona presente nella barra delle applicazioni.

7.5. 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 9.0.xx, dove 9.0 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

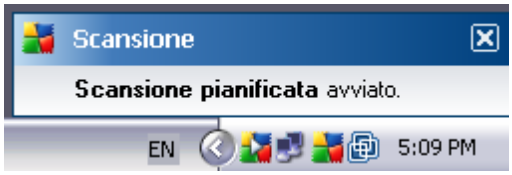
7.6. Icona della barra delle applicazioni

L'icona della barra delle applicazioni (*presente nella barra delle applicazioni di Windows*) indica lo stato corrente di **AVG 9 Anti-Virus**. 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***.

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



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

8. Componenti di AVG

8.1. Anti-Virus

8.1.1. 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.

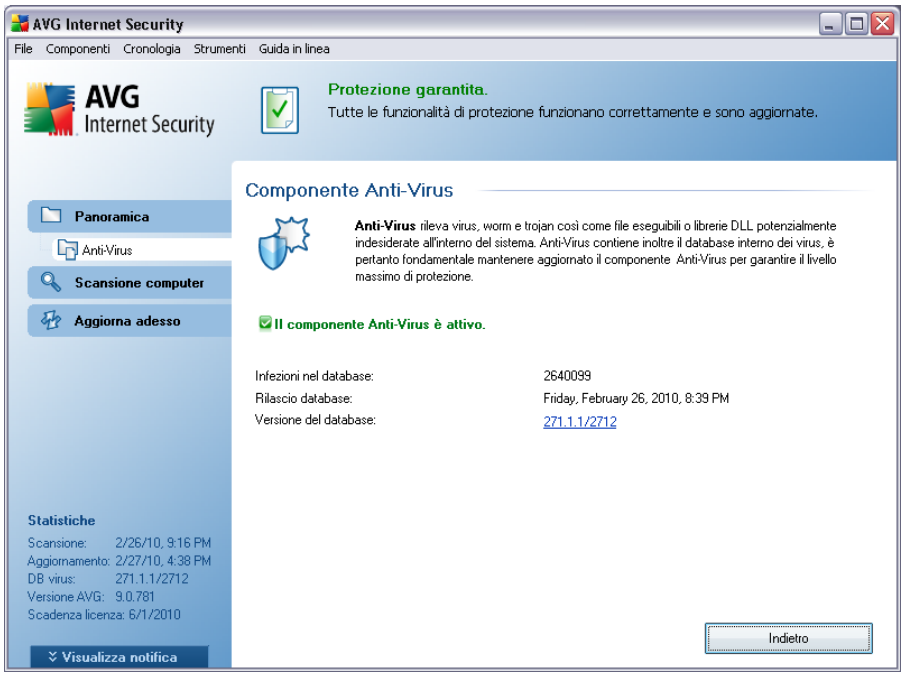
La funzione principale della protezione antivirus è impedire l'esecuzione di virus noti sul computer.

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 dai 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.

8.1.2. Interfaccia dell'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 dei virus
- ***Ultimo aggiornamento del database***: specifica in che giorno e a che ora è stato eseguito l'ultimo aggiornamento del database dei virus
- ***Versione del database***: indica il numero della versione più recente del database dei virus. Il numero viene incrementato dopo ogni aggiornamento del database 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 del software ha impostato tutti i componenti AVG per fornire prestazioni ottimali. A meno che non vi sia un motivo valido, 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 del menu di sistema ***Strumenti / Impostazioni avanzate*** *e modificare la configurazione di AVG nella finestra di dialogo Impostazioni AVG avanzate visualizzata.*

8.2. Anti-Spyware

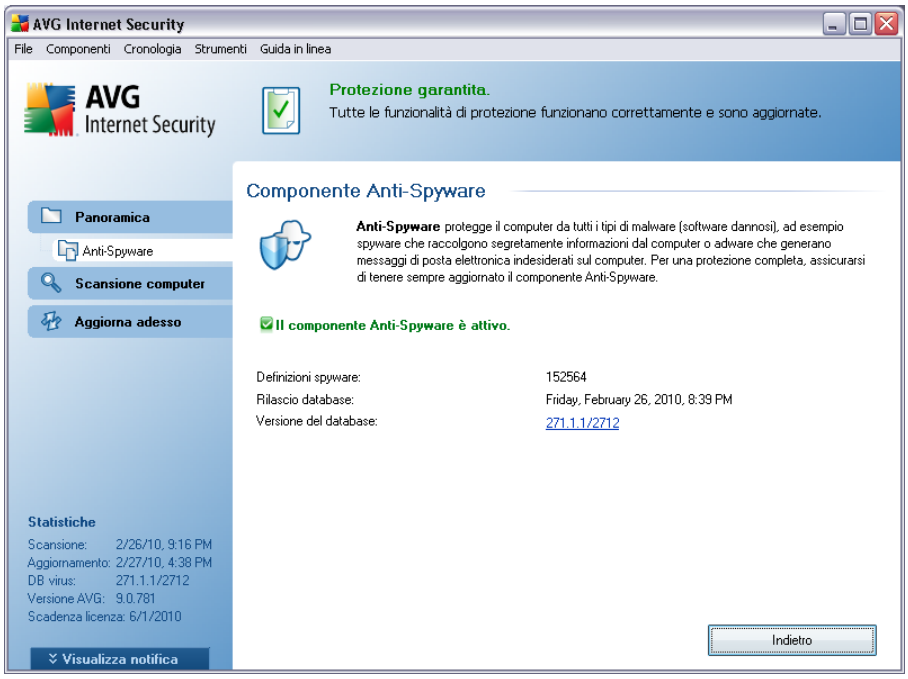
8.2.1. Anti-Spyware Principi

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 9 Anti-Virus** con gli aggiornamenti del programma e del database più recenti. 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.

8.2.2. Interfaccia dell'Anti-Spyware



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 in che giorno e a che ora è stato eseguito l'ultimo aggiornamento del database di spyware
- ***Versione del database***: indica il numero della versione più recente del database di spyware. Il numero viene incrementato dopo ogni aggiornamento del database 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 del software ha impostato tutti i componenti AVG per fornire prestazioni ottimali. A meno che non vi sia un motivo valido, 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 del menu di sistema**Strumenti / Impostazioni avanzate** e modificare la configurazione di AVG nella finestra di dialogo Impostazioni AVG avanzate visualizzata.*

8.3. Anti-Rootkit

Un rootkit è un programma progettato per assumere il controllo di base di un sistema senza autorizzazione da parte dei proprietari e dei gestori legittimi del sistema. 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.

8.4. Scansione E-mail

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

8.4.1. Principi di Scansione E-mail

Il componente ***Scansione E-mail*** esegue automaticamente la scansione delle e-mail in entrata e in uscita. È possibile utilizzarlo con i client e-mail che non dispongono di un plug-in in AVG (*ad esempio Outlook Express, Mozilla, Incredimail e così via*).

Durante l'installazione di AVG vengono creati due server per il controllo dell'e-mail: uno per il controllo delle e-mail in entrata e l'altro per il controllo delle e-mail in uscita. Grazie a questi due server, i messaggi e-mail vengono automaticamente controllati sulle porte 110 e 25 (*porte standard per l'invio e la ricezione dei messaggi*).

Scansione E-mail funziona come interfaccia tra il client e-mail e i server e-mail in Internet.

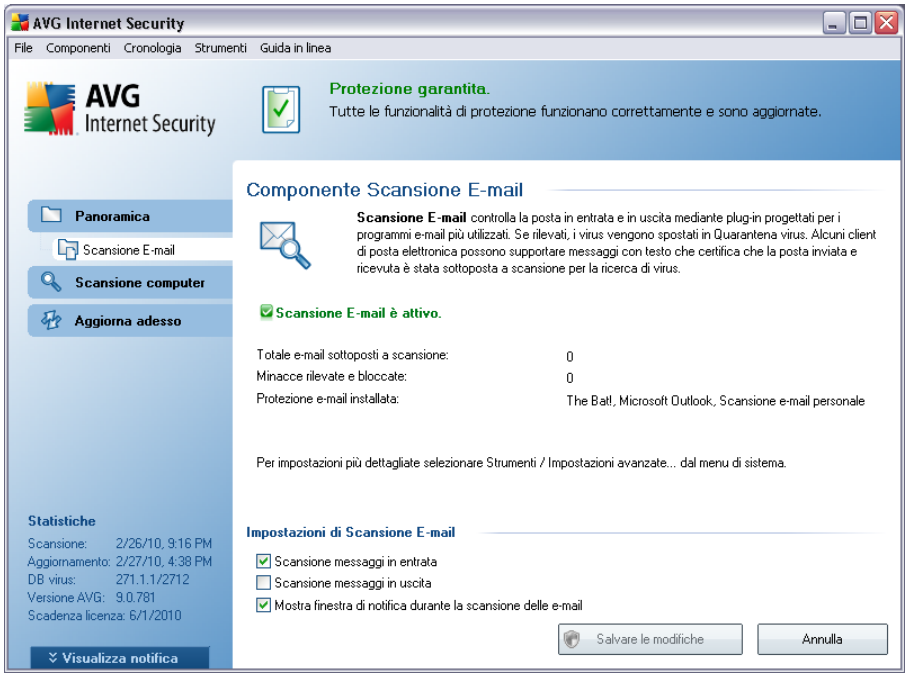
- ***Posta in entrata:*** quando viene ricevuto un messaggio dal server, il

componente ***Scansione E-mail*** lo sottopone a scansione per il rilevamento di virus, rimuove gli allegati infetti e aggiunge la certificazione. Se rilevati, i virus vengono immediatamente inseriti in ***Quarantena virus***. Quindi il messaggio viene passato al client e-mail.

- ***Posta in uscita:*** il messaggio viene inviato dal client e-mail a Scansione E-mail, che lo sottopone a scansione, insieme agli allegati, per il rilevamento di virus, quindi lo invia al server SMTP (*la scansione delle e-mail in uscita è disattivata per impostazione predefinita e può essere impostata manualmente*).

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

8.4.2. 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***: numero di 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, tramite 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 questa voce per specificare che tutte le e-mail consegnate all'account in uso devono essere sottoposte a scansione per il rilevamento di virus. Questa voce è attivata per impostazione predefinita e si consiglia di non modificare questa impostazione.

- ***Scansione messaggi in uscita***: selezionare questa voce per confermare che tutte le e-mail inviate dall'account in uso 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***: selezionare la voce per confermare che si desidera essere informati tramite finestra di dialogo di notifica visualizzata sopra l'icona AVG presente nella barra delle applicazioni durante la scansione dell'e-mail da parte del componente ***Scansione E-mail***. Questa voce è attivata per impostazione predefinita e si consiglia di non modificare questa impostazione.

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

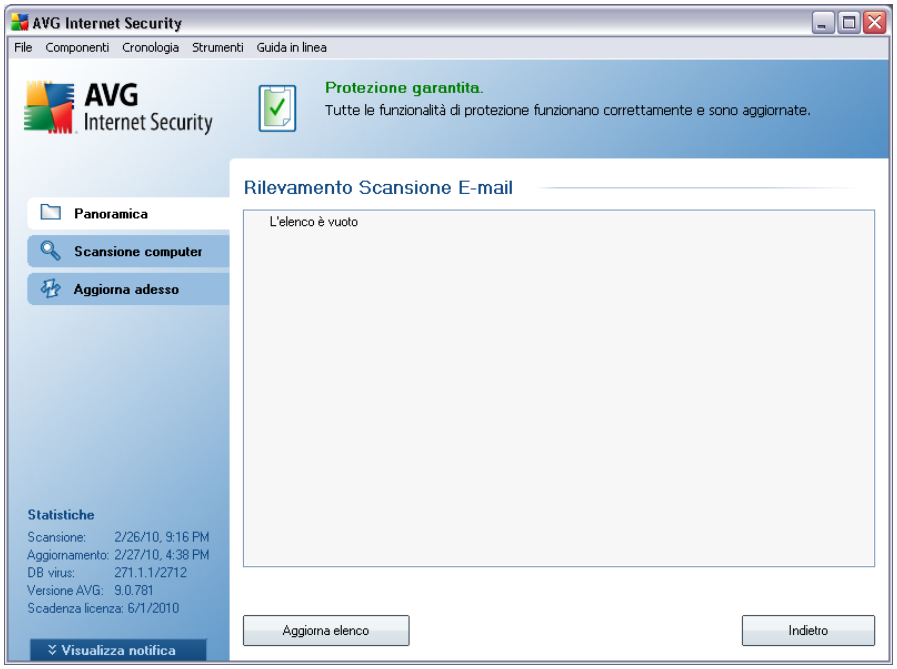
Nota:*il fornitore del software ha impostato tutti i componenti AVG per fornire prestazioni ottimali. A meno che non vi sia un motivo valido, si consiglia di non modificare la configurazione di AVG. Tutte le eventuali modifiche alle impostazioni dovrebbero essere eseguite da un utente esperto. Se è necessario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

8.4.3. 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.
- ***Ora di rilevamento***: data e ora in cui l'oggetto sospetto è stato rilevato

- ***Tipo di oggetto***: tipo di oggetto rilevato.

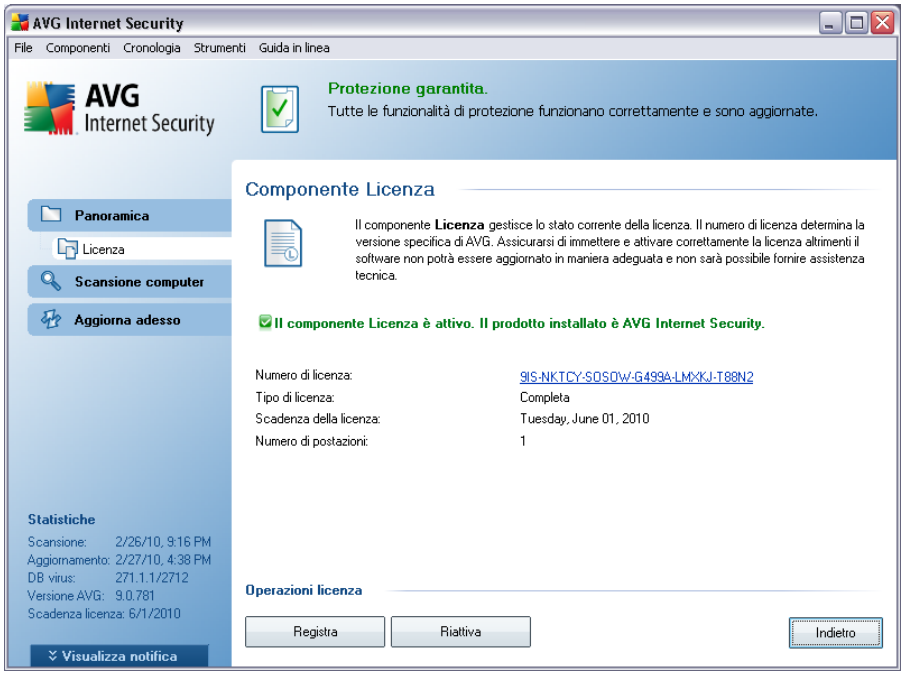
Nella parte inferiore della finestra di dialogo, sotto l'elenco, sono disponibili informazioni sul numero totale degli oggetti rilevati elencati in alto. È inoltre possibile esportare l'intero elenco di oggetti rilevati in un file (***Esporta elenco in file***) ed eliminare tutte le voci relative agli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

Pulsanti di controllo

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

- ***Aggiorna elenco***: aggiorna l'elenco delle minacce rilevate
- ***Indietro***: consente di tornare all'***Interfaccia utente di AVG*** predefinita (panoramica dei componenti)

8.5. 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. Pertanto si consiglia di utilizzare sempre il metodo "copia e incolla" per l'immissione del numero di licenza.

- ***Tipo di licenza***: specifica il tipo di prodotto installato.

- ***Scadenza licenza***: questa data determina il periodo di validità della licenza. Se si desidera continuare a utilizzare **AVG 9 Anti-Virus** dopo questa data, sarà necessario rinnovare la licenza. Il rinnovo della licenza può essere effettuato in linea sul sito Web di AVG (http://www.avg.com/it).

- ***Numero di postazioni***: indica il numero di workstation nelle quali è possibile installare **AVG 9 Anti-Virus**.

Pulsanti di controllo

- ***Registra***: consente di aprire la pagina relativa alla registrazione del sito Web di AVG (http://www.avg.com/it). Immettere i dati di registrazione; solo i clienti che registrano il prodotto AVG possono ricevere assistenza tecnica gratuita.

- ***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*).

Nota: se è in uso la versione Trial di *AVG 9 Anti-Virus*, **i pulsanti appaiono come** *Acquista ora* **e** *Attiva, consentendo di acquistare subito la versione completa del programma. Per* **AVG 9 Anti-Virus** *installato con un numero di vendita, i pulsanti vengono visualizzati come* ***Registra*** *e* ***Attiva****.*

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

8.6. Link Scanner

8.6.1. Principi di Link Scanner

Il componente ***LinkScanner*** fornisce la protezione dai siti Web creati per installare malware nel computer dell'utente tramite il browser Web o i relativi plug-in. La tecnologia ***LinkScanner*** è costituita da due funzionalità, ***AVG Search-Shield*** e ***AVG Active Surf-Shield***:

- ***AVG Search-Shield***contiene un elenco di siti Web (*indirizzi URL*) notoriamente pericolosi. Quando si effettuano ricerche con Google, Yahoo!, Bing, Baidu, Altavista o Yandex, tutti i risultati delle ricerche vengono controllati in base a questo elenco e viene visualizzata un'icona relativa al livello di sicurezza (*per i risultati delle ricerche Yahoo! vengono visualizzate solo le icone relative ai siti Web dannosi*). Inoltre, se si digita un indirizzo direttamente nel browser oppure si fa clic su un collegamento contenuto in un sito Web o in un'e-mail, il sito di destinazione viene controllato automaticamente e bloccato se necessario.

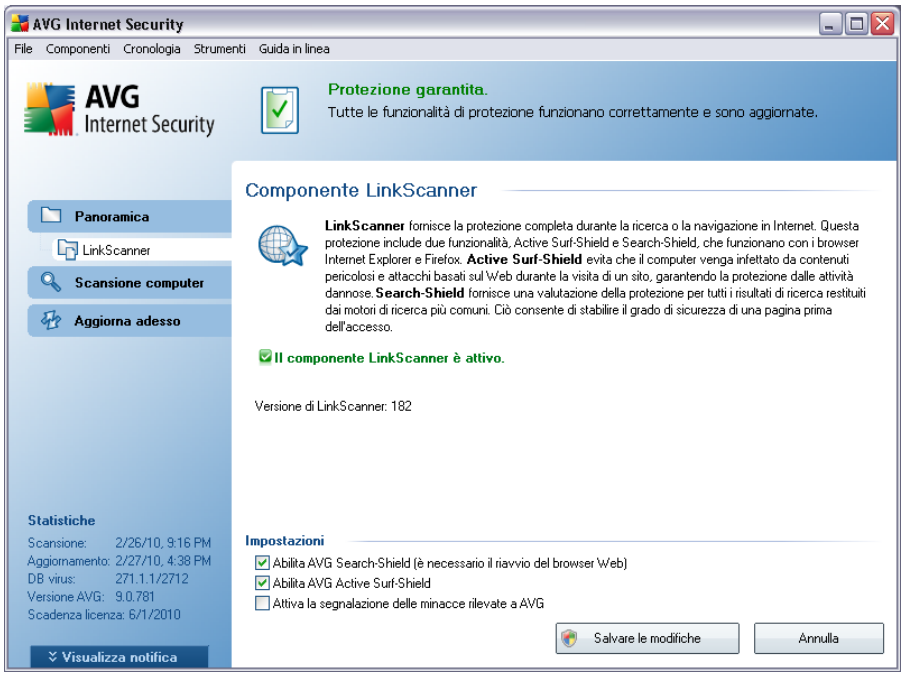
- ***AVG Active Surf-Shield***esegue la scansione dei contenuti dei siti Web visitati, indipendentemente dall'indirizzo del sito. Anche se un sito Web non viene rilevato da ***AVG Search Shield*** (*ad esempio se viene creato un nuovo sito dannoso o se un sito in precedenza sicuro contiene ora un malware*), verrà rilevato e bloccato da ***AVG Active Surf-Shield*** una volta che si tenterà di accedervi.

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

8.6.2. Interfaccia di Link Scanner

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

L'interfaccia del componente ***LinkScanner***fornisce una breve descrizione delle funzionalità del componente e informazioni sul relativo stato (*Il componente LinkScanner è attivo*). Inoltre, sono disponibili informazioni sul numero di versione del database ***LinkScanner*** più recente (|*Versione LinkScanner*).



Nella parte inferiore della finestra di dialogo è possibile modificare diverse opzioni:

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

- ***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*).

- ***Attiva la segnalazione delle minacce rilevate a AVG***: selezionare questa voce per attivare la segnalazione di siti fraudolenti e dannosi trovati dall'utente mediante ***Safe Surf*** o ***Safe Search*** e consentire la raccolta di informazioni nell'apposito database in merito ad attività dannose svolte sul Web.

8.6.3. AVG Search-Shield

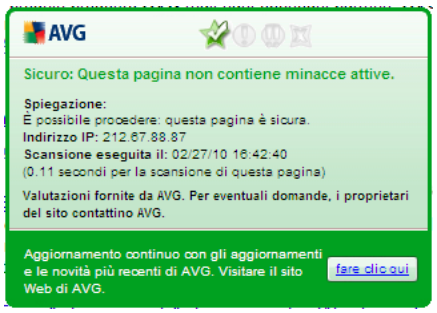
Quando si eseguono ricerche in Internet con ***AVG Search-Shield*** attivato, tutti i risultati di ricerca restituiti dai motori di ricerca più comuni quali Yahoo!, Google, Bing, Altavista, Yandex e così via vengono valutati per rilevare collegamenti pericolosi o

sospetti. Con il controllo dei collegamenti e l'assegnazione di un contrassegno ai collegamenti dannosi, ***AVG Link Scanner*** avvisa l'utente prima che questi 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*).
- 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.

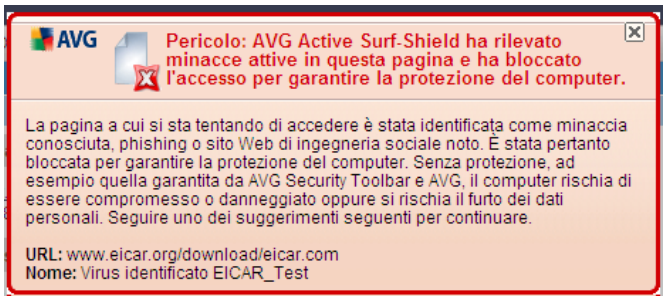
Se si passa il mouse sopra una singola icona che indica la valutazione verranno visualizzati i dettagli relativi al collegamento specifico. Nelle informazioni sono inclusi gli eventuali dettagli aggiuntivi relativi alla minaccia, l'indirizzo IP del collegamento e il momento in cui è stata eseguita la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



8.6.4. 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 tramite il semplice accesso al sito infetto. È per questo che, quando si richiedono pagine Web contenenti exploit o altre minacce gravi, ***AVG Link Scanner*** non ne consentirà la visualizzazione.

Se si incorre in siti Web dannosi, all'interno del browser ***AVG Link Scanner*** visualizzerà un avviso simile al seguente:



L'accesso a questo sito Web è molto rischioso e non consigliabile.

8.7. Online Shield

8.7.1. Principi di Online Shield

Online 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.

Online Shield rileva che la pagina che sta per essere aperta contiene alcuni javascript dannosi e impedisce 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 Online Shield non è destinato alle piattaforme server.*

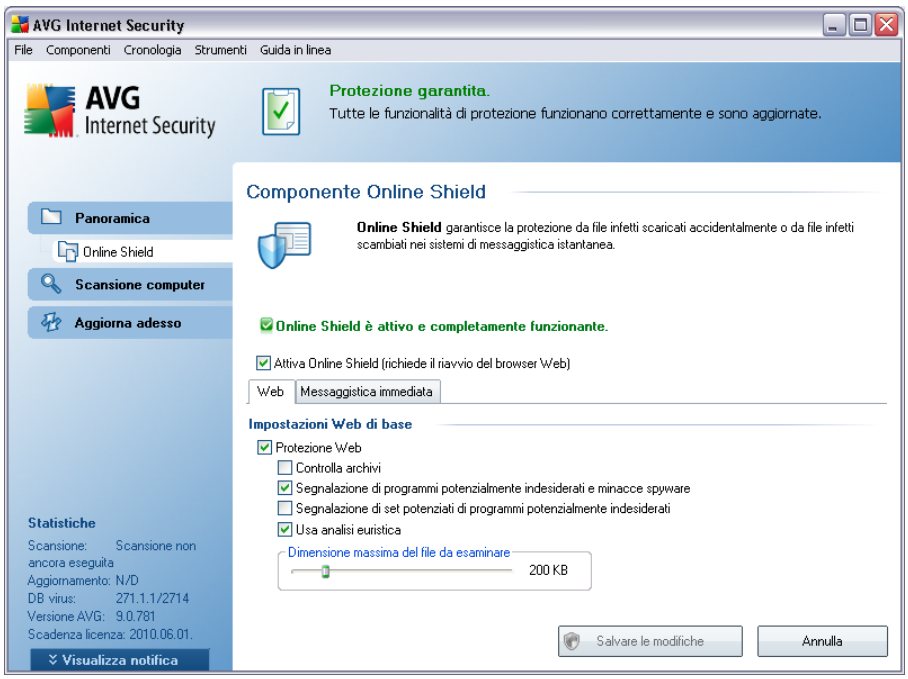
8.7.2. Interfaccia di Online Shield

L'interfaccia del componente ***Online Shield*** descrive il comportamento di questo tipo di protezione. Inoltre, è possibile trovare informazioni sullo stato corrente del componente (*Online 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 ***Online Shield*** selezionando la voce ***Abilita Online Shield***. Questa opzione è abilitata per impostazione predefinita e il componente ***Online 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 ***Online 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 ***Online 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

- ***Segnalazione di programmi potenzialmente indesiderati e minacce spyware*** – (*attivata per impostazione predefinita*) selezionare questa casella di controllo per attivare il motore ***Anti-Spyware*** ed eseguire la scansione per ricercare spyware e virus. Gli spyware rappresentano una categoria di malware anomala: anche se solitamente costituiscono un rischio per la sicurezza, alcuni di questi programmi possono essere installati intenzionalmente. Si consiglia di mantenere questa funzionalità attivata in quanto consente di aumentare la protezione del computer

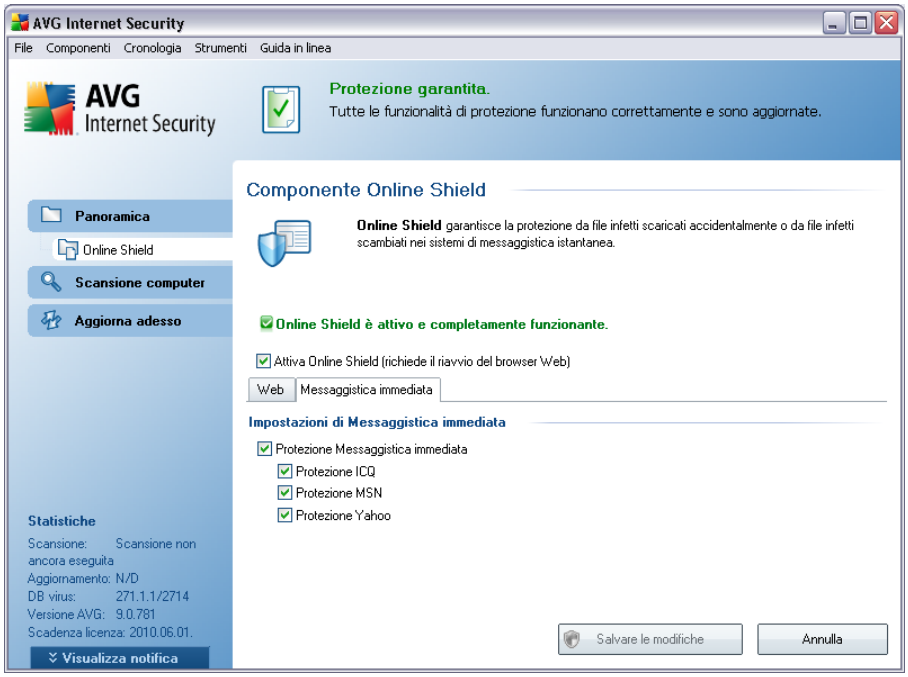
- ***Segnalazione di set potenziati di programmi potenzialmente indesiderati*** – se la precedente opzione è attivata, è inoltre possibile selezionare questa casella per rilevare pacchetti estesi di spyware: programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita.

- ***Usa analisi euristica***: consente di eseguire la scansione del contenuto della pagina da visualizzare utilizzando il metodo dell'analisi euristica, ossia simulazione e valutazione delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale. Di conseguenza, è in grado di rilevare il codice dannoso non ancora descritto nel database dei virus *(vedere Principi dell'Anti-Virus*).

- ***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 da ***Online Shield***. Anche se le dimensioni del file scaricato sono superiori a quelle specificate, quindi il file non verrà sottoposto a scansione da ***Online Shield***, il computer è comunque protetto: se il file fosse infetto, verrebbe rilevato immediatamente 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 Online 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 9 Anti-Virus** supporta le applicazioni ICQ, MSN e Yahoo.

Nota: il *fornitore del software ha impostato tutti i componenti AVG per fornire prestazioni ottimali. A meno che non vi sia un motivo valido, 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 del menu di sistema****Strumenti / Impostazioni avanzate*** *e modificare la configurazione di AVG nella finestra di dialogo Impostazioni AVG avanzate visualizzata.*

Pulsanti di controllo

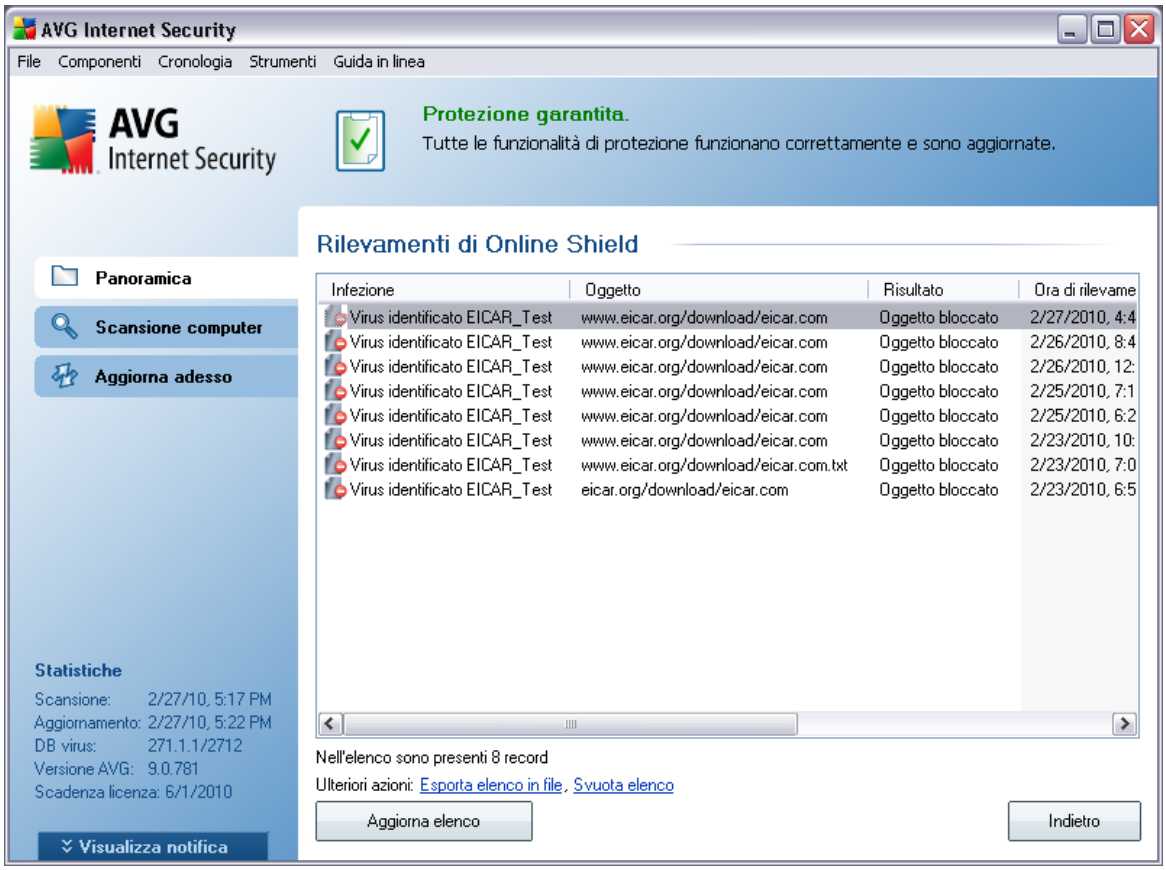
I pulsanti di controllo disponibili nell'interfaccia di ***Online Shield*** sono i seguenti:

- ***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*)

8.7.3. Rilevamenti di Online Shield

Online 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 Online Shield***; questa panoramica delle minacce rilevate è accessibile tramite il menu di sistema ***Cronologia / Rilevamenti di Online Shield***.



Per ogni oggetto rilevato vengono fornite le seguenti informazioni:

- ***Infezione***: descrizione *possibilmente anche il nome*) dell'oggetto rilevato
- ***Oggetto***: origine dell'oggetto (*pagina Web*)
- ***Risultato***: azione eseguita sull'oggetto rilevato.
- ***Ora di rilevamento***: data e ora in cui la minaccia è stata rilevata e bloccata
- ***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 ***Online Shield***. Il pulsante ***Indietro*** consente di tornare all'***Interfaccia utente di AVG*** predefinita (panoramica dei componenti).

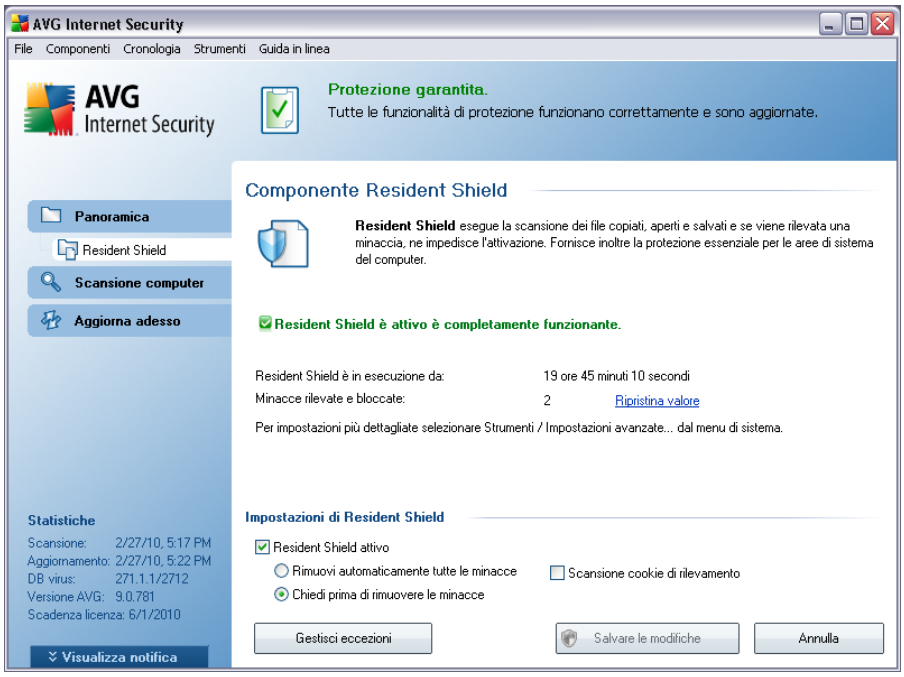
8.8. Resident Shield

8.8.1. Resident Shield Principi

Il componente ***Resident Shield*** fornisce al computer una protezione continua. Esegue la scansione di ogni singolo file aperto, salvato o copiato e sorveglia le aree di sistema del computer. Quando ***Resident Shield*** rileva un virus durante l'accesso a un file, arresta l'operazione in corso impedendo l'attivazione del virus. Normalmente, questo processo non viene notato in quanto viene eseguito "in background": l'utente riceve notifiche solo quando vengono rilevate minacce. Contemporaneamente, ***Resident Shield*** blocca l'attivazione della minaccia e la rimuove. ***Resident Shield*** viene caricato nella memoria del computer all'avvio del sistema.

Attenzione: Resident Shield viene caricato nella memoria del computer all'avvio ed è importante che resti sempre attivato.

8.8.2. Interfaccia di 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 la cui esecuzione/ apertura è stata bloccata (*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 tramite la voce Strumenti/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 ***Scansione cookie di rilevamento***. 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 del software ha impostato tutti i componenti AVG per fornire prestazioni ottimali. A meno che non vi sia un motivo valido, 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 del menu di sistema****Strumenti / Impostazioni avanzate*** *e modificare la configurazione di AVG nella finestra di dialogo Impostazioni AVG avanzate visualizzata.*

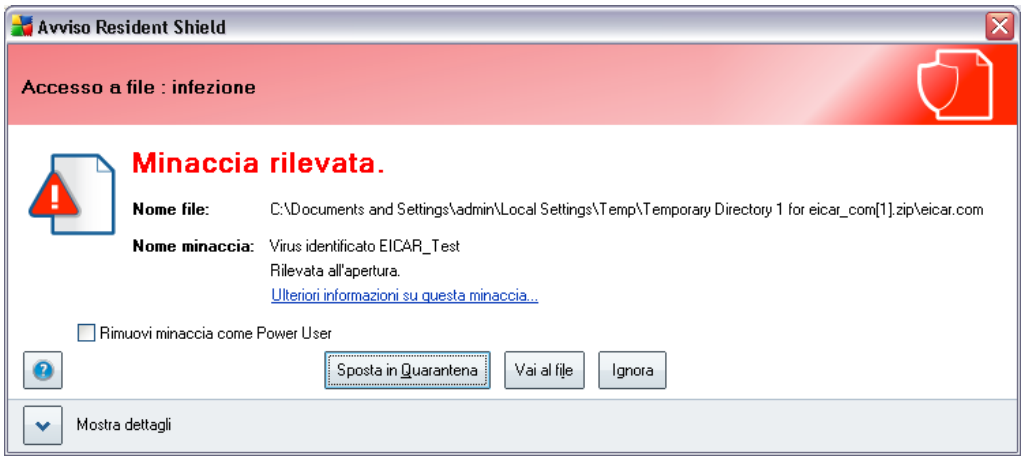
Pulsanti di controllo

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

- ***Gestisci eccezioni***: consente di aprire la finestra di dialogo ***Resident Shield - Esclusioni di directory*** 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)

8.8.3. Rilevamento Resident Shield

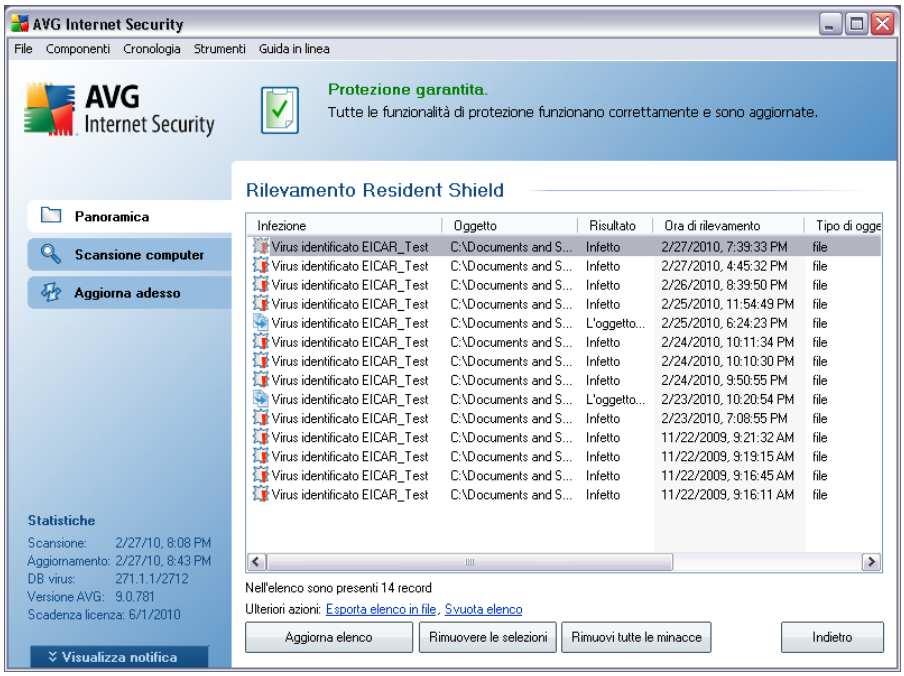
Resident Shield esegue la scansione dei file mentre vengono copiati, aperti o salvati. Quando viene rilevato un virus o altra minaccia, l'utente viene avvisato immediatamente tramite la successiva finestra di dialogo:



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***
- ***Vai al file***: questa opzione reindirizza alla posizione esatta dell'oggetto sospetto (*apre una nuova finestra di Esplora risorse*)
- ***Ignora***: si consiglia di NON utilizzare questa opzione a meno che non sussista un motivo valido per farlo

L'intera panoramica delle minacce rilevate da ***Resident Shield*** è disponibile nella finestra di dialogo ***Rilevamento Resident Shield*** accessibile tramite l'opzione del menu di sistema ***Cronologia / Rilevamenti di Resident Shield***:



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.
- ***Ora di rilevamento***: data e ora in cui l'oggetto è stato 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).

8.9. Gestore aggiornamenti

8.9.1. Principi di Gestore aggiornamenti

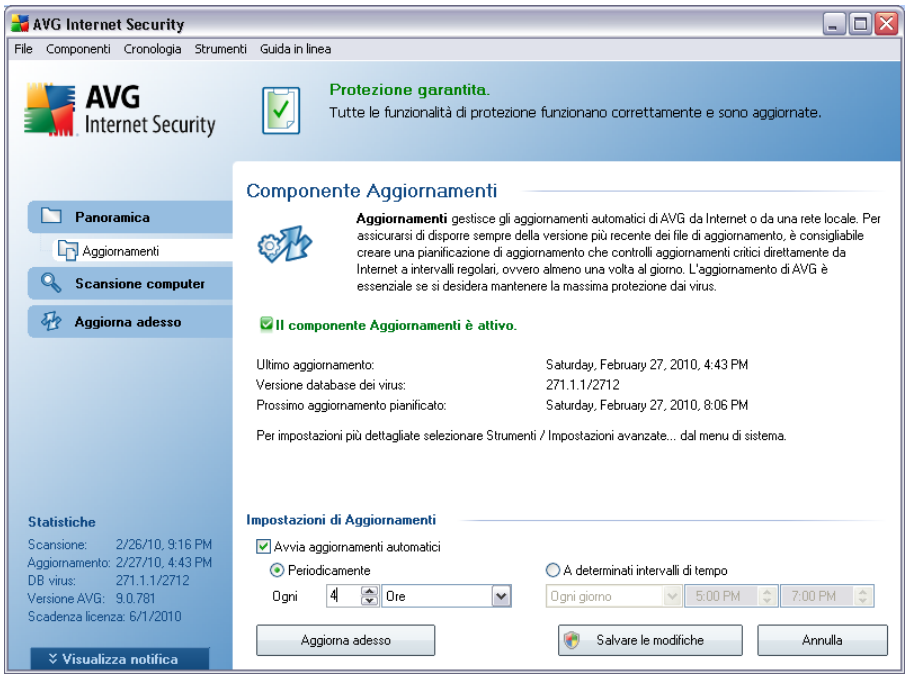
Nessun software per la protezione è in grado di garantire una vera e propria protezione da vari tipi di minacce se non viene aggiornato con regolarità. Gli autori di virus vanno sempre alla ricerca di nuove imperfezioni che possano sfruttare sia nei sistemi operativi che nel software. Tutti i giorni 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.*

8.9.2. Interfaccia di Gestore 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
- ***Prossimo aggiornamento pianificato***: specifica per che giorno e per che ora è stato pianificato il successivo aggiornamento del database

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 modificarla. 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 del software ha impostato tutti i componenti AVG per fornire prestazioni ottimali. A meno che non vi sia un motivo valido, 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 del 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 ***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 questo pulsante per tornare all'impostazione predefinita dell' ***interfaccia utente di AVG*** (panoramica dei componenti)

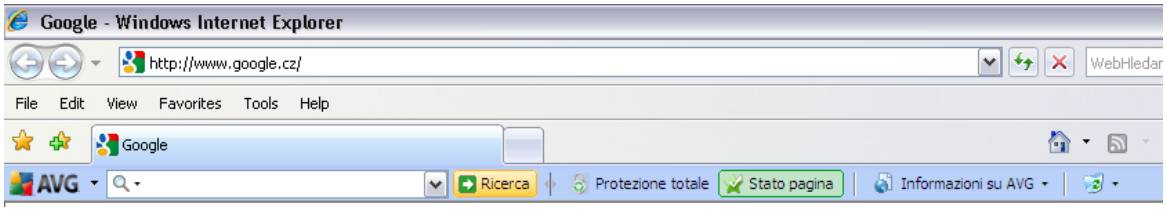
9. AVG Security Toolbar

AVG Security Toolbar è un nuovo strumento che funziona insieme al componente ***Link Scanner*** e controlla i risultati forniti dai motori di ricerca Internet supportati (*Yahoo!, Google, Bing, Altavista, Baidu*). ***AVG Security Toolbar*** può essere utilizzata per controllare le funzioni di ***AVG Link Scanner*** e regolarne il comportamento.

Se si sceglie di installare la barra degli strumenti durante l'installazione di **AVG 9 Anti-Virus**, questa verrà aggiunta al browser Web automaticamente. Se si utilizza un browser Internet alternativo (*ad esempio Avant Browser*) potrebbero verificarsi comportamenti inattesi.

9.1. AVG Security Toolbar Interfaccia

AVG Security Toolbar è progettata per funzionare con ***MS Internet Explorer*** (*versione 6.0 o superiore*) e ***Mozilla Firefox*** (*versione 2.0 o superiore*). Se si è deciso di installare ***AVG Security Toolbar****(durante il processo di installazione di AVG è stato richiesto se installare o meno il componente*), il componente verrà posizionato nel browser Web sotto la barra degli indirizzi:



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

AVG Security Toolbar è composta di quanto segue:

- ***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 (http://www.avg.com/it). Se si fa clic con il 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***
    - ***AvviaAVG 9 Anti-Virus***: consente di aprire l'interfaccia utente di **AVG 9 Anti-Virus**
    - ***Opzioni***: consente di aprire una finestra di dialogo di configurazione in cui

è possibile regolare le impostazioni di ***AVG Security Toolbar*** in base alle esigenze. Vedere il seguente capitolo ***Opzioni di AVG Security Toolbar***

- ***Elimina cronologia***: questo pulsante consente di utilizzare le opzioni *Elimina cronologia completa* relativa a AVG Security Toolbar oppure *Elimina cronologia ricerche, Elimina cronologia browser, Elimina cronologia download* e *Elimina cookie*.

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

- ***Guida in linea***: fornisce le opzioni per aprire il file della Guida, inviare commenti sul prodotto oppure visualizzare i dettagli della versione corrente della barra degli strumenti

- ***Casella di ricerca***: immettere una parola o una frase nella casella di ricerca. Selezionare ***Ricerca*** per avviare la ricerca utilizzando il motore di ricerca specificato (*è possibile specificare il motore di ricerca da utilizzare nelle opzioni avanzate di AVG Security Toolbar, scegliendo tra Yahoo!, Wikipedia, Baidu, WebHledani o Yandex*), indipendentemente dalla pagina 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.

- ***Protezione totale***: questo pulsante viene visualizzato come ***Protezione totale*** / ***Protezione limitata*** / ***Nessuna protezione*** in base alla **AVG 9 Anti-Virus**configurazione

- ***Stato pagina***: direttamente nella barra degli strumenti, questo pulsante visualizza la valutazione della pagina Web caricata al momento in base ai criteri del componente ***AVG Search-Shield*** (*la pagina è sicura / sospetta / decisamente pericolosa / contiene minacce / non può essere sottoposta a scansione*). Fare clic sul pulsante per aprire un riquadro informativo con dati dettagliati sulla pagina Web specifica.

- ***Informazioni su AVG***: fornisce i collegamenti a informazioni importanti sulla protezione contenute nel sito Web di AVG (http://www.avg.com/it).

  - ***Informazioni barra degli strumenti***: consente di accedere alla pagina principale di ***AVG Security Toolbar con informazioni dettagliate sulla protezione della barra degli strumenti***

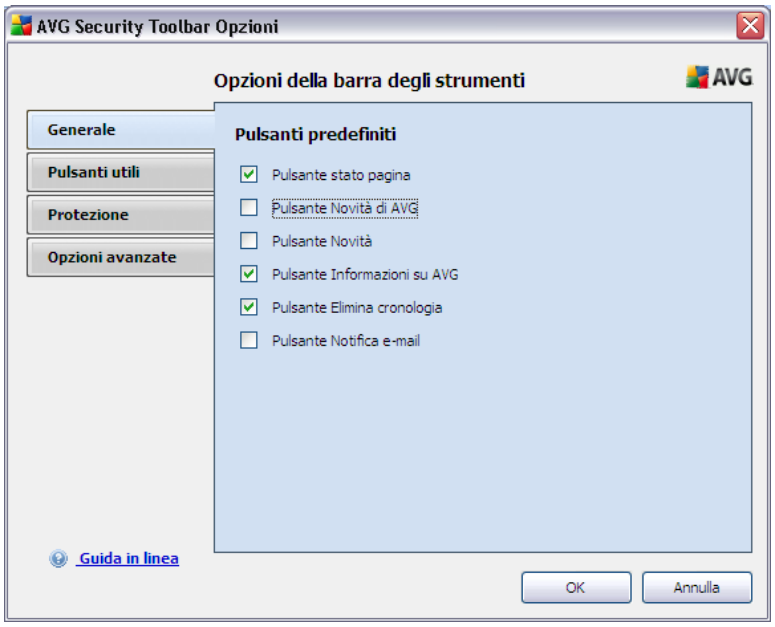
  - ***Informazioni sulle minacce***: consente di aprire la pagina Web di AVG contenente informazioni su virus e minacce presenti in Internet

- ***Novità di AVG***: consente di aprire la pagina Web contenente i comunicati stampa più recenti relativi a AVG
- ***Livello di minacce corrente***: consente di aprire la pagina Web di Virus Lab contenente la visualizzazione grafica del livello di minacce corrente sul Web
- ***Enciclopedia dei virus***: consente di aprire la pagina dell'Enciclopedia dei virus in cui è possibile ricercare virus specifici in base al nome e ottenere informazioni dettagliate su ciascuno di essi

9.2. Opzioni di AVG Security Toolbar

La configurazione di tutti i parametri di ***AVG Security Toolbar*** è accessibile direttamente dal riquadro ***AVG Security Toolbar***. L'interfaccia di modifica si apre tramite la voce di menu della barra degli strumenti *AVG / Opzioni* in una nuova finestra di dialogo denominata ***Opzioni barra degli strumenti*** divisa in quattro sezioni:

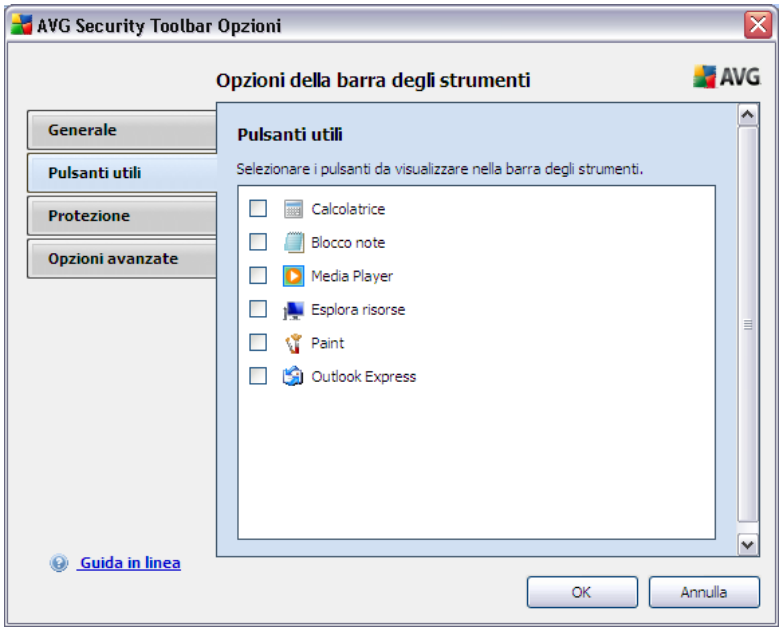
9.2.1. Scheda Generale



In questa scheda è possibile specificare i pulsanti di controllo della barra degli strumenti da visualizzare o nascondere nel riquadro ***AVG Security Toolbar***. Selezionare un'opzione per visualizzare il rispettivo pulsante. Vengono descritte di seguito le funzionalità di ciascun pulsante della barra degli strumenti:

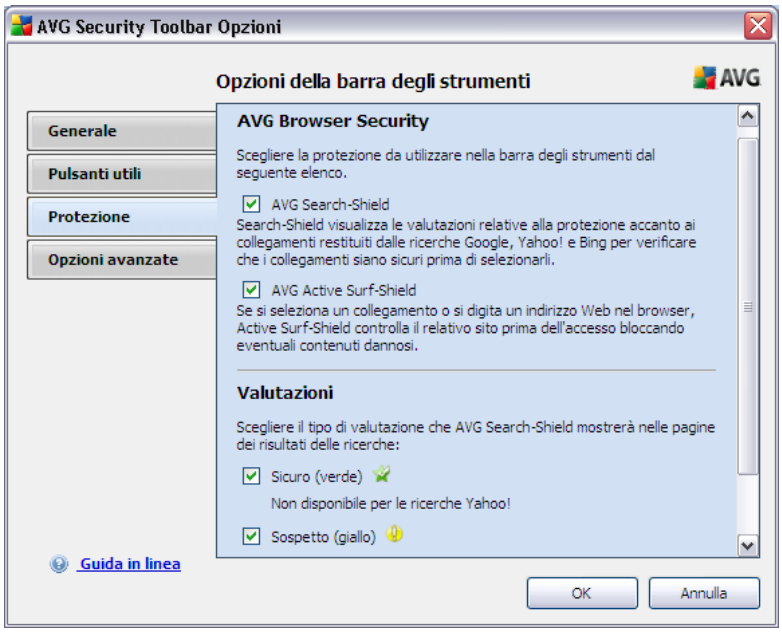
- ***Pulsante Novità di AVG***: questo pulsante consente di aprire la pagina Web contenente i comunicati stampa più recenti relativi a AVG
- ***Pulsante Novità***: questo pulsante fornisce una panoramica articolata delle ultime notizie presenti sui vari quotidiani
- ***Pulsante Informazioni su AVG***: questo pulsante offre informazioni sulla barra degli strumenti di AVG, sulle minacce correnti e sul livello di minacce in Internet, apre l'enciclopedia dei virus e fornisce ulteriori notizie correlate ai prodotti AVG
- ***Pulsante Elimina cronologia***: questo pulsante consente di utilizzare le opzioni Elimina cronologia completa oppure Elimina cronologia ricerche, Elimina cronologia browser, Elimina cronologia download oppure Elimina cookie direttamente dal riquadro AVG Security Toolbar.

9.2.2. Scheda Pulsanti utili



La scheda ***Pulsanti utili*** consente di selezionare varie applicazioni da un elenco e visualizzare la relativa icona nell'interfaccia della barra degli strumenti. L'icona servirà quindi come collegamento rapido e consentirà di avviare la relativa applicazione immediatamente.

9.2.3. Scheda Protezione

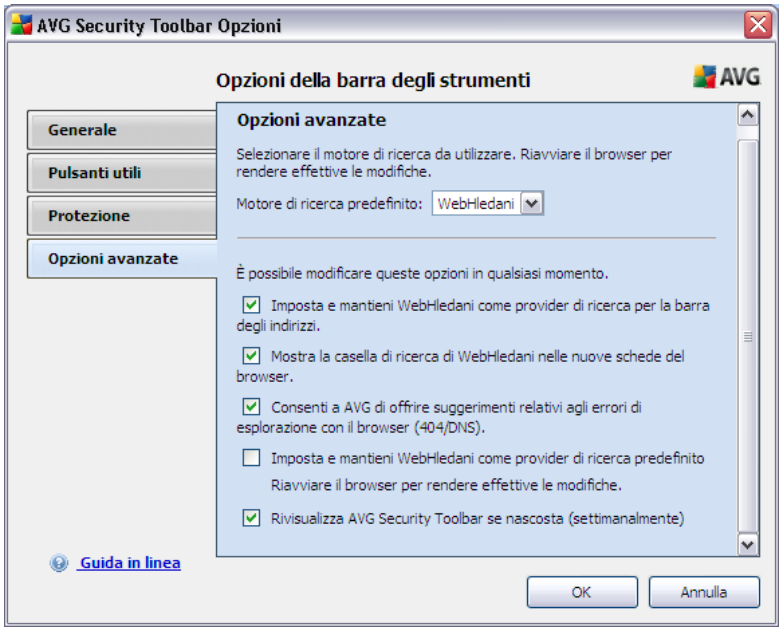


La scheda ***Protezione*** è divisa in due sezioni, ***AVG Browser Security*** e ***Valutazioni***, in cui è possibile selezionare caselle di controllo specifiche per determinare la funzionalità di ***AVG Security Toolbar*** da utilizzare:

- ***AVG Browser Security***: selezionare questa voce per attivare o disattivare i servizi ***AVG Search-Shield*** e/o ***AVG Active Surf-Shield***
- ***Valutazioni***: selezionare i simboli grafici utilizzati per le valutazioni dei risultati di ricerca dal componente ***AVG Search-Shield*** che si desidera utilizzare:
  - o  la pagina è sicura
  - o  la pagina è sospetta
  - o  la pagina contiene collegamenti a pagine sicuramente pericolose
  - o  la pagina contiene minacce attive
  - o  la pagina non è accessibile, pertanto non è stato possibile eseguirne la scansione

Selezionare l'opzione pertinente per confermare che si desidera essere informati sullo specifico livello di minaccia. La visualizzazione del contrassegno rosso assegnato alle pagine contenenti minacce attive e pericolose, tuttavia, non può essere disattivata. ***Si consiglia nuovamente di mantenere la configurazione predefinita impostata dal fornitore del programma a meno che non siano presenti motivi validi per modificarla.***

9.2.4. Scheda Opzioni avanzate



Nella scheda ***Opzioni avanzate*** selezionare innanzitutto il motore di ricerca predefinito da utilizzare. È possibile scegliere tra *Yahoo!, Baidu, WebHledani* e *Yandex*. Se il motore di ricerca predefinito viene modificato, riavviare il browser Internet per rendere effettiva la modifica.

Inoltre, è possibile attivare o disattivare altre impostazioni specifiche di ***AVG Security Toolbar***:

- ***Imposta e mantieni Yahoo! come provider di ricerca per la barra degli indirizzi***: (*attivata per impostazione predefinita*) se selezionata, questa opzione consente di digitare una parola chiave per la ricerca direttamente nella barra degli indirizzi del browser Internet; il servizio Yahoo! verrà utilizzato automaticamente per ricercare i siti Web correlati.

- ***Consenti ad AVG di fornirti suggerimenti relativi agli errori di navigazione***

con il browser (404/DNS): (*attivata per impostazione predefinita*) se, durante la ricerca sul Web, ci si imbatte in una pagina inesistente o in una pagina che non è possibile visualizzare (errore 404), si verrà automaticamente reindirizzati a una pagina Web che consente di effettuare la selezione da una panoramica di pagine alternative correlate all'argomento.

- ***Imposta e mantieni Yahoo! come provider di ricerca per il browser***: (*disattivata per impostazione predefinita*) Yahoo! è il motore di ricerca predefinito per la ricerca Web in AVG Security Toolbar e, attivando questa opzione, può inoltre diventare il motore di ricerca predefinito per il browser Web.

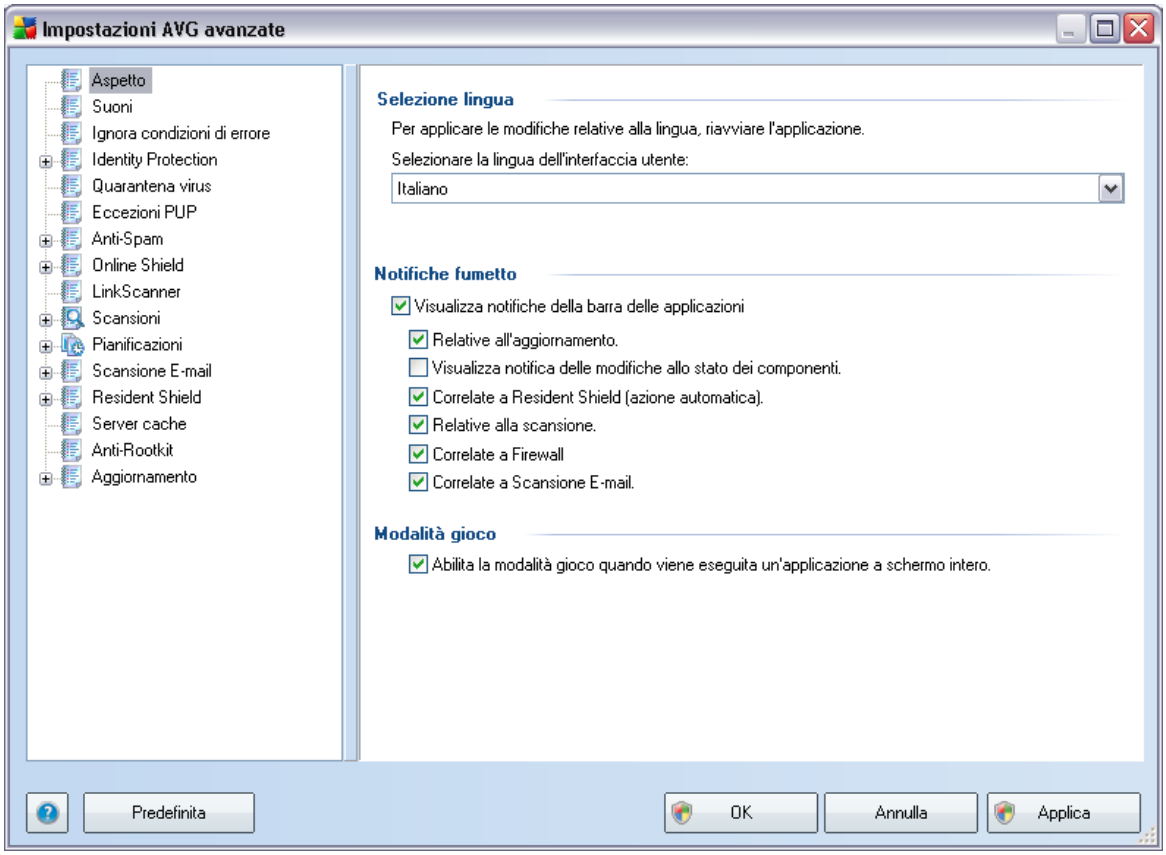
- ***Rivisualizza AVG Security Toolbar se nascosta (settimanalmente)***: (*attivata per impostazione predefinita*) se ***AVG Security Toolbar*** viene nascosta accidentalmente, questa opzione consente di visualizzarla nuovamente entro una settimana.

10. Impostazioni AVG avanzate

Le opzioni di configurazione avanzata di **AVG 9 Anti-Virus** sono disponibili 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.

10.1. Aspetto

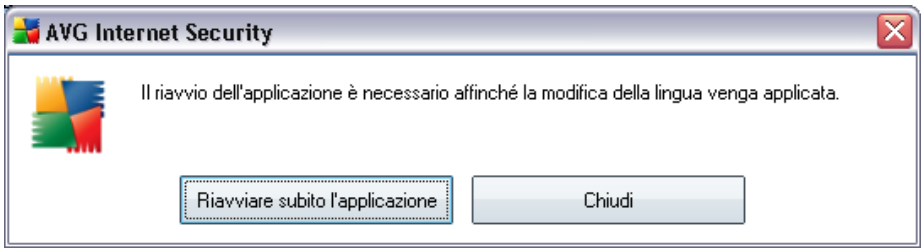
La prima voce della struttura di esplorazione, ***Aspetto***, fa riferimento alle impostazioni generali di Interfaccia utente di AVG e ad alcune opzioni di base del comportamento dell'applicazione:



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 facendo clic sul pulsante ***Applica*** (nell'angolo inferiore destro)
- Fare clic sul pulsante ***OK*** per confermare
- Viene visualizzata una nuova finestra di dialogo che comunica che la modifica della lingua dell'Interfaccia utente di AVG richiede il riavvio dell'applicazione:



Notifiche tramite fumetto

All'interno di questa sezione è possibile disattivare la visualizzazione delle notifiche tramite fumetto presenti sulla barra delle applicazioni 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 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 dell'icona della barra delle applicazioni (cambio di colore) per indicare un problema di un componente di AVG;

- ***Visualizza notifiche della barra delle applicazioni relative a Resident Shield***: consente di decidere se visualizzare o meno le informazioni relative ai processi di salvataggio, copia e apertura dei file (*questa configurazione è disponibile solo se l'opzione Correzione automatica di Resident Shield è attiva*);

- ***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;

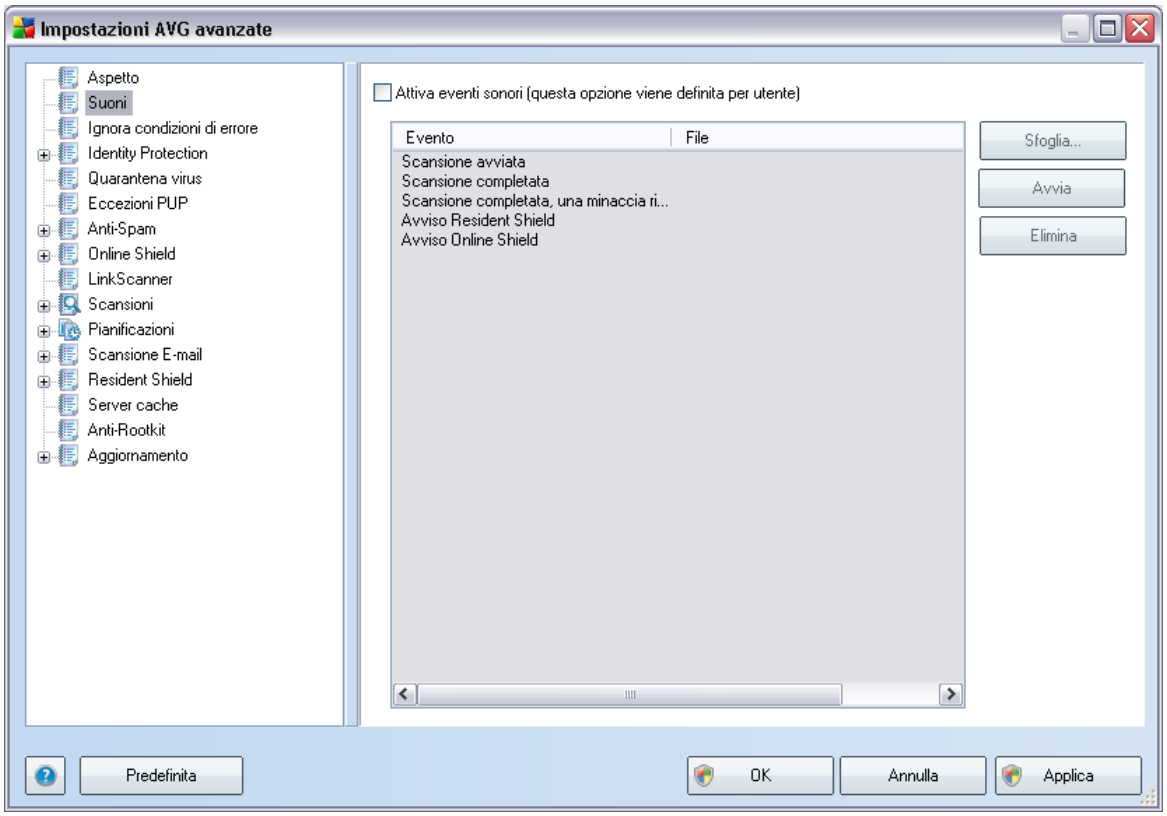
- ***Visualizza notifiche della barra delle applicazioni correlate a Scansione E-mail***: consente di decidere se visualizzare le informazioni relative alla scansione di tutti i messaggi e-mail in entrata e in uscita.

Modalità gioco

Questa funzione di AVG è stata progettata per le applicazioni a schermo intero, per le quali eventuali notifiche tramite fumetto di AVG (*visualizzate ad esempio all'avvio di una scansione pianificata*) potrebbero rappresentare una fonte di disturbo (*riducendole a icona o alterandone la grafica*). Per evitare questa situazione, mantenere selezionata la casella di controllo dell'opzione ***Abilita la modalità gioco quando viene eseguita un'applicazione a schermo intero*** (*impostazione predefinita*).

10.2. Suoni

Nella finestra di dialogo ***Suoni*** è possibile specificare se si desidera essere informati circa specifiche azioni di AVG tramite una notifica sonora. In caso affermativo, selezionare l'opzione ***Attiva eventi sonori*** (*disattivata per impostazione predefinita*) per attivare l'elenco delle azioni AVG:

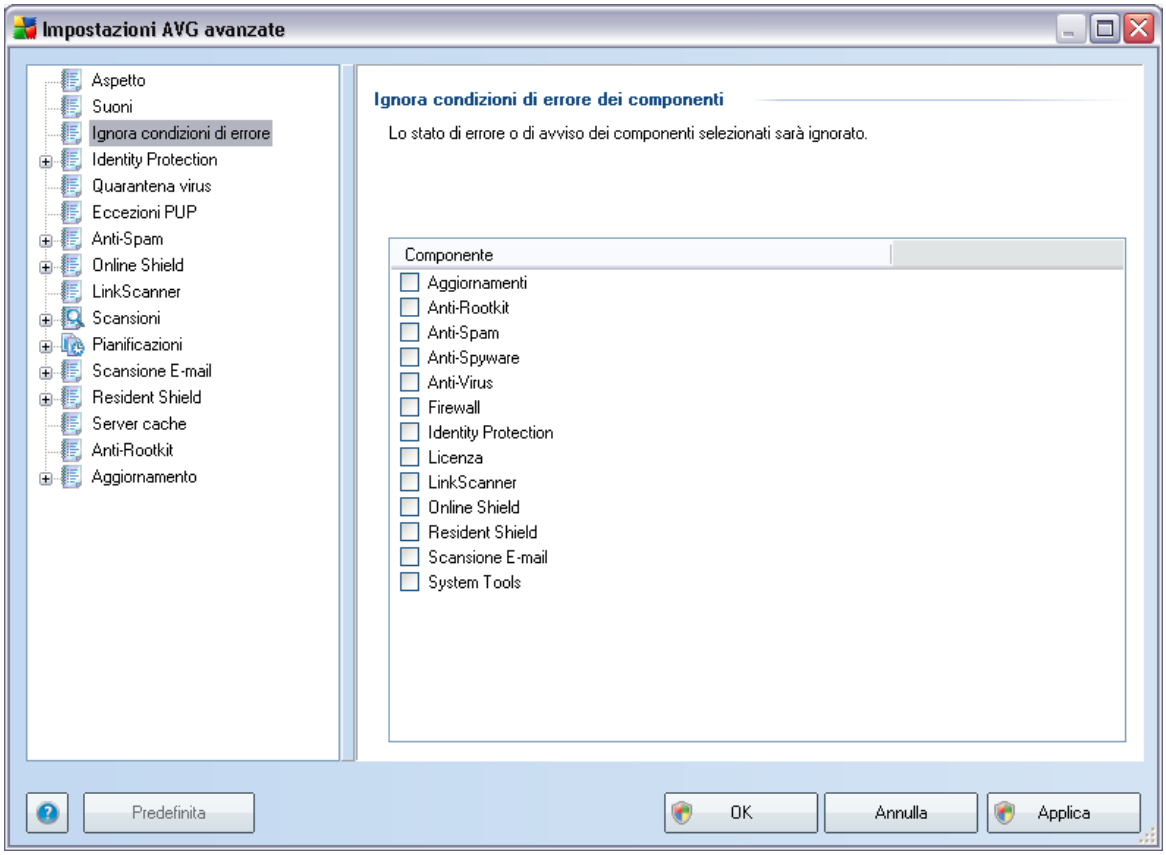


Quindi, selezionare l'evento pertinente dall'elenco e ricercare nel disco rigido (tramite ***Sfoglia***) un suono appropriato da assegnare all'evento. Per ascoltare il suono selezionato, evidenziare l'evento nell'elenco e fare clic sul pulsante ***Avvia***. Utilizzare il pulsante ***Elimina*** per rimuovere il suono assegnato a uno specifico evento.

Nota: *sono supportati solo i suoni *.wav.*

10.3. 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:

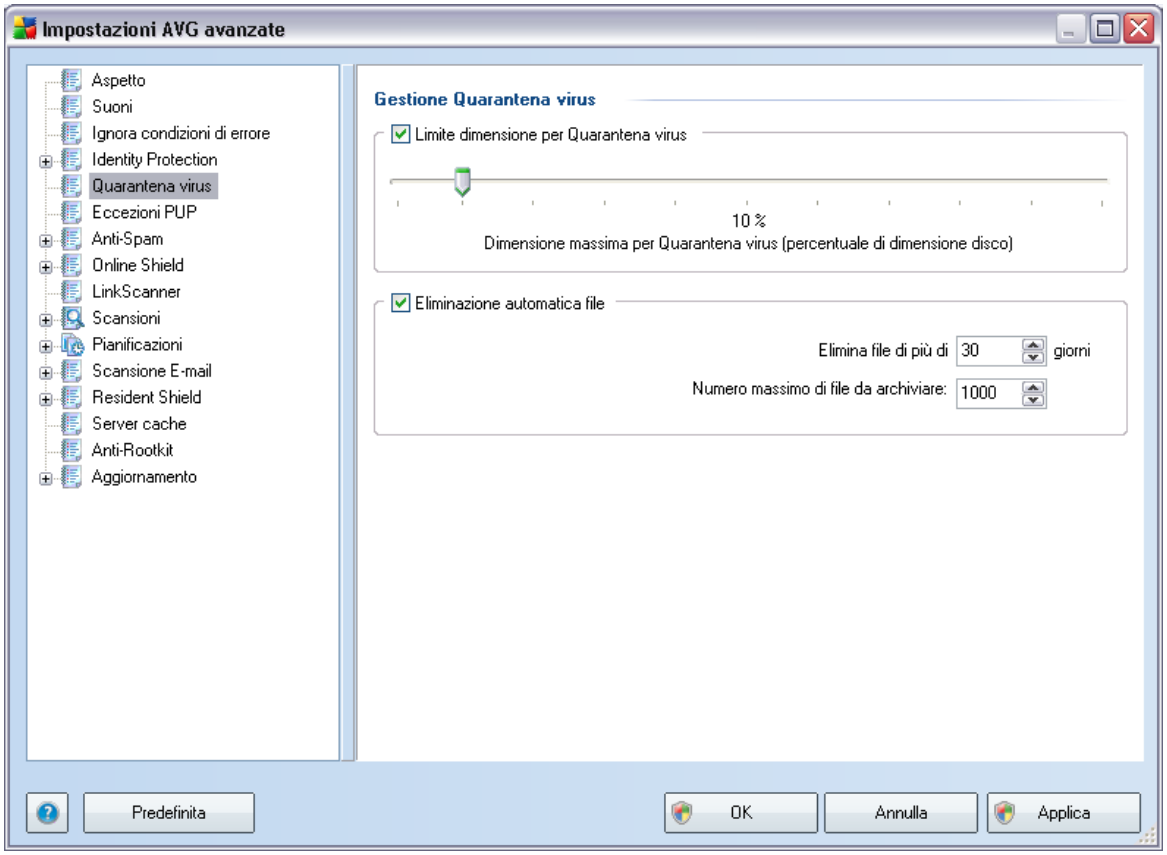
- ***l'icona presente nella barra delle applicazioni***: quando tutte le parti di AVG funzionano correttamente, l'icona viene visualizzata in quattro colori; se si verifica un errore, l'icona viene visualizzata con un punto esclamativo giallo,
- una descrizione del problema esistente visualizzata nella 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.

10.4. Quarantena virus



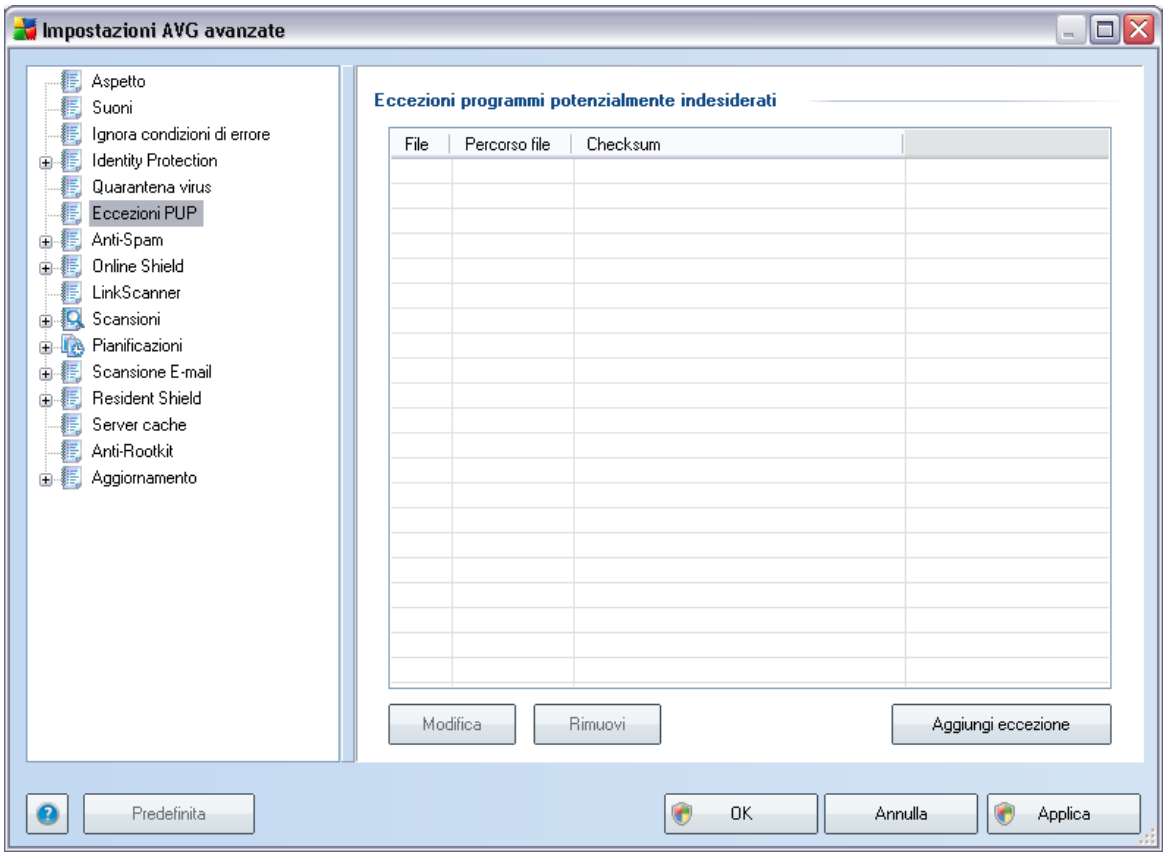
La finestra di dialogo ***Gestione Quarantena virus*** consente di definire diversi parametri relativi alla gestione degli oggetti archiviati in ***Quarantena virus***:

- ***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***)

10.5. Eccezioni PUP

AVG 9 Anti-Virus 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 scegliere 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 l'elenco, eliminare voci esistenti o aggiungere nuove eccezioni. L'elenco fornisce le seguenti informazioni per ciascuna eccezione:

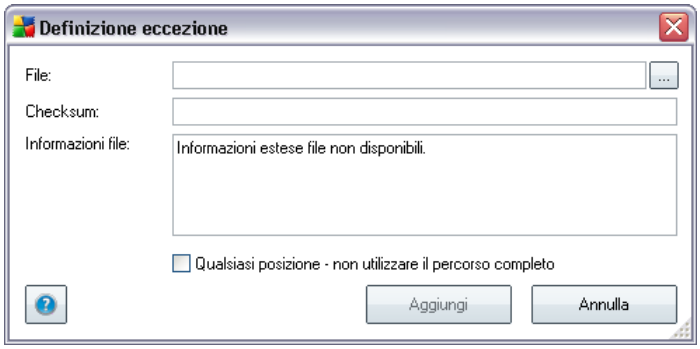
- ***File***: fornisce il nome della rispettiva applicazione
- ***Percorso file***: mostra la posizione dell'applicazione
- ***Checksum***: viene visualizzata la "firma" univoca del file prescelto. Questo checksum è una stringa di caratteri generata automaticamente che consente a AVG di distinguere in modo inequivocabile il file scelto dagli altri file. Il checksum viene generato e visualizzato dopo che il file è stato aggiunto.

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:



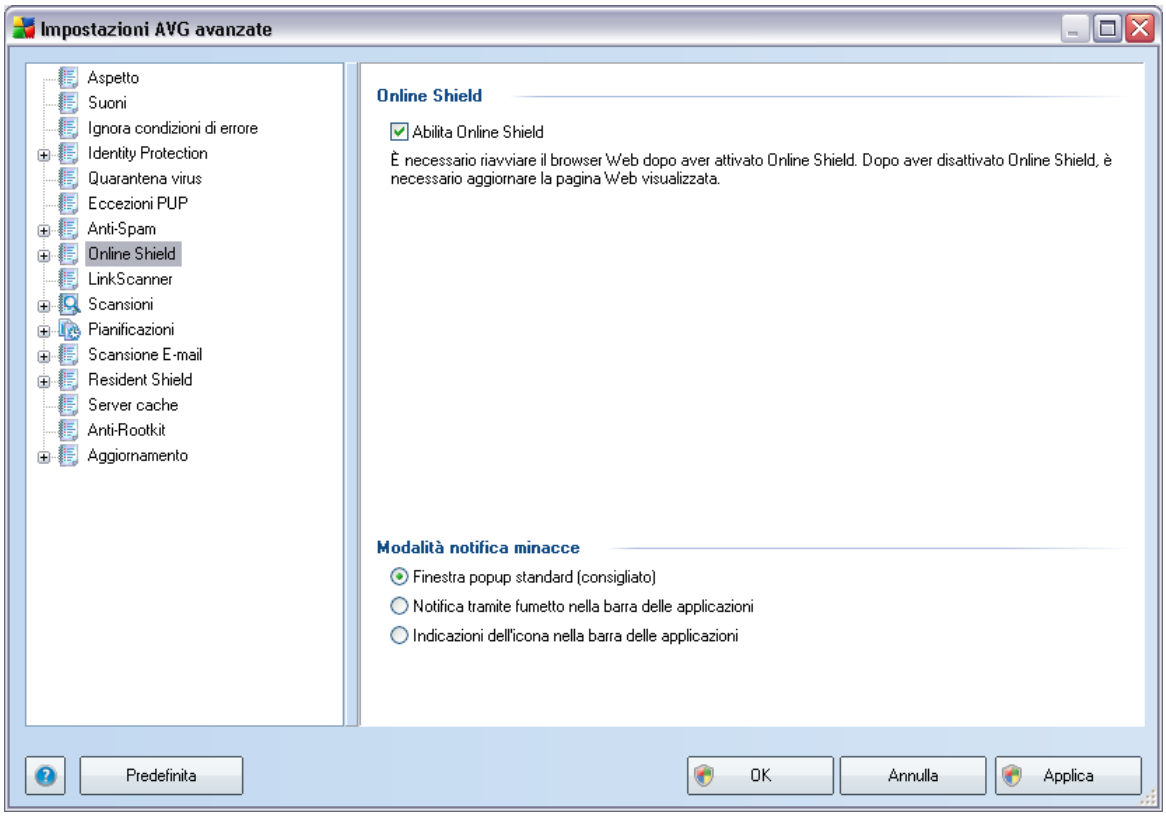
  - ***File***: digitare il percorso completo del file da contrassegnare come eccezione.

  - ***Checksum***: viene visualizzata la "firma" univoca del file prescelto. Questo checksum è una stringa di caratteri generata automaticamente che consente a 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.

  - ***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.

10.6. Online Shield



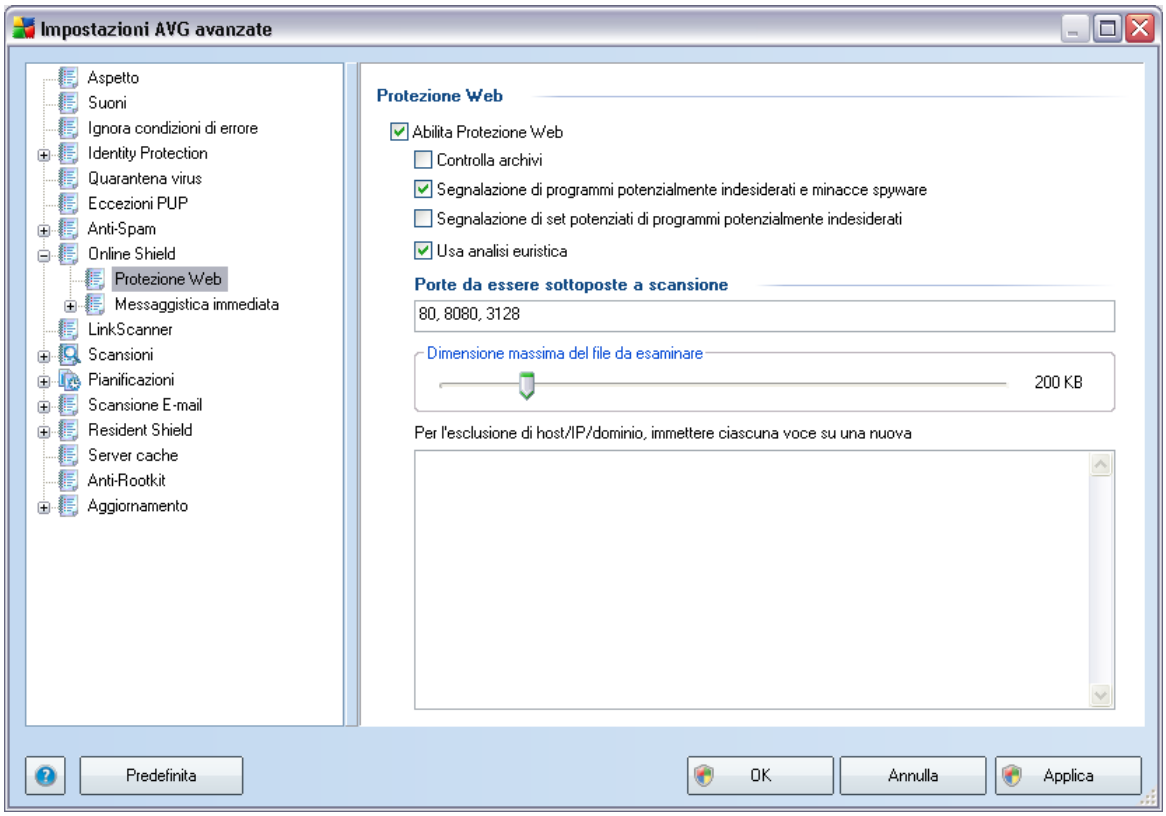
La finestra di dialogo ***Protezione Web*** consente di attivare/disattivare completamente il componente ***Online Shield*** tramite l'opzione ***Abilita Online Shield*** (*attivata per impostazione predefinita*). Per altre impostazioni avanzate del componente passare alle finestre di dialogo successive elencate nella struttura di esplorazione:

- ***Protezione Web***
- ***Messaggistica immediata***

Modalità notifica minacce

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 le informazioni dell'icona nella barra delle applicazioni.

10.6.1. 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:

- ***Abilita protezione Web***: questa opzione conferma l'esecuzione della scansione del contenuto delle pagine Web da parte del componente ***Online 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.
    - ***Segnalazione di programmi potenzialmente indesiderati e minacce spyware*** – (*attivata per impostazione predefinita*) selezionare questa casella di controllo per attivare il motore ***Anti-Spyware*** ed eseguire la scansione per ricercare spyware e virus. Gli spyware rappresentano una categoria di malware anomala: anche se solitamente costituiscono un

rischio per la sicurezza, alcuni di questi programmi possono essere installati intenzionalmente. Si consiglia di mantenere questa funzionalità attivata in quanto consente di aumentare la protezione del computer.

- ***Segnalazione di set potenziati di programmi potenzialmente indesiderati*** – se la precedente opzione è attivata, è inoltre possibile selezionare questa casella per rilevare pacchetti estesi di spyware: programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita.

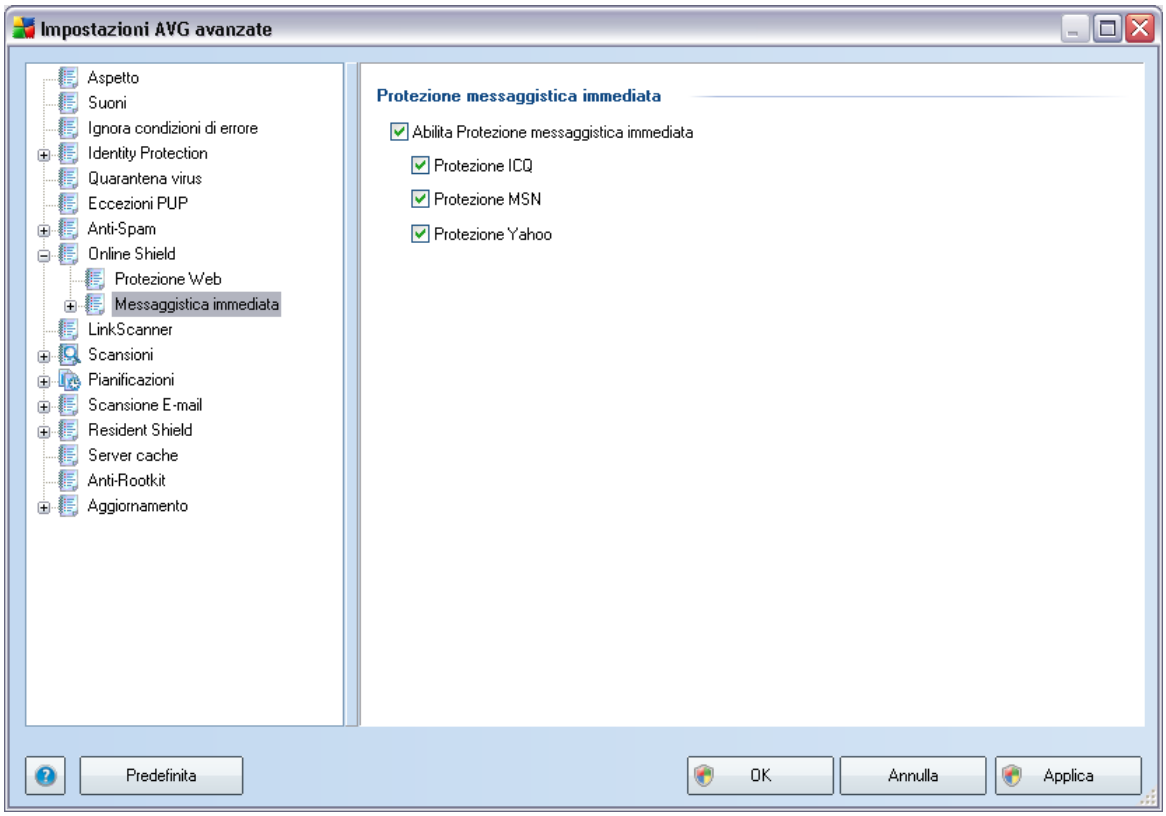
- ***Usa analisi euristica***: consente di eseguire la scansione del contenuto della pagina da visualizzare utilizzando il metodo dell'analisi euristica (*emulazione dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale*).

- ***Porte da sottoporre a scansione*** : 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 massima del file da esaminare***: se i file inclusi sono presenti nella pagina visualizzata, è inoltre possibile eseguire la scansione del relativo contenuto prima che questi 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 da ***Online Shield***. Anche se le dimensioni del file scaricato sono superiori a quelle specificate, quindi il file non verrà sottoposto a scansione da Online Shield, 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 ***Online Shield***. Pertanto, escludere un host solo se si è assolutamente certi che non fornirà mai contenuti Web pericolosi.

10.6.2. Instant Messaging

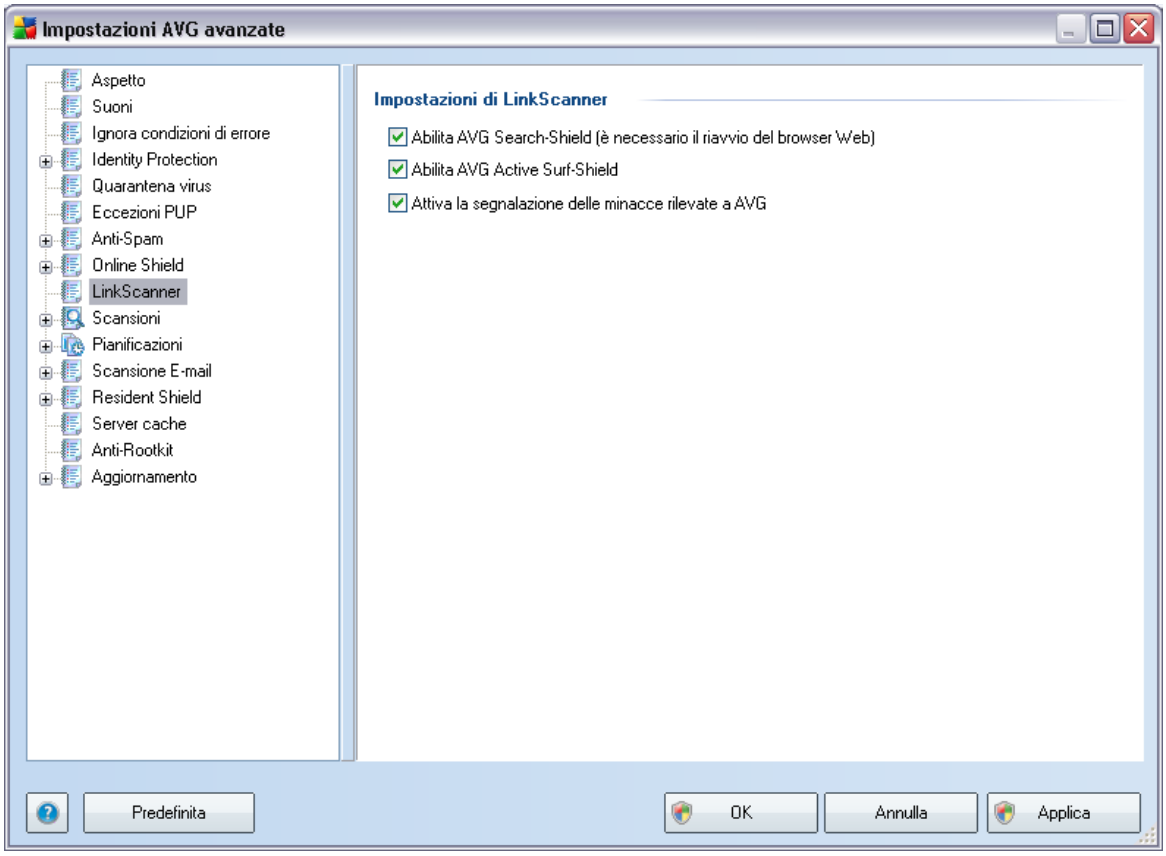


Nella finestra di dialogo ***Protezione messaggistica immediata*** è possibile modificare le impostazioni dei componenti di ***Online Shield*** che si riferiscono alla scansione della messaggistica immediata. Attualmente sono supportati tre programmi di messaggistica immediata: ***ICQ***, ***MSN*** e ***Yahoo***. Selezionare la voce corrispondente per ciascuno di essi se si desidera che ***Online 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, Yahoo avanzato***) e specificare la ***Whitelist*** (*l'elenco di utenti che saranno autorizzati a comunicare*) e la ***Blacklist*** (*gli utenti che devono essere bloccati*).

10.7. Link Scanner

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



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

- ***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*).

- ***Attiva la segnalazione delle minacce rilevate ad AVG***: (*attivata per*

impostazione predefinita) selezionare questa voce per attivare la segnalazione di siti fraudolenti e dannosi trovati dall'utente mediante ***AVG Active Surf-Shield*** o ***AVG Search-Shield*** e consentire la raccolta di informazioni nell'apposito database in merito ad attività dannose svolte sul Web.

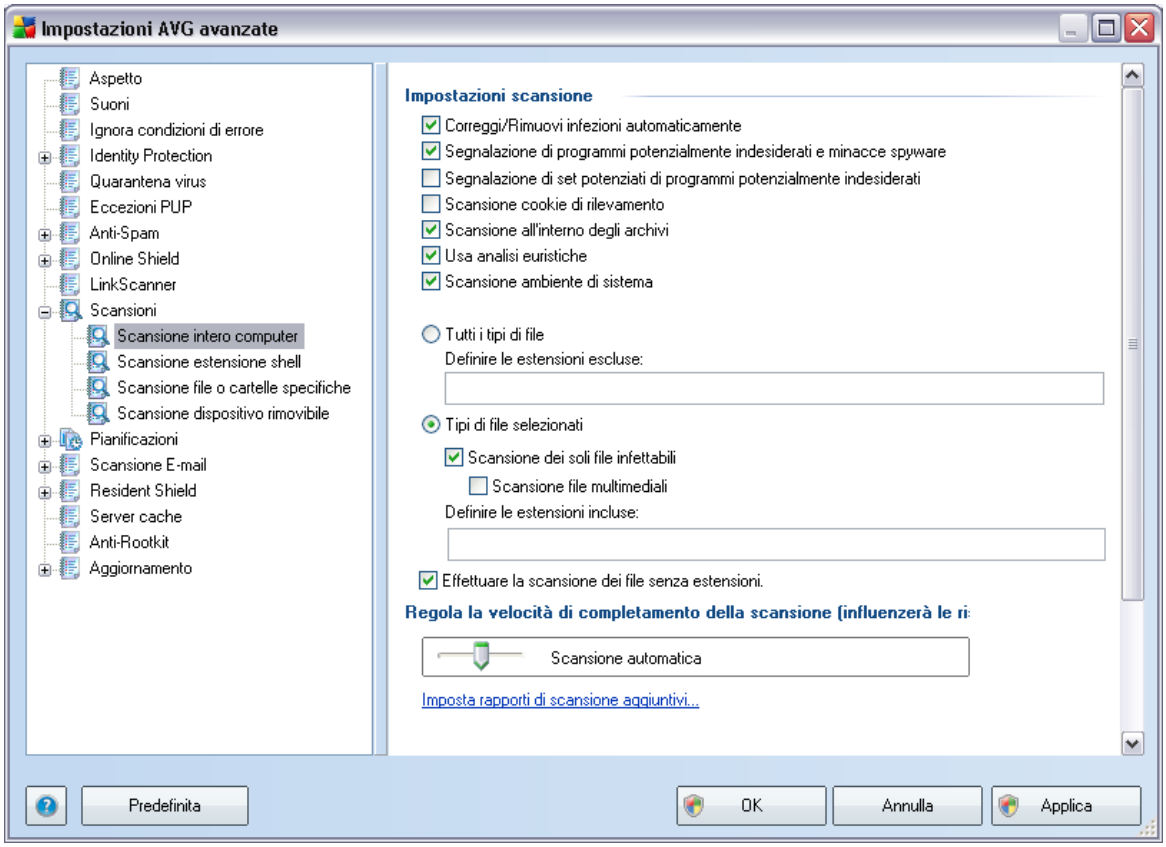
10.8. Scansioni

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

10.8.1. 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 può essere corretto automaticamente, l'oggetto infetto verrà spostato in ***Quarantena virus***.
- ***Segnalazione di programmi potenzialmente indesiderati e minacce***

spyware – (*attivata per impostazione predefinita*) selezionare questa casella di controllo per attivare il motore ***Anti-Spyware*** ed eseguire la scansione per ricercare spyware e virus. Gli spyware rappresentano una categoria di malware anomala: anche se solitamente costituiscono un rischio per la sicurezza, alcuni di questi programmi possono essere installati intenzionalmente. Si consiglia di mantenere questa funzionalità attivata in quanto consente di aumentare la protezione del computer.

- ***Segnalazione di set potenziati di programmi potenzialmente indesiderati*** – se la precedente opzione è attivata, è inoltre possibile selezionare questa casella per rilevare pacchetti estesi di spyware: programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita.

- ***Scansione cookie di rilevamento***: 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 o 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.

Quindi è necessario decidere se si desidera sottoporre a scansione

- ***Tutti i tipi di file***: è possibile definire eccezioni fornendo un elenco di estensioni di file separate da virgola (*dopo il salvataggio, le virgole si trasformano in punto e virgola*) da non sottoporre a scansione;

- ***Tipi di file selezionati***: è possibile specificare che si desidera sottoporre a scansione solo file potenzialmente infettabili (*i file che non possono essere infettati non verranno sottoposti a scansione, ad esempio alcuni file di testo normale o altri file non eseguibili*), inclusi i file multimediali (*file video e audio; se non si seleziona questa casella, il tempo di scansione risulterà ulteriormente ridotto, poiché questi file sono spesso di grandi dimensioni e non*

facilmente infettabili dai virus.). Anche in questo caso, è possibile specificare tramite le estensioni quali file devono essere sempre sottoposti a scansione.

- Facoltativamente, è possibile sottoporre a scansione i file senza estensione tramite ***Effettuare la scansione dei file senza estensioni***: questa opzione è attivata per impostazione predefinita e si consiglia di non modificare questa impostazione a meno che non siano presenti motivi validi per farlo. I file senza estensione sono piuttosto sospetti e devono essere sempre sottoposti a scansione.

Priorità processi di scansione

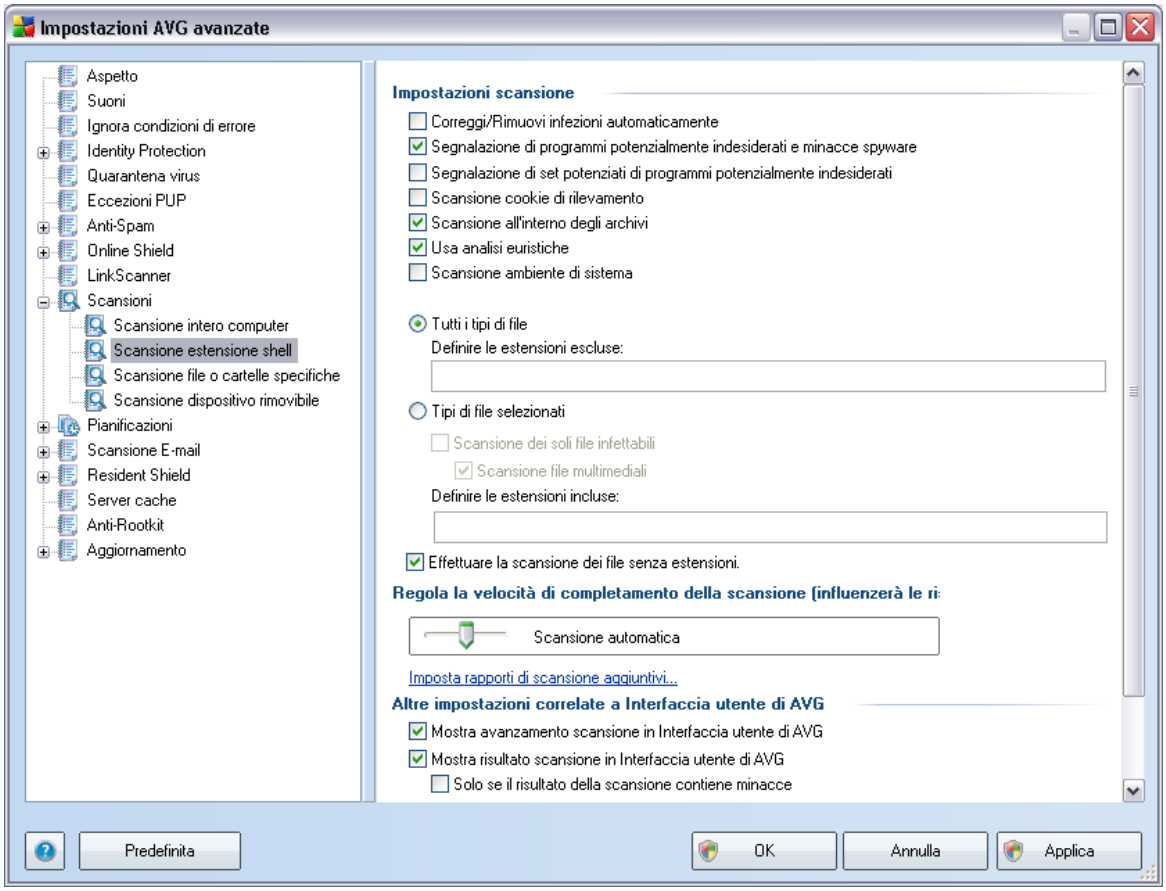
All'interno della sezione ***Priorità processi di scansione*** è inoltre possibile specificare la velocità di scansione desiderata in base all'utilizzo delle risorse di sistema. Per impostazione predefinita, il valore di questa opzione è impostato sul livello medio di utilizzo automatico delle risorse. 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:

10.8.2. 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***:

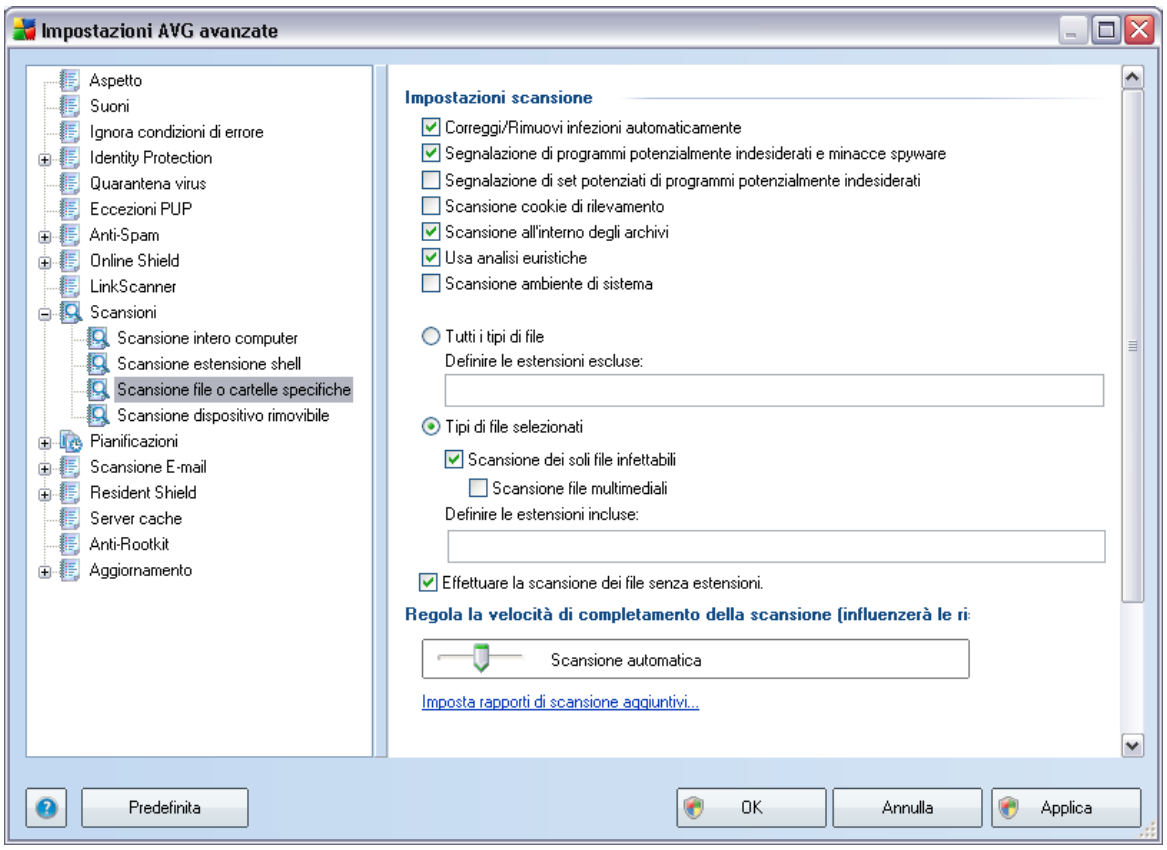


L'elenco dei parametri è identico a quello disponibile per ***Scansione intero computer***. Tuttavia, le impostazioni predefinite sono diverse: con ***Scansione intero computer*** la maggior parte dei parametri è selezionata, mentre per ***Scansione estensione shell*** (***Scansione in Esplora risorse***)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

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

10.8.3. 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***:

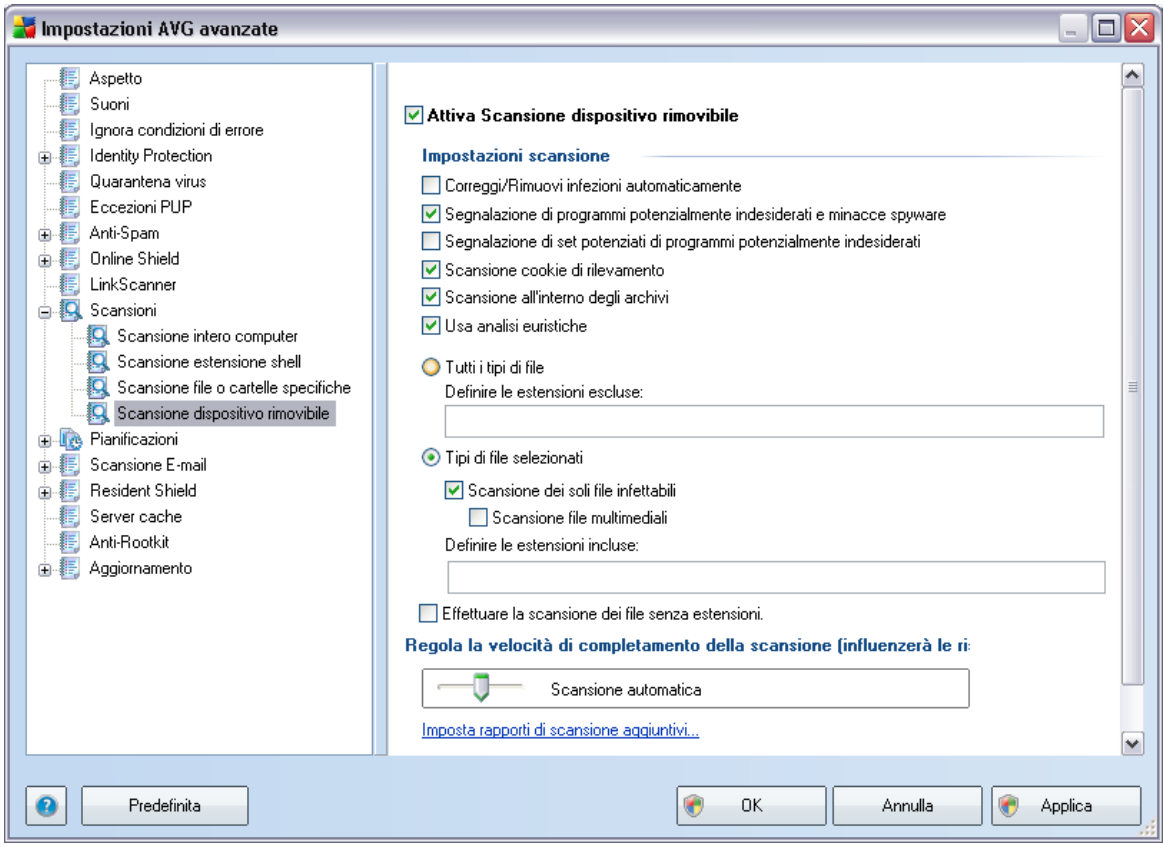


Tutti i parametri impostati in questa finestra di dialogo di configurazione si applicano solo alle aree selezionate per la scansione con il comando ***Scansione file o cartelle specifiche***!

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

10.8.4. 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***.

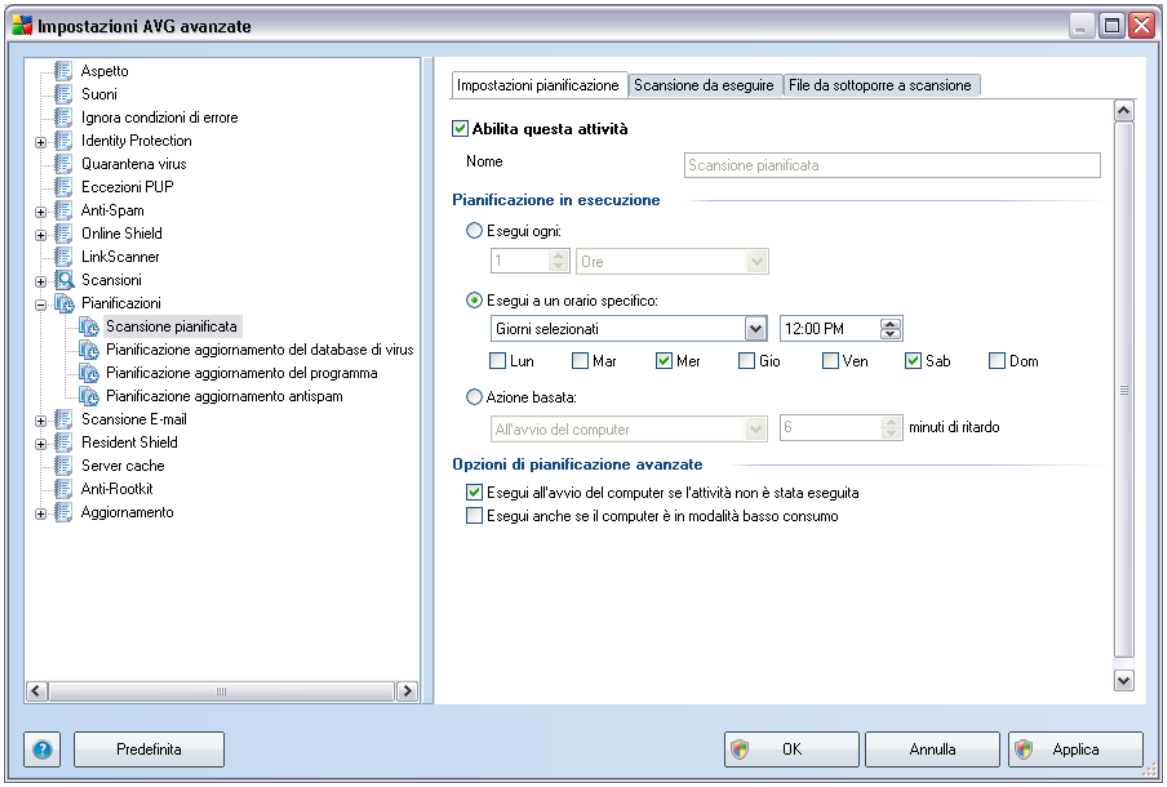
10.9. Pianificazioni

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

- Pianificazione scansione intero computer
- Pianificazione aggiornamento del database di virus
- Pianificazione aggiornamento del programma

10.9.1. 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, nel campo di testo ***Nome*** (*disattivato per tutte le pianificazioni predefinite*) è presente il nome assegnato alla pianificazione in oggetto dal fornitore del programma. Per le pianificazioni aggiunte successivamente (*è possibile aggiungere una nuova pianificazione facendo clic con il pulsante destro del mouse sulla voce* ***Scansione pianificata*** *nella struttura di esplorazione a sinistra*) è possibile specificare un nome personalizzato. In tal caso, il campo di testo sarà attivo per la modifica. Denominare le scansioni assegnando sempre 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 selezionati.*

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

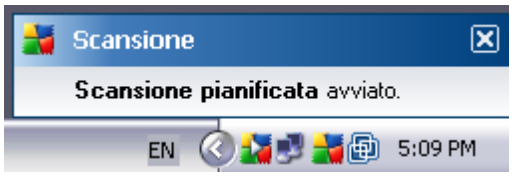
Pianificazione in esecuzione

Consente di specificare gli intervalli di tempo per l'avvio della nuova scansione pianificata. È possibile definire l'ora tramite l'avvio ripetuto della scansione dopo un certo periodo di tempo (***Esegui ogni...***) oppure specificando data e ora esatte (***Esegui a determinati intervalli di tempo...***) o specificando un evento a cui dovrà essere associato l'avvio della scansione (***Azione in base all'avvio del computer***).

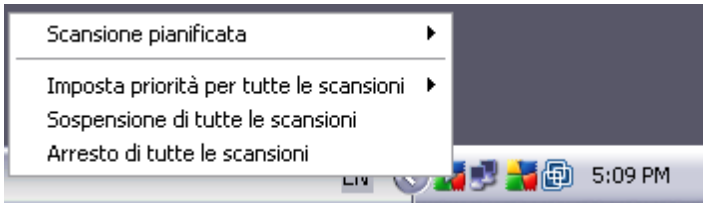
Opzioni di pianificazione avanzate

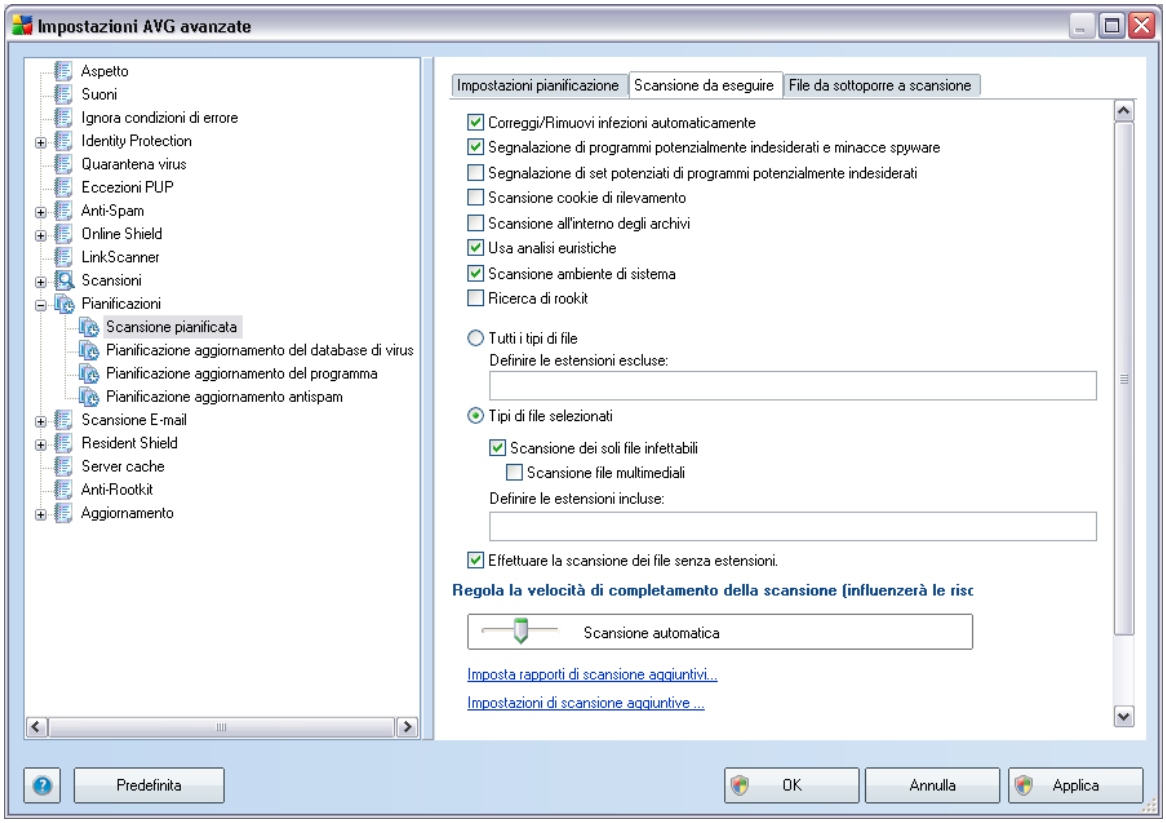
Questa sezione consente di definire le circostanze in cui deve essere avviata o non avviata la scansione se il computer si trova in modalità basso consumo oppure se è completamente spento.

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***: 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, l'oggetto infetto verrà spostato in ***Quarantena virus***.

- ***Segnalazione di programmi potenzialmente indesiderati e minacce spyware*** – (*attivata per impostazione predefinita*) selezionare questa casella di controllo per attivare il motore ***Anti-Spyware*** ed eseguire la scansione per ricercare spyware e virus. Gli spyware rappresentano una categoria di malware anomala: anche se solitamente costituiscono un rischio per la sicurezza, alcuni di questi programmi possono essere installati

intenzionalmente. Si consiglia di mantenere questa funzionalità attivata in quanto consente di aumentare la protezione del computer.

- ***Segnalazione di set potenziati di programmi potenzialmente indesiderati*** – se la precedente opzione è attivata, è inoltre possibile selezionare questa casella per rilevare pacchetti estesi di spyware: programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita.

- ***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 o 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*) 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*** : (*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 in versione autonoma all'interno del componente ***Anti-Rootkit*** ;

Quindi è necessario decidere se si desidera sottoporre a scansione

- ***Tutti i tipi di file***: è possibile definire eccezioni fornendo un elenco di estensioni di file separate da virgola (*dopo il salvataggio, le virgole si trasformano in punto e virgola*) da non sottoporre a scansione;

- ***Tipi di file selezionati***: è possibile specificare che si desidera sottoporre a scansione solo file potenzialmente infettabili (*i file che non possono essere infettati non verranno sottoposti a scansione, ad esempio alcuni file di testo normale o altri file non eseguibili*), inclusi i file multimediali (*file video e audio;*

se non si seleziona questa casella, il tempo di scansione risulterà ulteriormente ridotto, poiché questi file sono spesso di grandi dimensioni e non facilmente infettabili dai virus.). Anche in questo caso, è possibile specificare tramite le estensioni quali file devono essere sempre sottoposti a scansione.

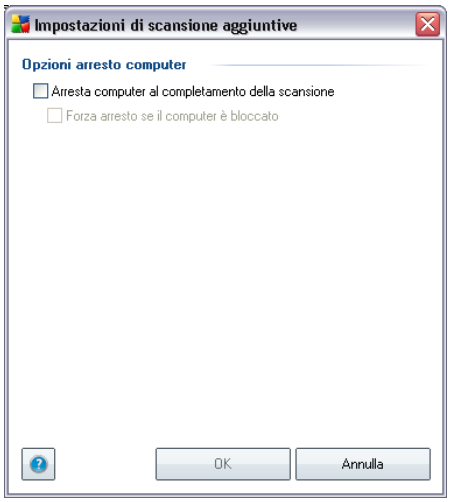
- Facoltativamente, è possibile sottoporre a scansione i file senza estensione tramite ***Effettuare la scansione dei file senza estensioni***: questa opzione è attivata per impostazione predefinita e si consiglia di non modificare questa impostazione a meno che non siano presenti motivi validi per farlo. I file senza estensione sono piuttosto sospetti e devono essere sempre sottoposti a scansione.

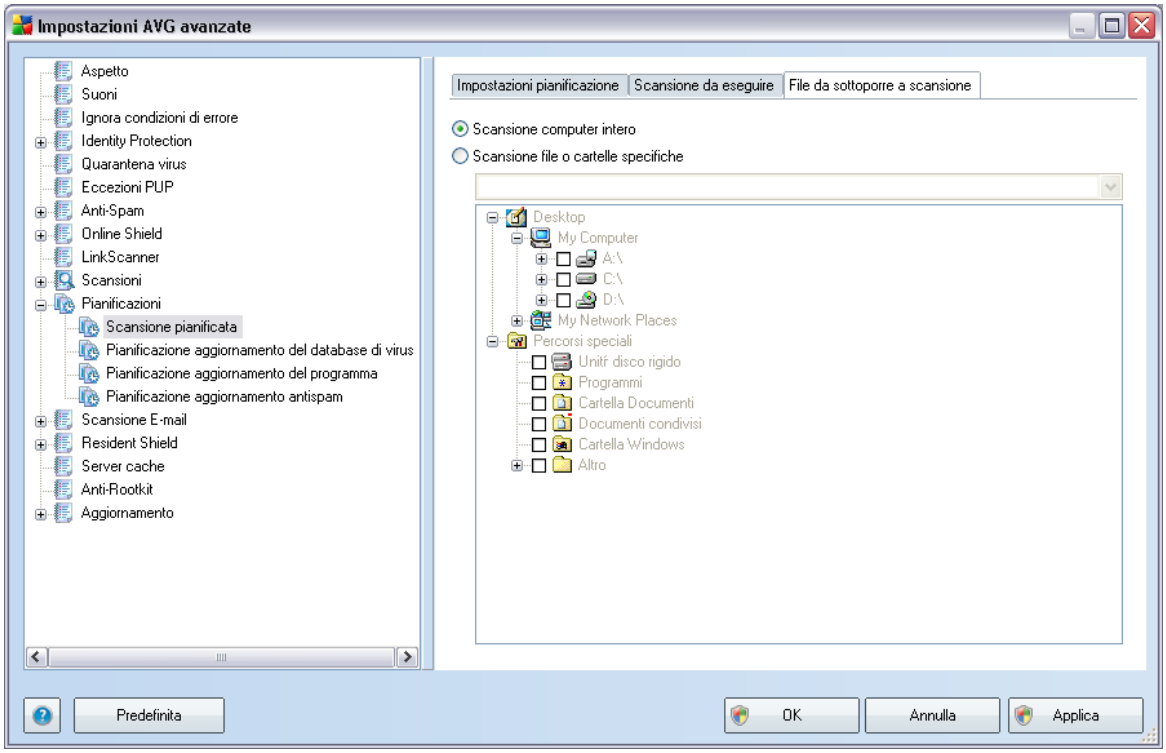
Priorità processi di scansione

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, 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 arrestato 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***).

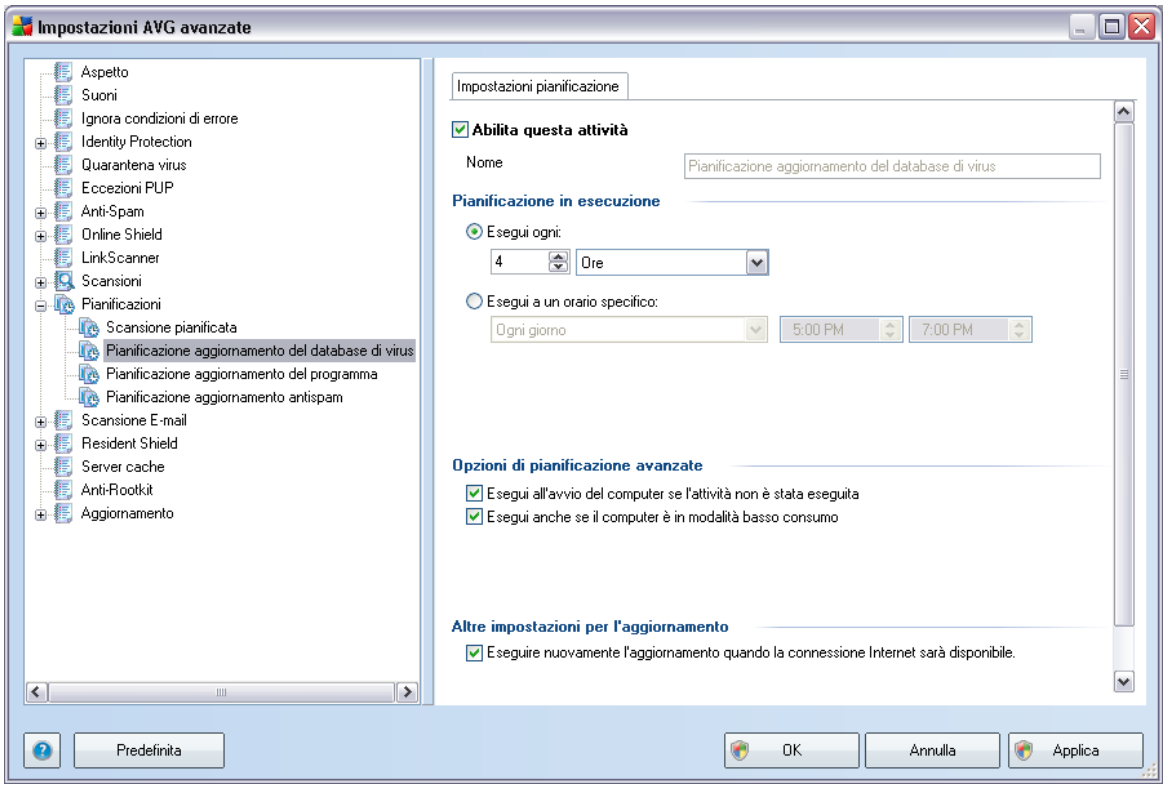




Nella scheda ***File da sottoporre a scansione*** è possibile definire se si desidera pianificare la scansione dell'intero computer o la scansione di file o cartelle specifiche.

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.

10.9.2. 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 dei virus viene eseguita all'interno del componente ***Gestore aggiornamenti***. Da questa finestra di dialogo è possibile impostare alcuni parametri dettagliati della pianificazione dell'aggiornamento del database di virus. Nel campo di testo ***Nome*** (*disattivato per tutte le pianificazioni predefinite*) è presente il nome assegnato alla pianificazione in oggetto dal fornitore del programma.

Pianificazione in esecuzione

In questa sezione, specificare gli intervalli di tempo per l'avvio del nuovo aggiornamento del database dei virus pianificato. L'intervallo può essere definito tramite l'avvio dell'aggiornamento ripetuto dopo un determinato periodo di tempo (***Esegui ogni...***) oppure specificando una data e un'ora esatte (***Esegui a un orario specifico...***).

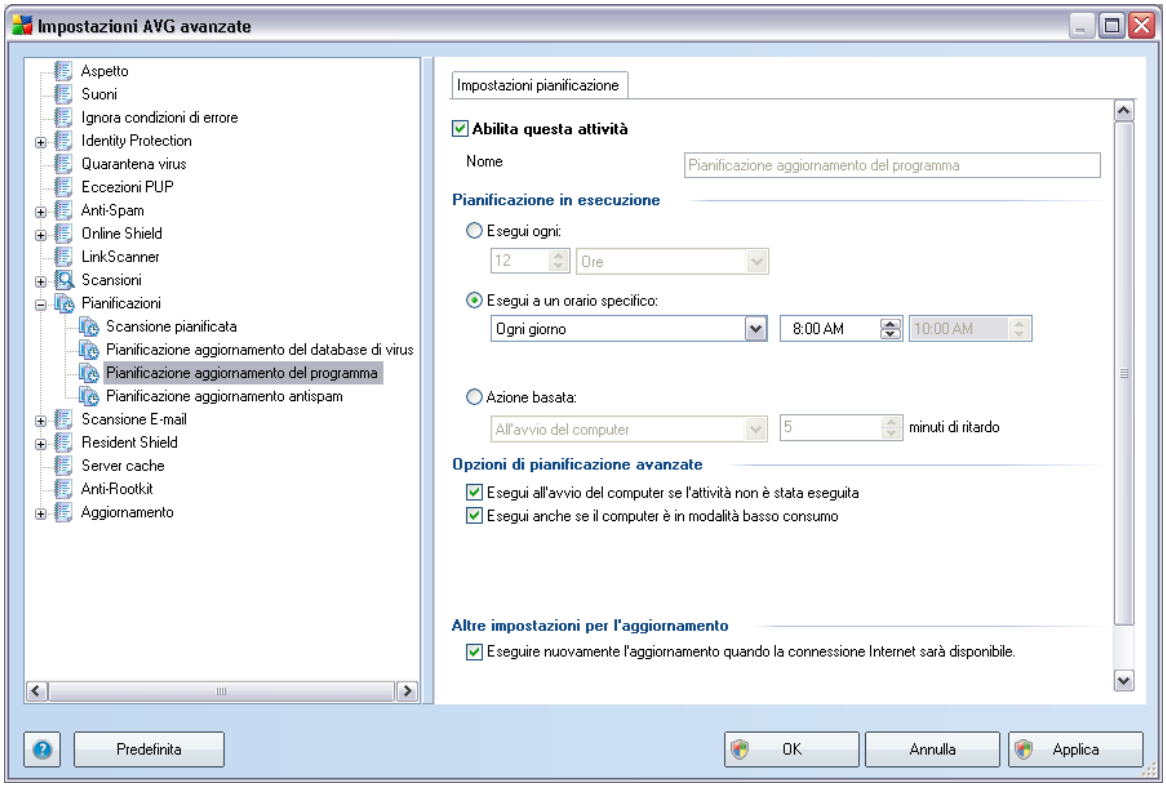
Opzioni di pianificazione avanzate

Questa sezione consente di definire le circostanze in cui deve o non deve essere avviato l'aggiornamento del database dei virus se il computer si trova in modalità basso consumo oppure se è completamente spento.

Altre impostazioni per l'aggiornamento

Infine, selezionare l'opzione ***Eseguire nuovamente l'aggiornamento quando la connessione Internet sarà disponibile*** per assicurarsi che, se la connessione Internet si interrompesse e il processo di aggiornamento non riuscisse, tale processo venga avviato di nuovo subito dopo il ripristino della connessione Internet.

Quando l'aggiornamento pianificato viene avviato 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***).



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. Nel campo di testo ***Nome*** (*disattivato per tutte le pianificazioni predefinite*) è presente il nome assegnato alla pianificazione in oggetto dal fornitore del programma.

Pianificazione in esecuzione

Consente di specificare gli intervalli di tempo per l'avvio del nuovo aggiornamento del programma pianificato. È possibile definire l'ora tramite l'avvio ripetuto dell'aggiornamento dopo un certo periodo di tempo (***Esegui ogni...***) oppure definendo data e ora esatte (***Esegui a un orario specifico...***) o 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.

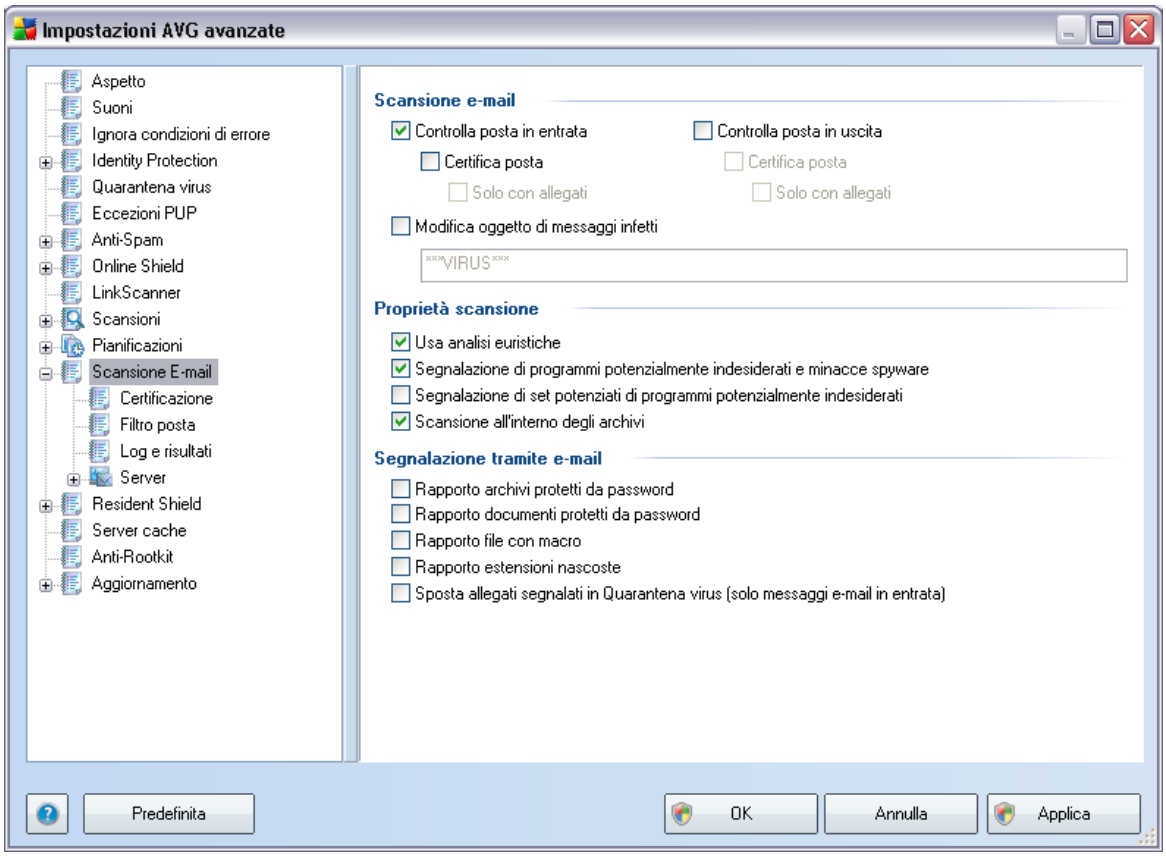
Altre impostazioni per l'aggiornamento

Selezionare l'opzione ***Eseguire nuovamente l'aggiornamento quando la connessione Internet sarà disponibile*** per assicurarsi che, se la connessione Internet si interrompesse e il processo di aggiornamento non riuscisse, tale processo venga avviato di nuovo subito dopo il ripristino della connessione Internet.

Quando l'aggiornamento pianificato viene avviato 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***).

Nota: *se gli orari di un aggiornamento del programma pianificato e di una scansione pianificata dovessero coincidere, il processo di aggiornamento acquista priorità e la scansione viene interrotta.*

10.10. Scansione E-mail



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

- ***Scansione e-mail*** - in questa sezione è possibile configurare le seguenti impostazioni di base per i messaggi e-mail in arrivo e/o in uscita:
    - Se deve essere eseguita la scansione dei messaggi e-mail alla ricerca di virus.
    - Se il testo di certificazione deve essere aggiunto alla fine di ciascun messaggio per indicare che il messaggio non contiene virus. Il testo può essere modificato nella finestra di dialogo Certificazione.
    - Se il testo di certificazione deve essere aggiunto soltanto ai messaggi con allegati.

Per ***modificare l'oggetto dei messaggi infetti da virus***, selezionare la casella di controllo e digitare il valore desiderato nella casella di testo. Il testo verrà aggiunto al campo oggetto di ogni messaggio infetto per facilitarne l'identificazione e il filtro. Il valore predefinito è ***VIRUS***. Si consiglia di mantenere questo valore.

- ***Proprietà scansione*** - in questa sezione è possibile specificare la modalità di scansione dei messaggi e-mail:
    - ***Usa analisi euristiche*** – selezionare questa casella di controllo per utilizzare il metodo di rilevamento dell'analisi euristica durante la scansione dei messaggi e-mail. Se questa opzione è attivata, è possibile filtrare gli allegati dei messaggi e-mail non solo per estensione ma anche in base al contenuto effettivo dell'allegato. Il filtro può essere impostato nella finestra di dialogo Filtro posta.
    - ***Segnalazione di programmi potenzialmente indesiderati e minacce spyware*** – (*attivata per impostazione predefinita*) selezionare questa casella di controllo per attivare il motore ***Anti-Spyware*** ed eseguire la scansione per ricercare spyware e virus. Gli spyware rappresentano una categoria di malware anomala: anche se solitamente costituiscono un rischio per la sicurezza, alcuni di questi programmi possono essere installati intenzionalmente. Si consiglia di mantenere questa funzionalità attivata in quanto consente di aumentare la protezione del computer.
    - ***Segnalazione di set potenziati di programmi potenzialmente indesiderati*** – se la precedente opzione è attivata, è inoltre possibile selezionare questa casella per rilevare pacchetti estesi di spyware: programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita.
    - ***Scansione all'interno degli archivi*** - selezionare questa casella di controllo per eseguire la scansione contenuto degli archivi allegati ai messaggi e-mail.
- ***Segnalazione allegati e-mail*** - in questa sezione è possibile impostare rapporti di scansione aggiuntivi sui file potenzialmente pericolosi o sospetti. Notare che non verrà visualizzato alcun messaggio di avviso, verrà soltanto aggiunto un testo di certificazione alla fine del messaggio e-mail e tutti i rapporti verranno elencati nella finestra di dialogo Rilevamento Scansione E-mail:

- ***Segnala documenti protetti da password:*** file di archivio (ZIP, RAR e così via). protetti da password, dei quali non è possibile eseguire la scansione alla ricerca di virus. Selezionare la casella di controllo se si desidera che questi file vengano segnalati come potenzialmente pericolosi.

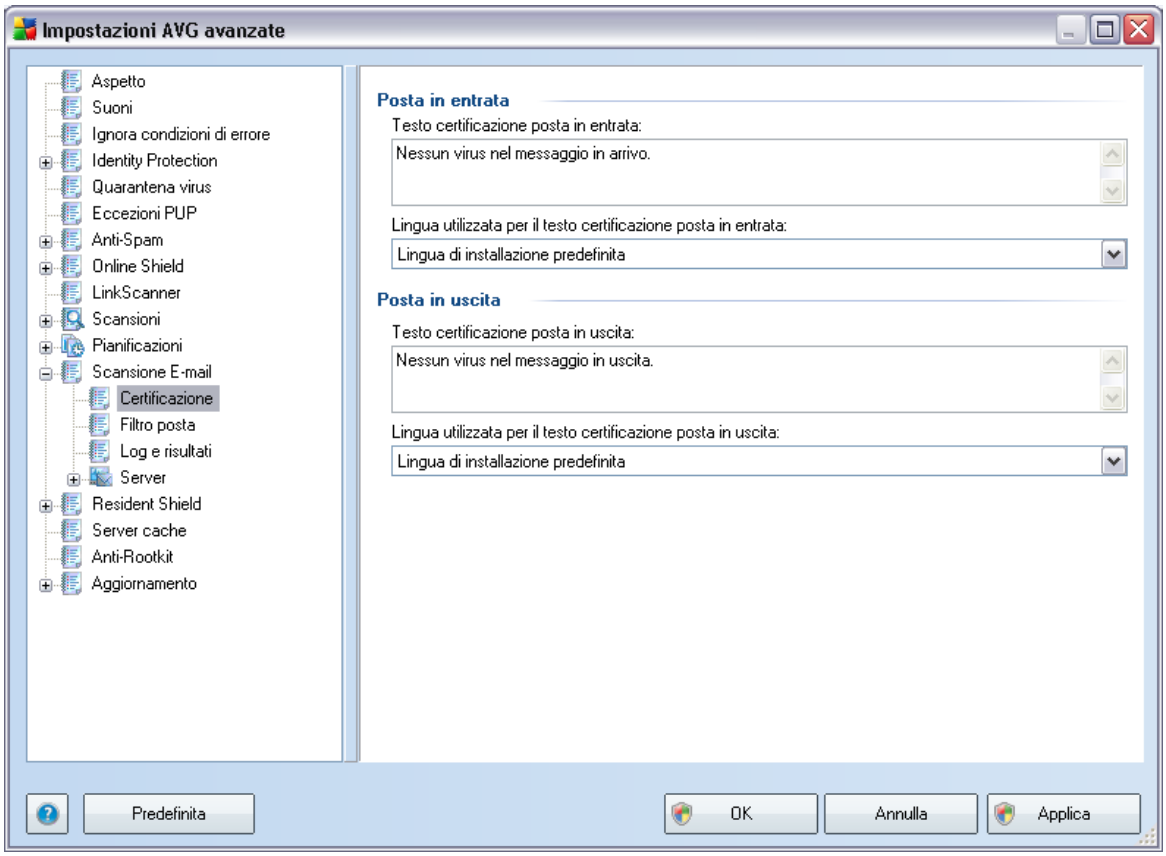
- ***Segnala documenti protetti da password*** – i documenti protetti da password non possono essere sottoposti a scansione alla ricerca di virus. Selezionare la casella di controllo se si desidera che questi file vengano segnalati come potenzialmente pericolosi.

- ***Segnala file contenenti macro*** – una macro è una sequenza di passaggi predefinita che consente di semplificare determinate attività (le macro di MS Word, ad esempio, sono ampiamente conosciute). Le macro possono contenere istruzioni potenzialmente pericolose. Selezionare la casella di controllo per assicurare che i file contenenti macro vengano segnalati come potenzialmente pericolosi.

- ***Segnala estensioni nascoste***: le estensioni nascoste possono far sembrare un file sospetto, ad esempio il file eseguibile "nomefile.txt.exe", un innocuo file di testo, ad esempio "nomefile.txt". Selezionare la casella di controllo se si desidera che questi file vengano segnalati come potenzialmente pericolosi.

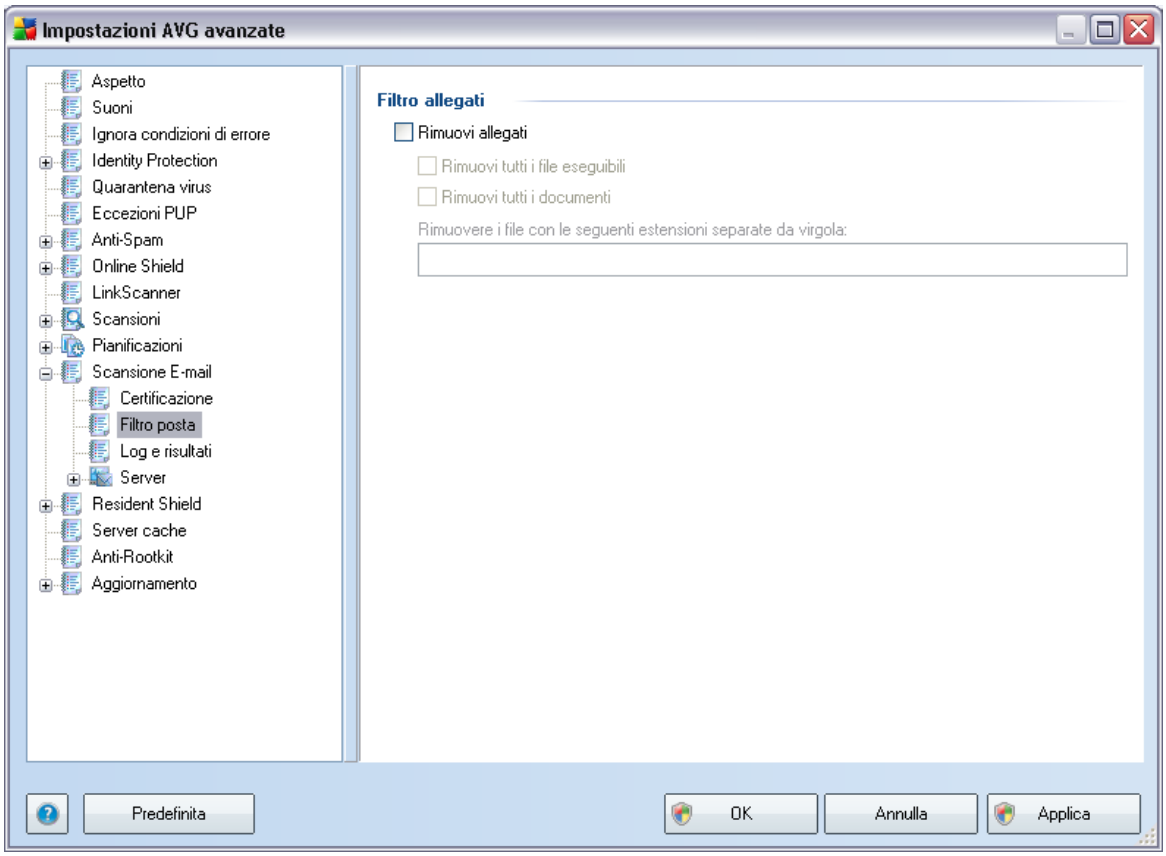
- ***Sposta allegati segnalati in Quarantena virus*** - specifica se si desidera ricevere una notifica via e-mail per gli archivi protetti da password, i documenti protetti da password, i file contenenti macro e/o i file con estensione nascosta rilevati come allegato del messaggio e-mail sottoposto a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

10.10.1. 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***.

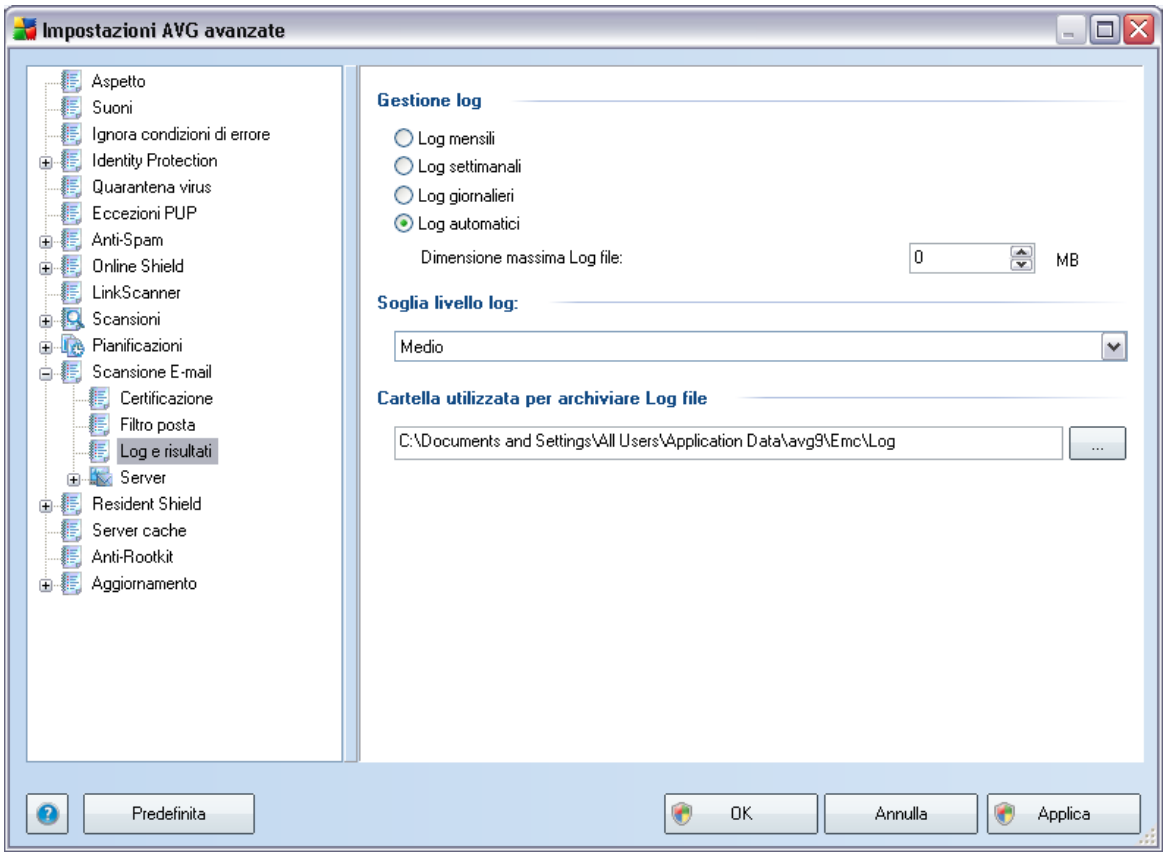
10.10.2. Filtro posta



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, *.docx, *.xls e *.xlsx verranno eliminati
- ***Rimuovere i file con le seguenti estensioni separate da virgola***: verranno rimossi tutti i file con le estensioni specificate

10.10.3. Log e risultati

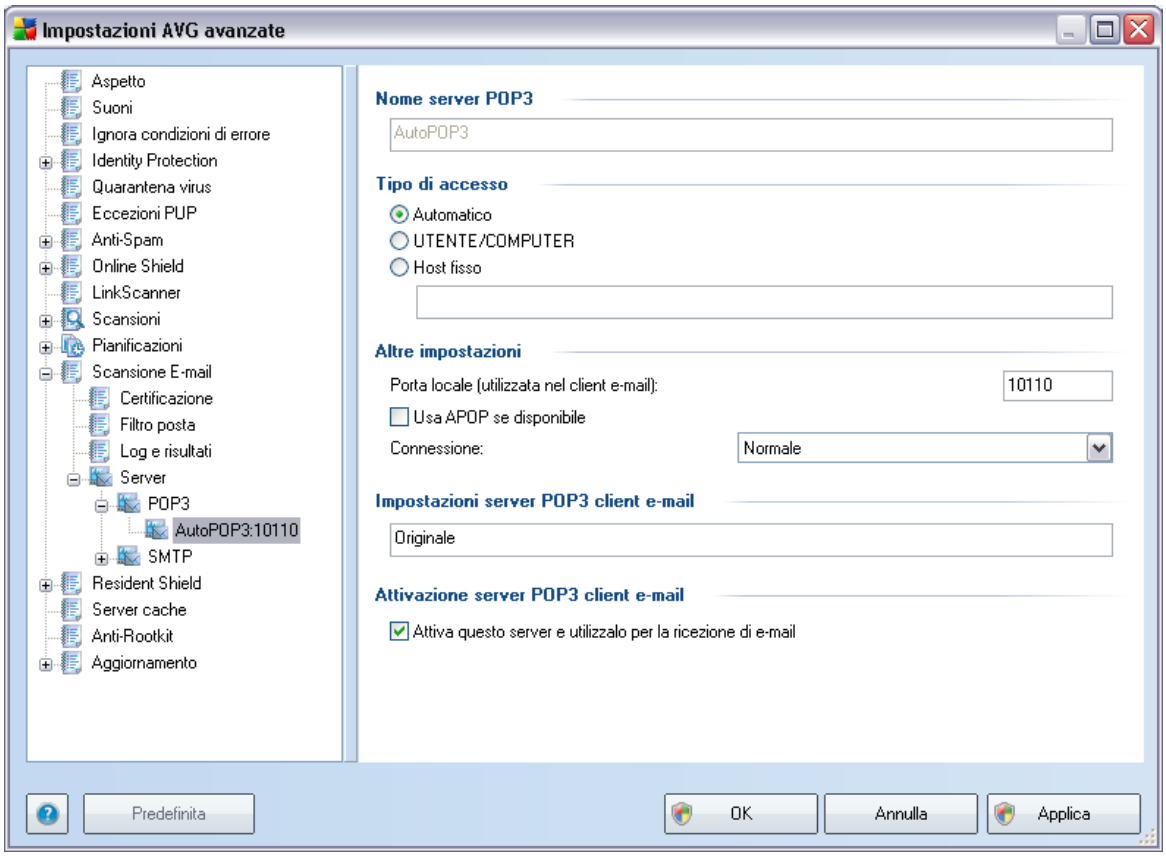


La finestra di dialogo aperta dall'elemento di spostamento ***Log e risultati*** consente di specificare i parametri per la gestione dei risultati di scansione e-mail. La finestra di dialogo è suddivisa in diverse sezioni:

- ***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

10.10.4. 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 automaticamente, in base alle impostazioni del client e-mail.

- ***UTENTE/COMPUTER***: il metodo più semplice e più frequentemente utilizzato per determinare il server e-mail di destinazione è il 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 verrà sempre utilizzato il server specificato in questo campo. 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:

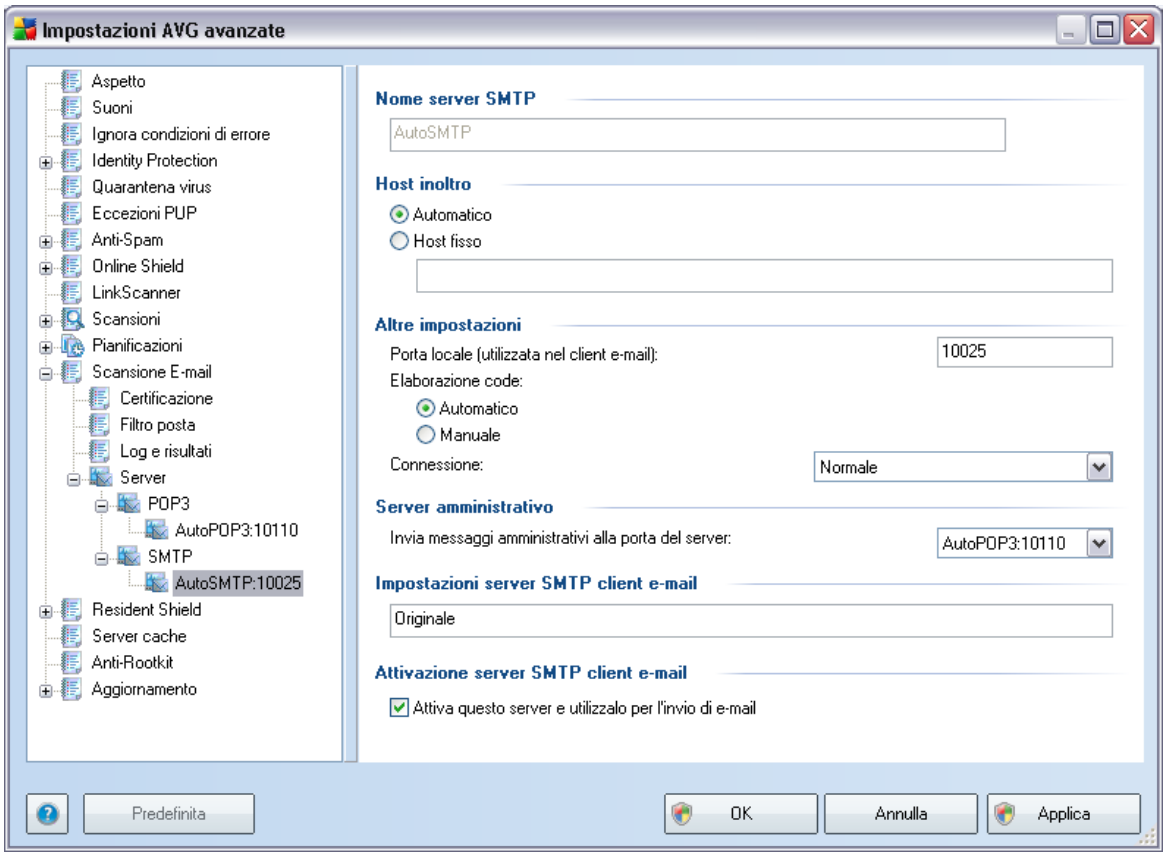
  - ***Porta locale***: specifica la porta su cui è prevista la comunicazione dall'applicazione e-mail. Nell'applicazione di posta sarà quindi necessario specificare tale porta come porta per la comunicazione POP3.

  - ***Usa APOP se disponibile***: questa opzione fornisce un accesso più protetto al server e-mail. 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***: nel 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.

- ***Impostazioni 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.

- ***Attivazione server POP3 client e-mail***: selezionare/deselezionare questa voce per attivare o disattivare il server POP3 specificato



Questa finestra di dialogo (che si apre tramite ***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:

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

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

    - 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.

  - ***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.

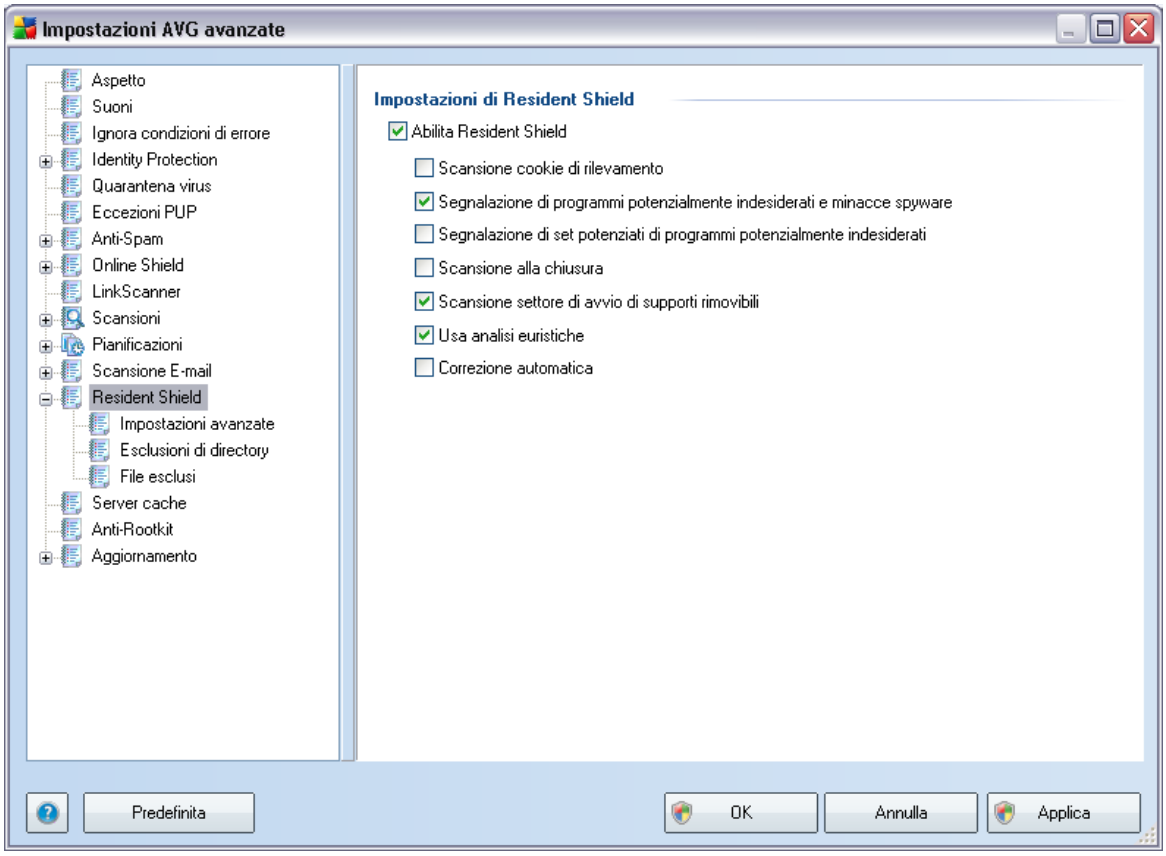
- ***Server amministrativo***: indica il numero della porta del server che verrà utilizzata per il recapito inverso dei rapporti amministrativi. Questi messaggi vengono generati, ad esempio, se il messaggio in entrata viene rifiutato dal server di posta di destinazione o se il server non è disponibile.

- ***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.

- ***Attivazione server SMTP client e-mail***: selezionare/deselezionare questa casella per attivare/disattivare il server SMTP specificato

10.11. 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 di rilevamento***: questo parametro stabilisce 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*)
- ***Segnalazione di programmi potenzialmente indesiderati e minacce***

spyware – (*attivata per impostazione predefinita*) selezionare questa casella di controllo per attivare il motore ***Anti-Spyware*** ed eseguire la scansione per ricercare spyware e virus. Gli spyware rappresentano una categoria di malware anomala: anche se solitamente costituiscono un rischio per la sicurezza, alcuni di questi programmi possono essere installati intenzionalmente. Si consiglia di mantenere questa funzionalità attivata in quanto consente di aumentare la protezione del computer.

- ***Segnalazione di set potenziati di programmi potenzialmente indesiderati*** – se la precedente opzione è attivata, è inoltre possibile selezionare questa casella per rilevare pacchetti estesi di spyware: programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita.

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

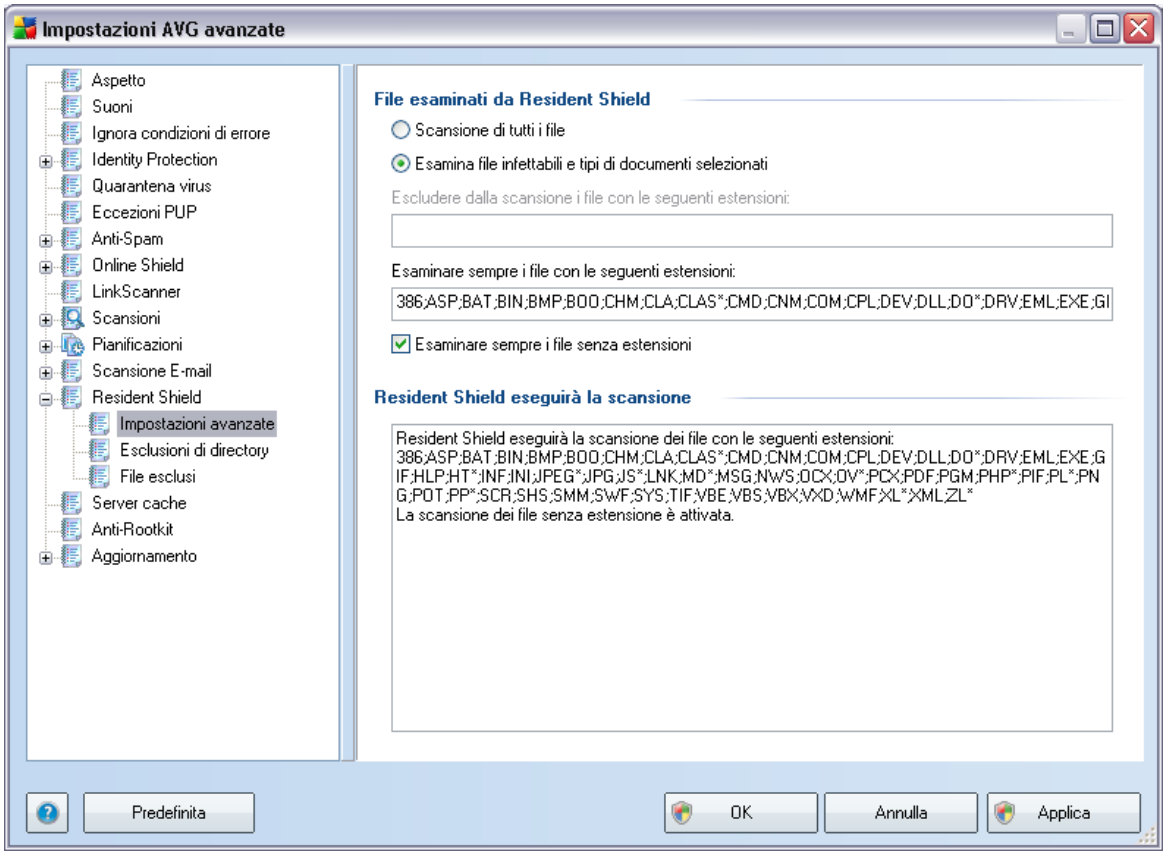
- ***Scansione settore di avvio di supporti rimovibili***: (*attivata per impostazione predefinita*)

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

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

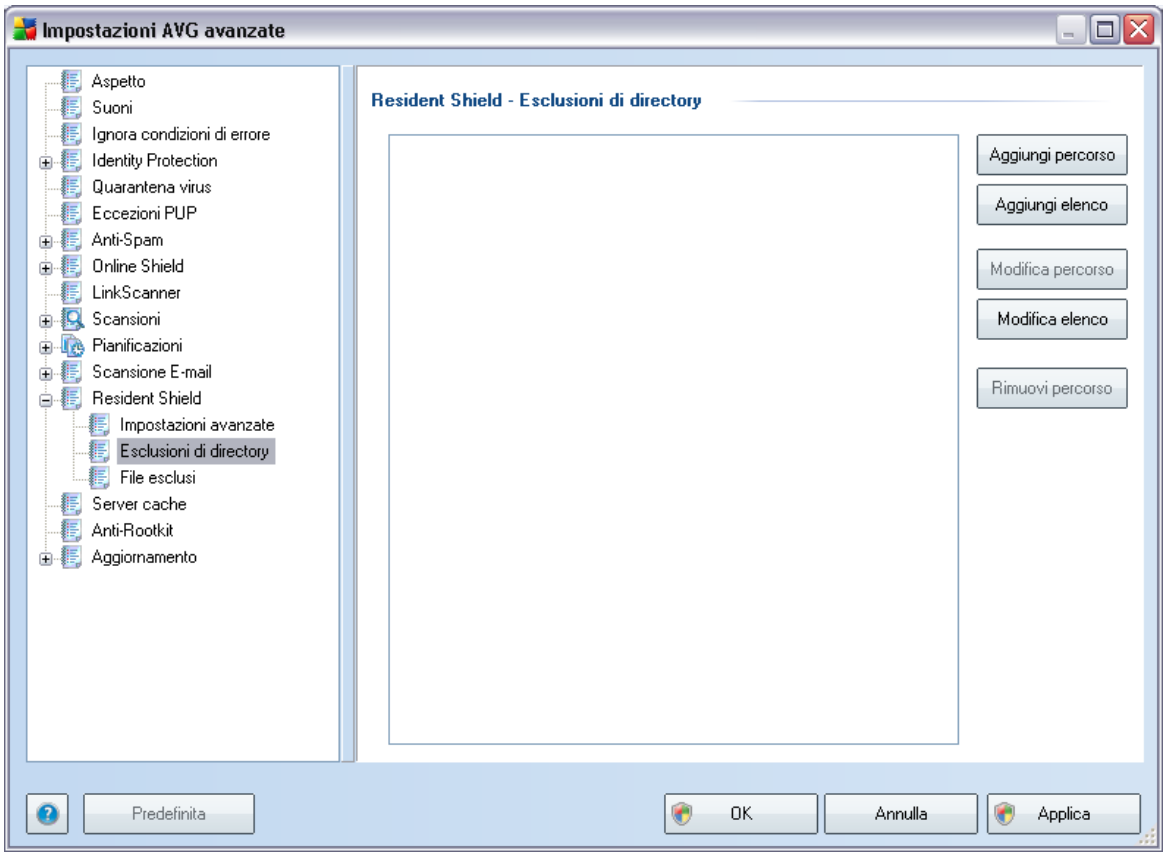
10.11.1. Impostazioni avanzate

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.

10.11.2. Esclusioni di directory



La finestra di dialogo ***Esclusioni da Resident Shield*** offre la possibilità di definire le cartelle che devono essere escluse dalla scansione di ***Resident Shield*** .

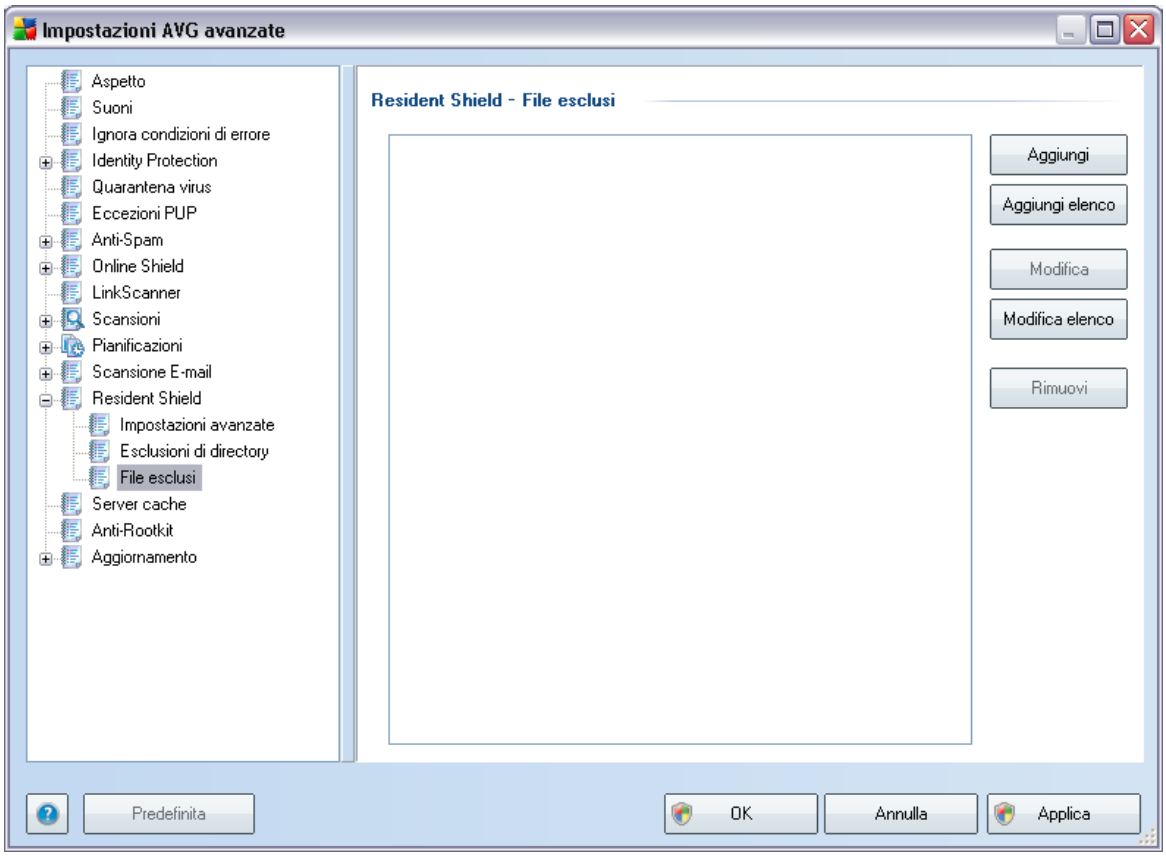
Se non è essenziale, si consiglia di non escludere alcuna directory.

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

10.11.3. File esclusi



La finestra di dialogo ***Resident Shield - File esclusi*** è simile alla finestra ***Resident Shield - Esclusioni di directory descritta in precedenza,*** ma invece delle cartelle è ora possibile definire file specifici da escludere dalla scansione ***Resident Shield***.

Se non è essenziale, si consiglia di non escludere alcun file.

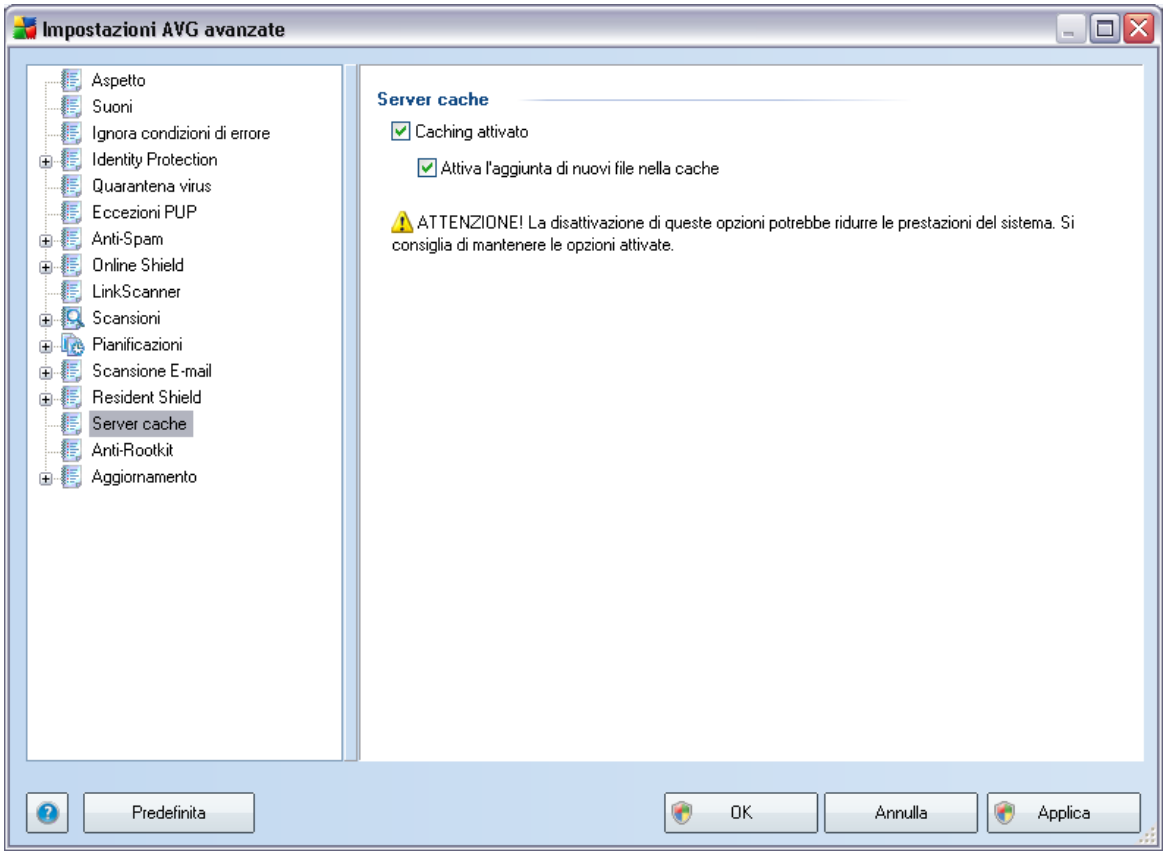
La finestra di dialogo fornisce i seguenti pulsanti di controllo:

- ***Aggiungi***: consente di specificare i file da escludere dalla scansione selezionandoli uno alla volta dalla struttura di esplorazione del disco locale

- ***Aggiungi elenco***: consente di immettere un elenco intero di file da escludere dalla scansione di ***Resident Shield***
- ***Modifica***: consente di modificare il percorso specificato di un file selezionato
- ***Modifica elenco***: consente di modificare l'elenco dei file
- ***Rimuovi***: consente di eliminare dall'elenco il percorso di un file selezionato

10.12. Server cache

Il ***Server cache*** costituisce un processo destinato a velocizzare qualsiasi tipo di scansione (*scansione su richiesta, scansione dell'intero computer pianificata, scansione di Resident Shield*). Il processo raccoglie e mantiene le informazioni relative ai file affidabili (*file di sistema con firma digitale e così via*): questi file vengono quindi considerati come sicuri e durante la scansione vengono ignorati.



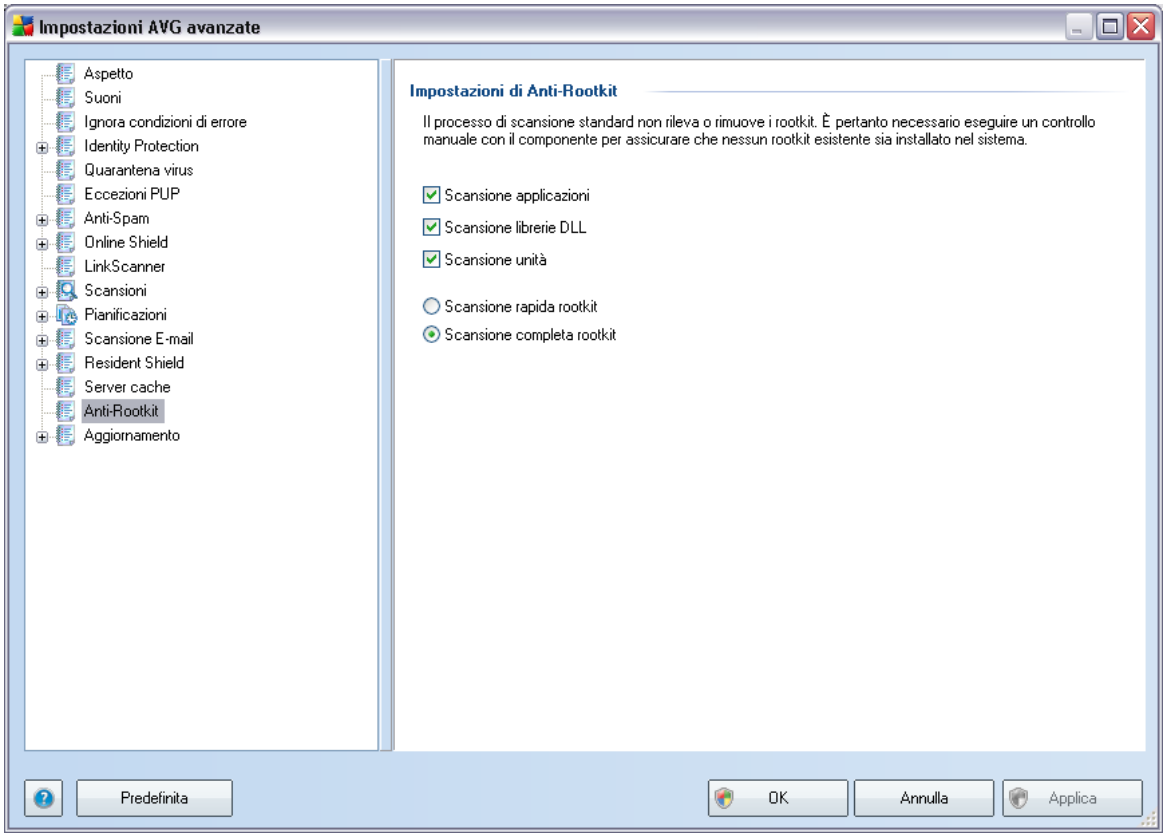
La finestra di dialogo di impostazione offre due opzioni:

- ***Caching attivato*** (*attivata per impostazione predefinita*) – deselezionare la casella per disattivare il ***Server cache*** e svuotare la memoria cache. Tenere presente che la scansione potrebbe subire un rallentamento e le prestazioni complessive del computer potrebbero ridursi, poiché per prima cosa ogni singolo file in uso verrà sottoposto alla scansione antivirus e antispyware.

- ***Attiva l'aggiunta di nuovi file nella cache*** (*attivata per impostazione predefinita*) – deselezionare la casella per arrestare l'aggiunta di ulteriori file nella memoria cache. Tutti i file già presenti nella cache verranno mantenuti e utilizzati finché l'inserimento nella cache non verrà disattivato completamente o finché non verrà eseguito il successivo aggiornamento del database dei virus.

10.13. 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***.

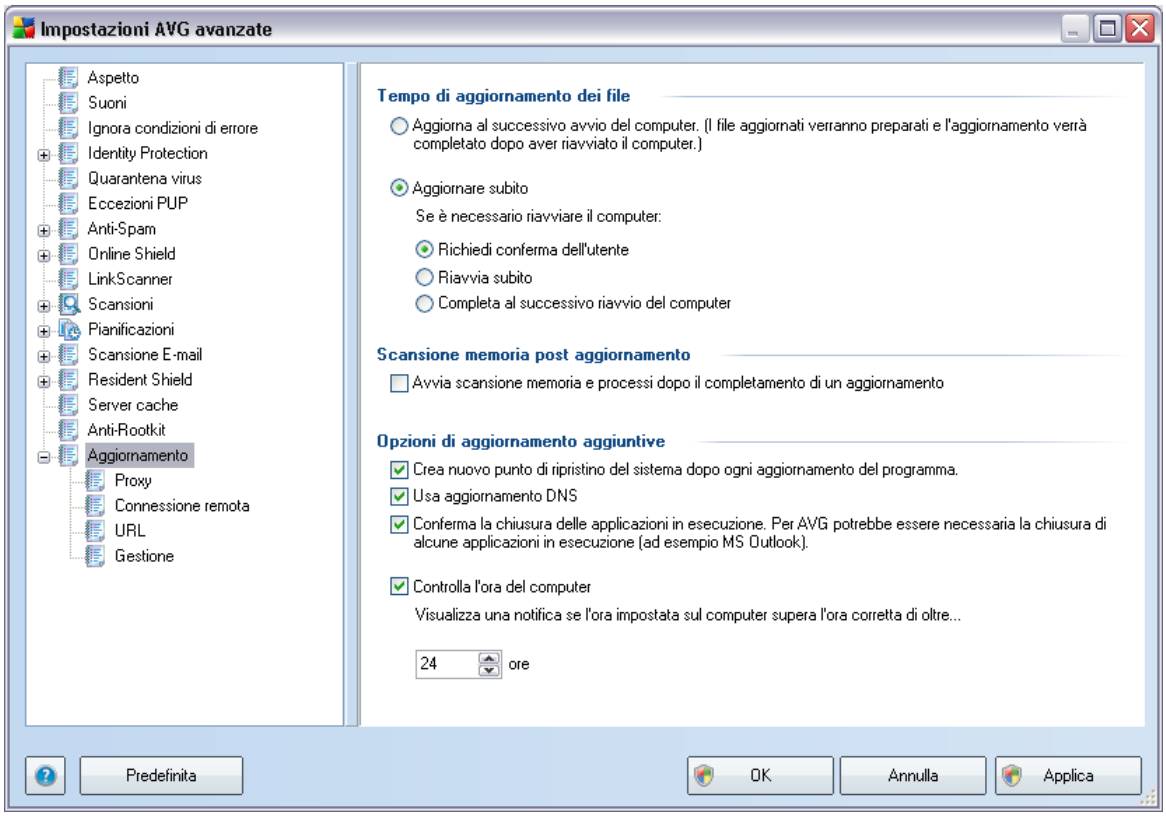
Selezionare le caselle di controllo pertinenti per specificare gli oggetti da sottoporre a scansione:

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

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

- ***Scansione rapida rootkit***: sottopone a scansione tutti i processi in esecuzione, i driver caricati e la cartella di sistema (*solitamente c:\Windows*)
- ***Scansione completa rootkit***: sottopone a scansione tutti i processi in esecuzione, i driver caricati e la cartella di sistema (*solitamente c:\Windows*), nonché tutte le unità locali (*inclusa l'unità di memoria flash, ma escluse le unità disco floppy/CD*)

10.14. 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

Scansione memoria post aggiornamento

Selezionare questa casella di controllo per specificare che si desidera avviare una nuova scansione della memoria al termine di ciascun aggiornamento. L'ultimo aggiornamento scaricato potrebbe contenere nuove definizioni dei virus e queste potrebbero applicarsi immediatamente alla scansione.

Opzioni di aggiornamento aggiuntive

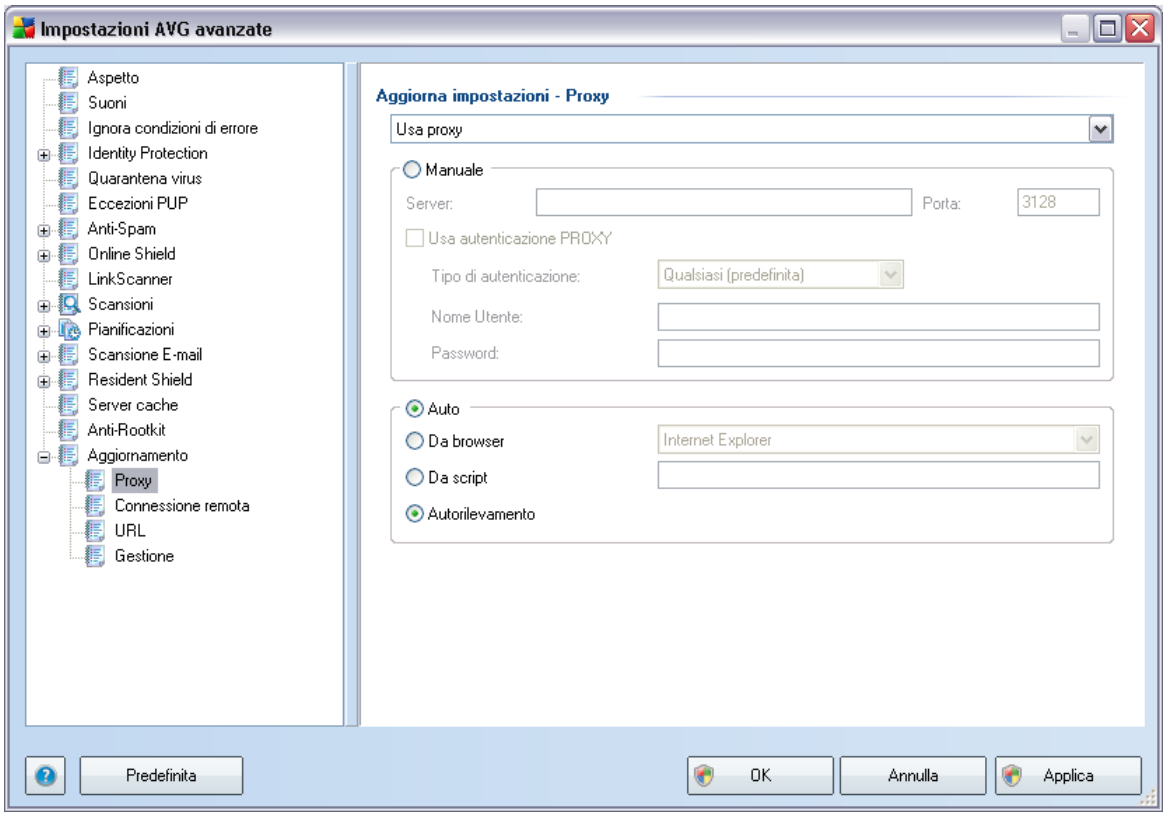
- ***Crea nuovo punto di ripristino del sistema dopo ogni aggiornamento del programma***: prima dell'avvio di ciascun aggiornamento del programma AVG viene creato un punto di ripristino del sistema. Se il processo di aggiornamento non ha esito positivo e il sistema operativo si blocca, è possibile ripristinare 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;

- ***Conferma la chiusura delle applicazioni in esecuzione*** (*attiva per impostazione predefinita*) garantirà che nessuna applicazione in esecuzione venga chiusa senza autorizzazione, nel caso fosse 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.

10.14.1. 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***: impostazione predefinita
- ***Tenta la connessione utilizzando il proxy e, se non riesce, esegui la connessione direttamente***

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***: specificare 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.

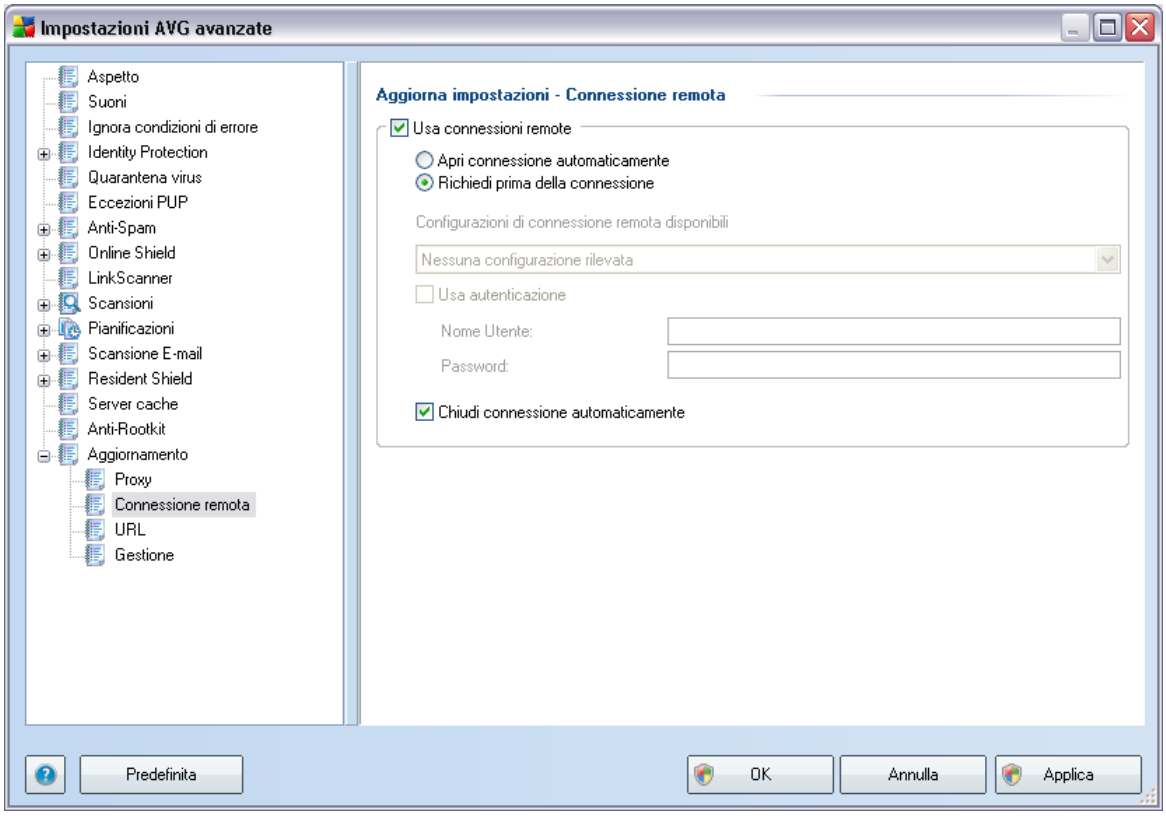
Configurazione automatica

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

- ***Da browser***: la configurazione verrà letta dal browser Internet predefinito
- ***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

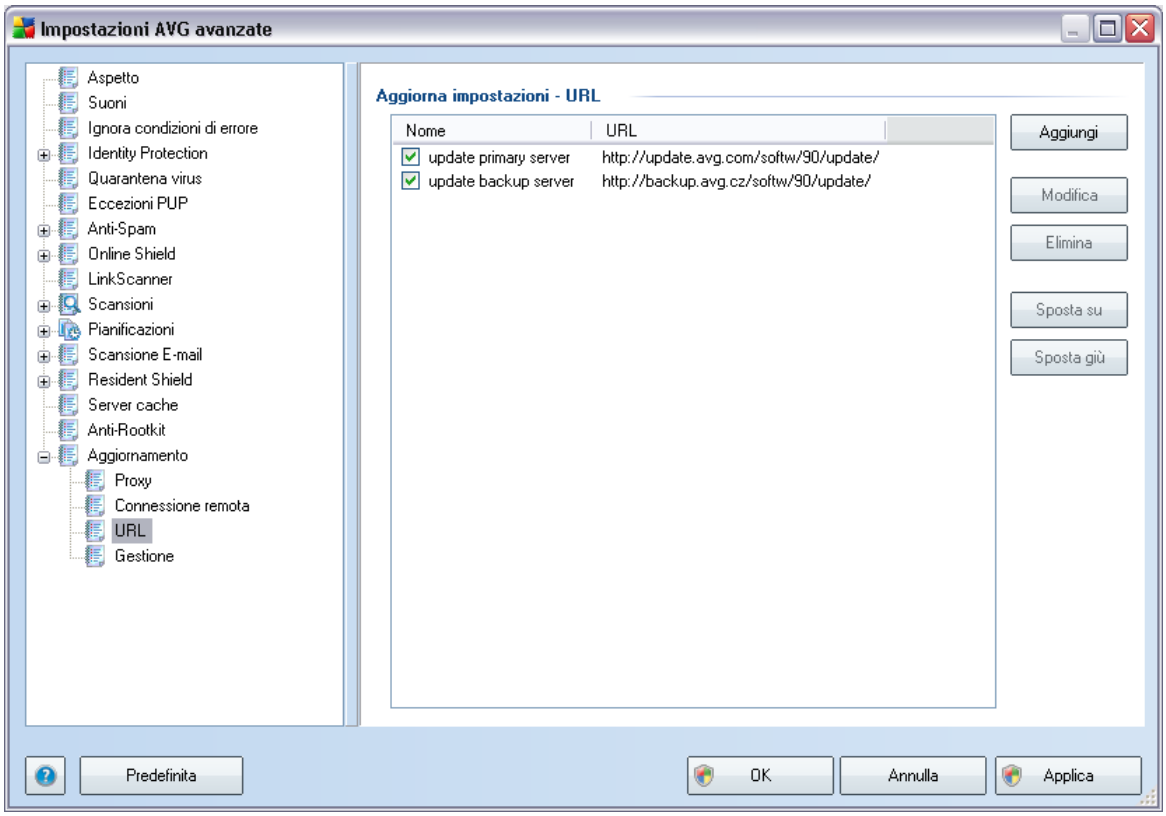
10.14.2. Connessione remota



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***).

10.14.3. URL

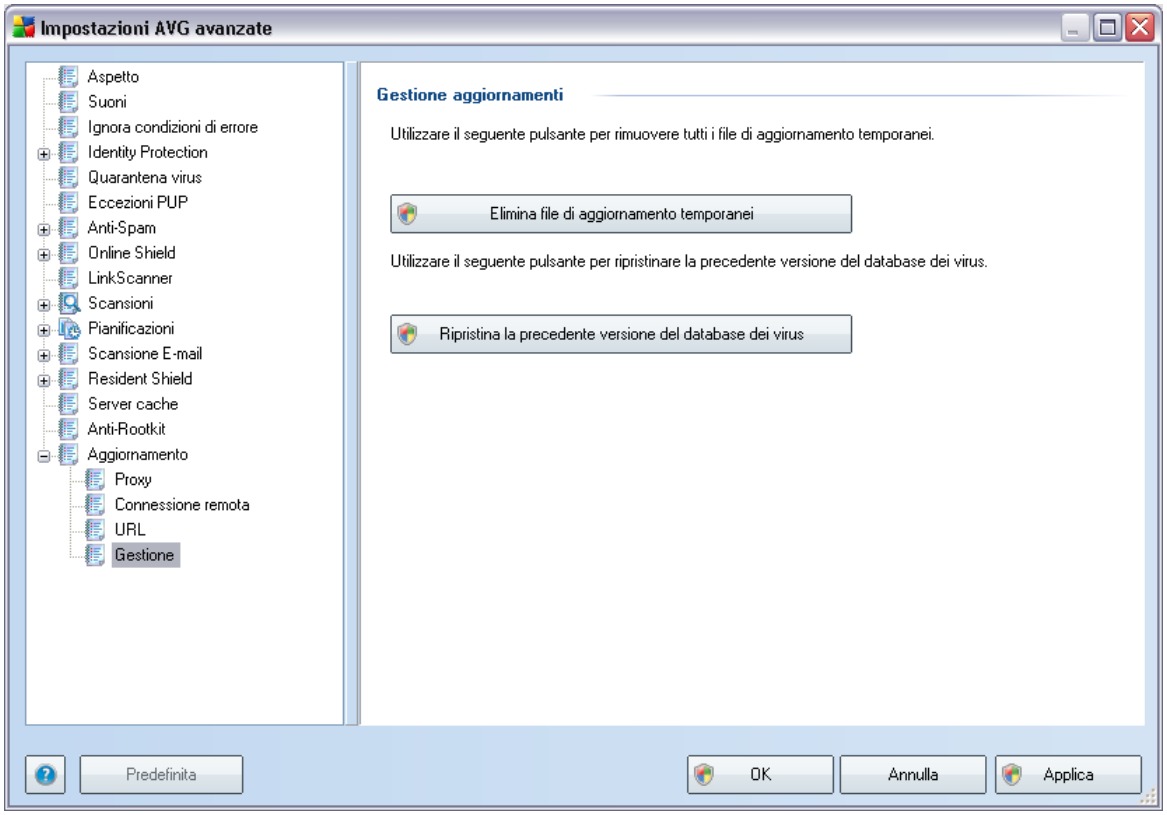


Nella finestra di dialogo ***URL*** è contenuto un elenco di indirizzi Internet da cui è possibile scaricare i file di aggiornamento. È possibile modificare l'elenco e i suoi elementi utilizzando i seguenti pulsanti di controllo:

- ***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
- ***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

10.14.4. Gestione

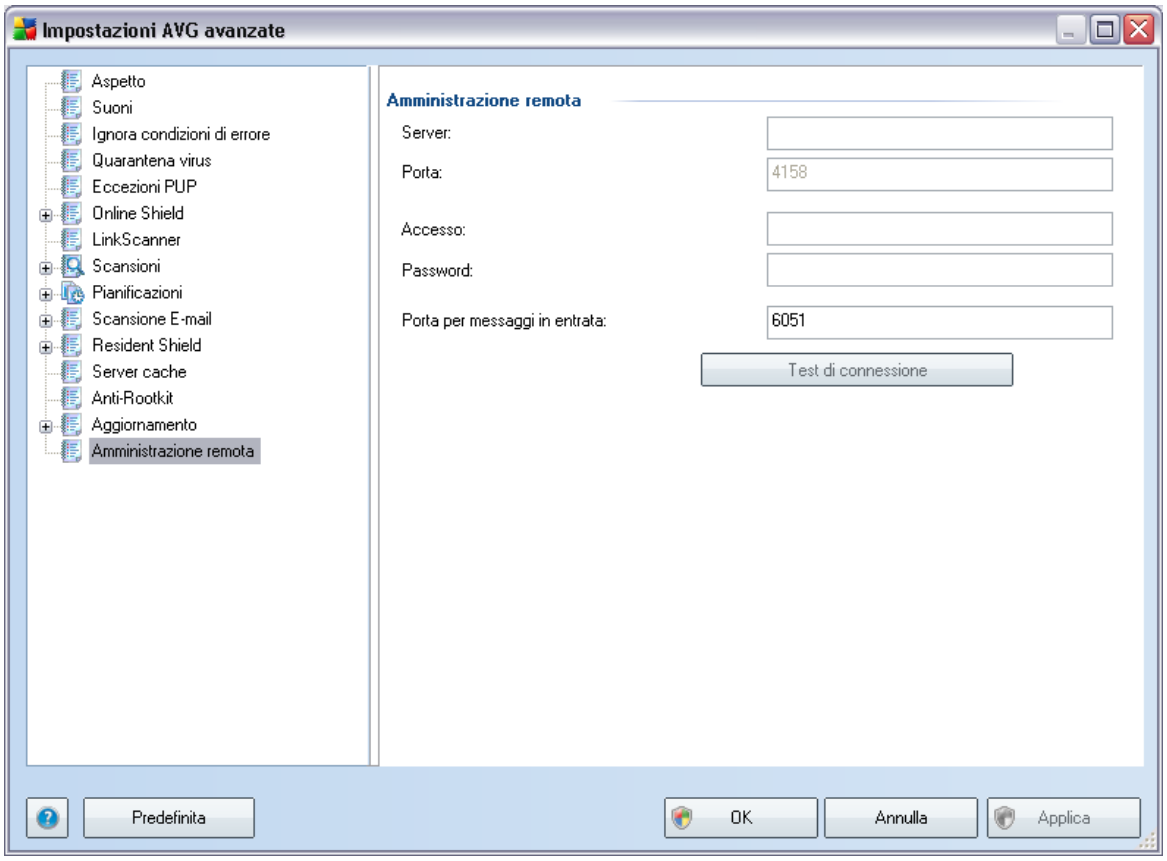
La finestra di dialogo ***Gestione*** offre due opzioni accessibili tramite due pulsanti:



- ***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*)

10.15. 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

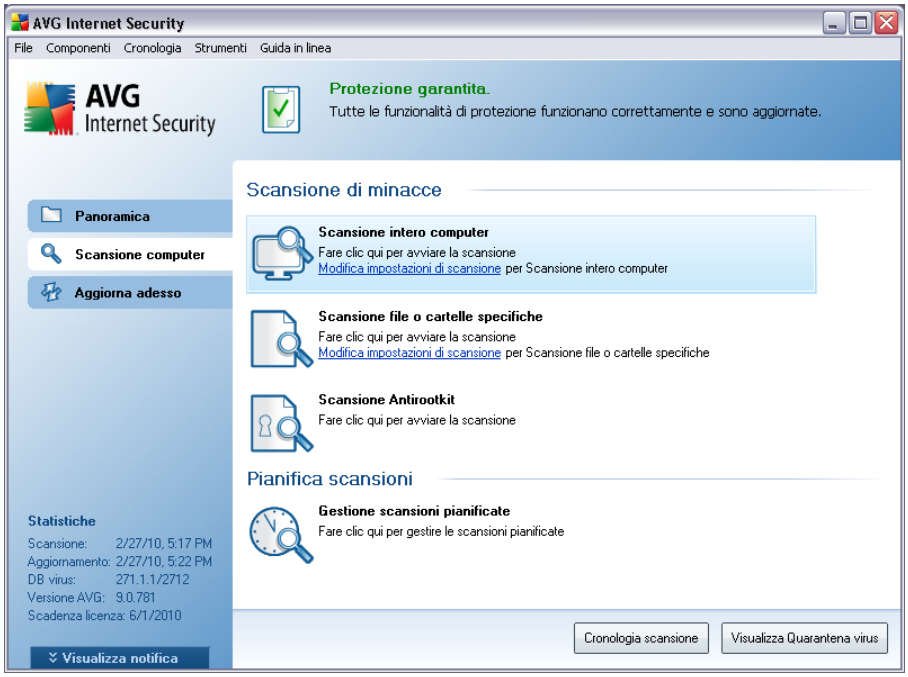
Il pulsante ***Test di connessione*** consente di verificare che tutti i dati indicati in alto sono validi e possono essere utilizzati per effettuare la connessione al DataCenter.

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

11. Scansione AVG

La scansione è una parte fondamentale della funzionalità di **AVG 9 Anti-Virus**. È possibile eseguire verifiche su richiesta o pianificarle affinché vengano eseguite su base giornaliera in un orario specifico.

11.1. 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 tre tipi di scansione definiti dal fornitore del software che possono essere utilizzati immediatamente su richiesta oppure pianificati:
  - ***Scansione intero computer***
  - ***Scansione file o cartelle specifiche***
  - ***Scansione Antirootkit***

- 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

11.2. Scansioni predefinite

Una delle funzioni principali di **AVG 9 Anti-Virus** 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 9 Anti-Virus** sono disponibili due tipi di scansione predefiniti dal fornitore del software:

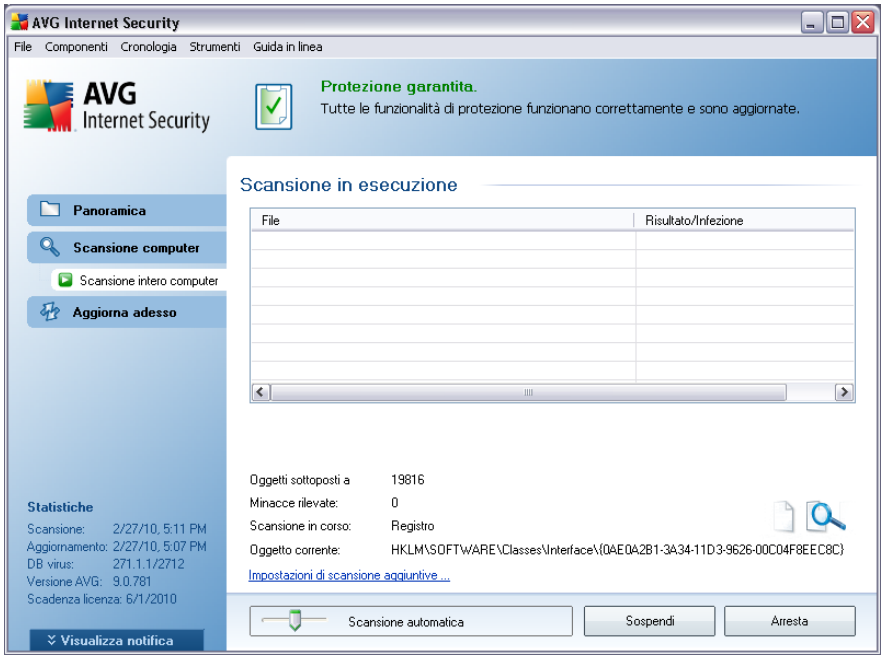
11.2.1. Scansione intero computer

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 completa di una workstation almeno una volta la settimana.

Avvio della scansione

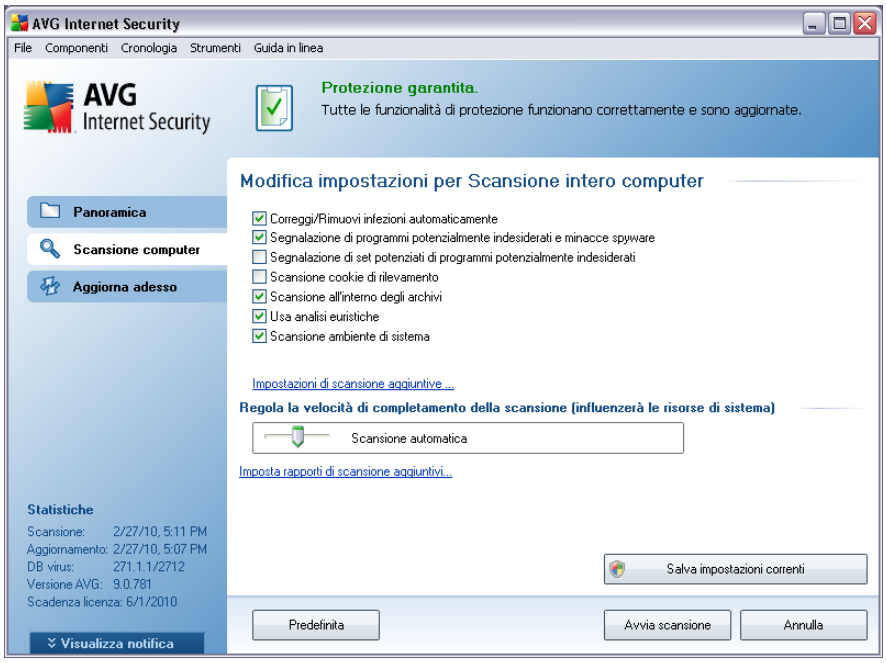
È possibile avviare ***Scansione intero computer*** direttamente dall'interfaccia di scansione facendo clic sull'icona di scansione. Non è necessario configurare ulteriori impostazioni specifiche per questo tipo di scansione. La scansione verrà avviata immediatamente nella finestra di dialogo ***Scansione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

annullata (***Arresta***) se necessario.



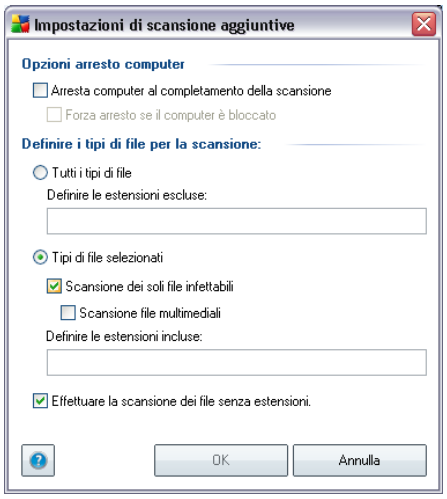
Modifica della configurazione della scansione

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.

- ***Impostazioni di scansione aggiuntive***: il collegamento consente di aprire una nuova finestra di dialogo ***Impostazioni di scansione aggiuntive*** in cui è possibile specificare i seguenti parametri:



- ***Opzioni arresto computer***: consente di decidere se il computer deve essere arrestato automaticamente 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***).

- ***Definire i tipi di file per la scansione***: specificare se si desidera sottoporre a scansione:

  - ***Tutti i tipi di file*** con la possibilità di definire le eccezioni fornendo un elenco di estensioni di file separate da virgola da non sottoporre a scansione;

  - ***Tipi di file selezionati***: è possibile specificare che si desidera sottoporre a scansione solo file potenzialmente infettabili (*i file che non possono essere infettati non verranno sottoposti a scansione, ad esempio alcuni file di testo normale o altri file non eseguibili*), inclusi i file multimediali (*file video e audio; se non si seleziona questa casella, il tempo di scansione risulterà ulteriormente ridotto, poiché questi file sono spesso di grandi dimensioni e non facilmente infettabili dai virus.*). Anche in questo caso, è possibile specificare tramite le estensioni quali file devono essere sempre sottoposti a scansione.

  - Facoltativamente, è possibile sottoporre a scansione i file senza estensione tramite ***Effettuare la scansione dei file senza estensioni***: questa opzione è attivata per impostazione predefinita e si consiglia di non modificare questa impostazione a meno che non

siano presenti motivi validi per farlo. I file senza estensione sono piuttosto sospetti e devono essere sempre sottoposti a 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 più lentamente così da ridurre al minimo il carico delle risorse di sistema (*utile quando è necessario lavorare al computer ma la durata della scansione non influisce*) o più velocemente con requisiti delle risorse di sistema più elevati (*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:

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.*

11.2.2. Scansione file o cartelle specifiche

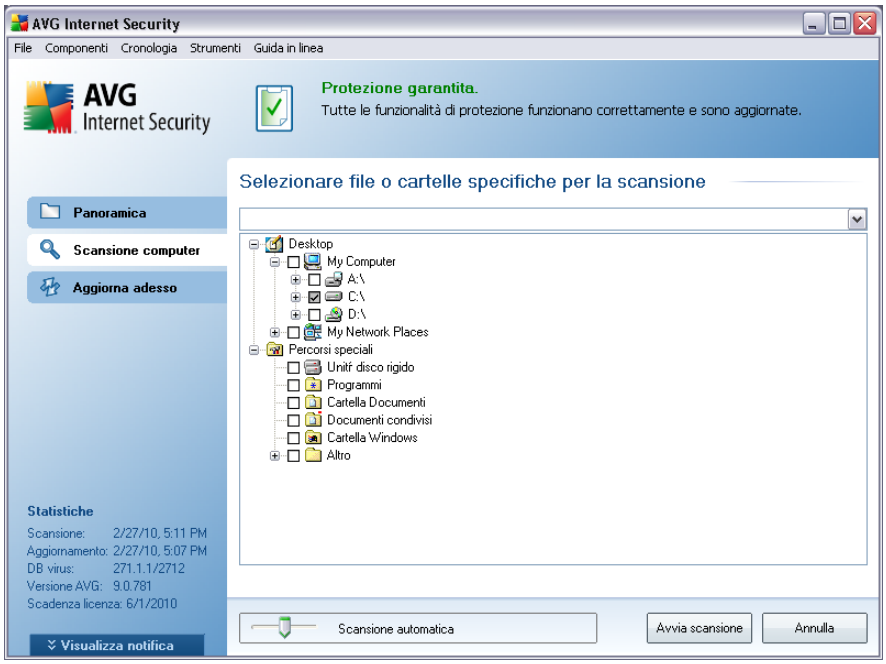
Scansione file o cartelle specifiche: consente di eseguire la scansione delle sole aree del computer selezionate per la scansione (*cartelle, dischi rigidi, dischi floppy, CD selezionati e così via*). L'avanzamento della scansione nel caso di rilevamento di virus e il relativo trattamento sono gli stessi 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.

Avvio della 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 "!".

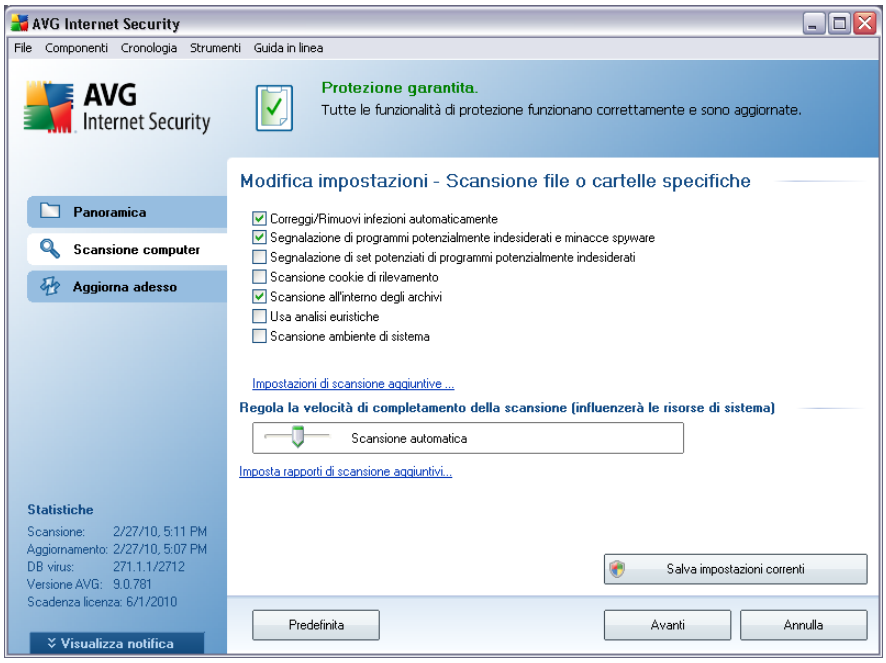
Infine, per avviare la scansione, premere il pulsante ***Avvia scansione*** ; il processo di scansione è praticamente identico a quello della scansione dell'intero computer.



Modifica della configurazione della scansione

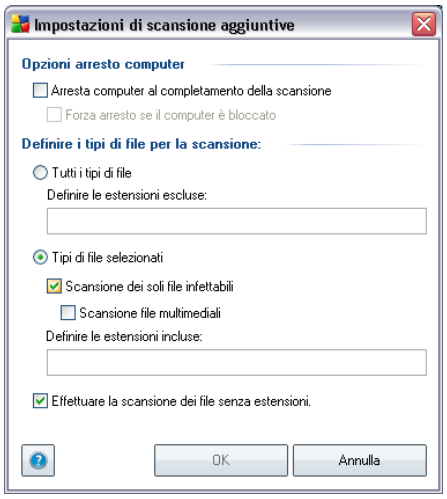
È possibile modificare le impostazioni predefinite di ***Scansione file o cartelle specifiche***. Premere il collegamento ***Modifica impostazioni di scansione*** per

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*).

- ***Impostazioni di scansione aggiuntive***: il collegamento consente di aprire una nuova finestra di dialogo Impostazioni di scansione aggiuntive in cui è possibile specificare i seguenti parametri:



- ***Opzioni arresto computer***: consente di decidere se il computer deve essere arrestato automaticamente 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***).

- ***Definire i tipi di file per la scansione***: specificare se si desidera sottoporre a scansione:

  - ***Tutti i tipi di file***: è possibile definire le eccezioni fornendo un elenco di estensioni di file separate da virgola da non sottoporre a scansione;

  - ***Tipi di file selezionati***: è possibile specificare che si desidera sottoporre a scansione solo file potenzialmente infettabili (*i file che non possono essere infettati non verranno sottoposti a scansione, ad esempio alcuni file di testo normale o altri file non eseguibili*), inclusi i file multimediali (*file video e audio; se non si seleziona questa casella, il tempo di scansione risulterà ulteriormente ridotto, poiché questi file sono spesso di grandi dimensioni e non facilmente infettabili dai virus.*). Anche in questo caso, è possibile specificare tramite le estensioni quali file devono essere sempre sottoposti a scansione.

  - Facoltativamente, è possibile sottoporre a scansione i file senza estensione tramite ***Effettuare la scansione dei file senza estensioni***: questa opzione è attivata per impostazione predefinita e si consiglia di non modificare questa impostazione a meno che non siano presenti motivi validi per farlo. I file senza estensione sono

piuttosto sospetti e devono essere sempre sottoposti a scansione.

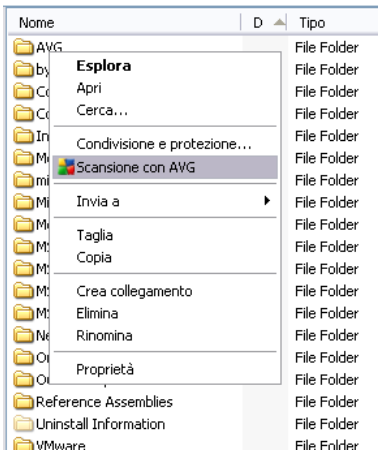
- ***Priorità processi di scansione***: è possibile utilizzare il dispositivo di scorrimento per modificare la priorità del processo di scansione. Per impostazione predefinita, la priorità è impostata sul livello medio (*Scansione automatica*) per ottimizzare la velocità del processo di scansione e l'utilizzo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

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).*

11.3. Scansione in Esplora risorse

Oltre alle scansioni predefinite avviate per l'intero computer o per le aree selezionate, **AVG 9 Anti-Virus** offre l'opzione di 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

11.4. Scansione riga di comando

In **AVG 9 Anti-Virus** è possibile 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 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 /parametro*** ... ad esempio ***avgscanx /comp*** per la scansione dell'intero computer

- ***avgscanx /parametro /parametro*** .. 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 del computer di cui eseguire la scansione ed è necessario fornire il percorso esatto della sezione selezionata), i valori vengono separati da punto e virgola. 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.

11.4.1. 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 intero computer

- ***/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

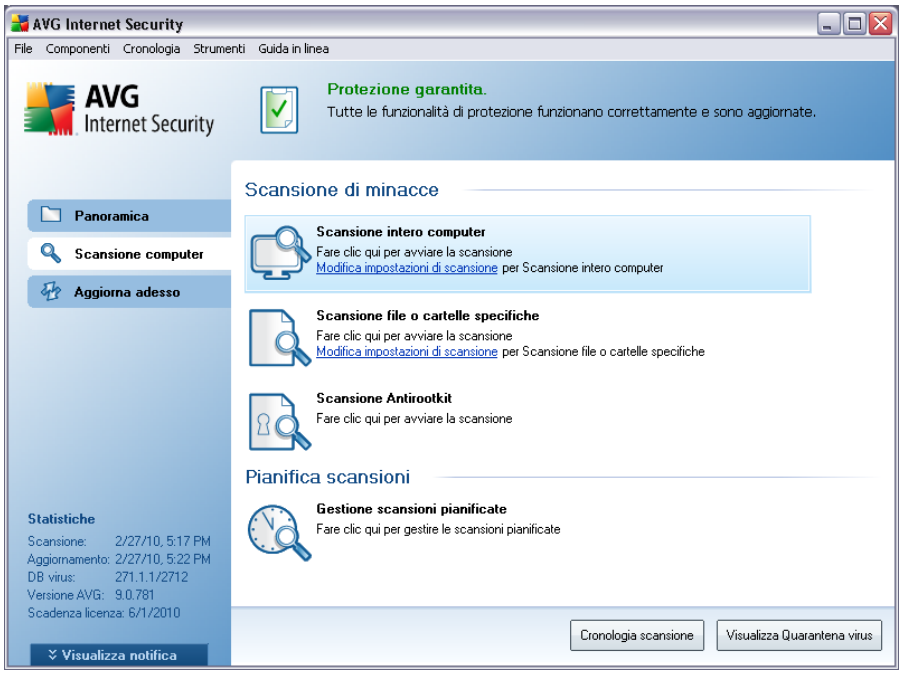
- ***/HELP*** Visualizza la Guida sull'argomento
- ***/PRIORITY*** Imposta priorità scansione /Bassa, Automatica, Elevata/ (vedere Impostazioni avanzate / Scansioni)
- ***/SHUTDOWN*** Arresta computer al completamento della scansione
- ***/FORCESHUTDOWN*** Forza arresto del computer al completamento della scansione
- ***/ADS*** Esegui scansione flussi di dati alternativi (solo NTFS)

11.5. Pianificazione di scansioni

AVG 9 Anti-Virus consente di eseguire scansioni 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.

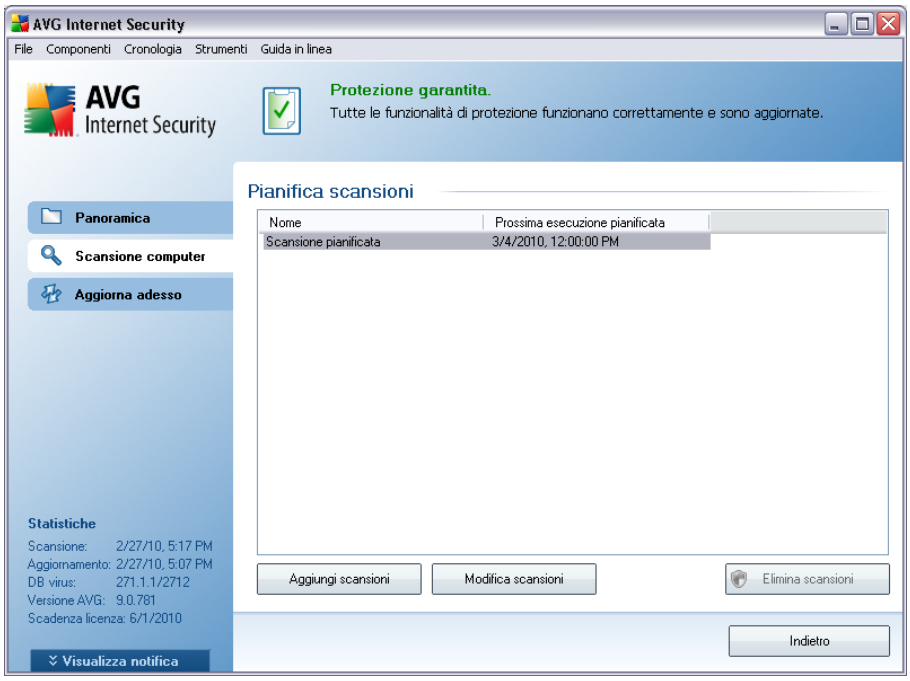
Si consiglia di avviare ***Scansione intero computer*** su base regolare, almeno una volta alla settimana. Tuttavia, se possibile, avviare la scansione dell'intero computer ogni giorno, come impostato nella configurazione predefinita della pianificazione della scansione. Se il computer è sempre acceso, 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***:



Pianificazione scansioni

Fare clic sull'icona grafica all'interno della sezione ***Pianificazione scansioni*** per aprire una nuova finestra di dialogo ***Pianificazione scansioni*** in cui è disponibile un elenco ti tutte le scansioni pianificate al momento:



È possibile modificare / aggiungere scansioni utilizzando 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.

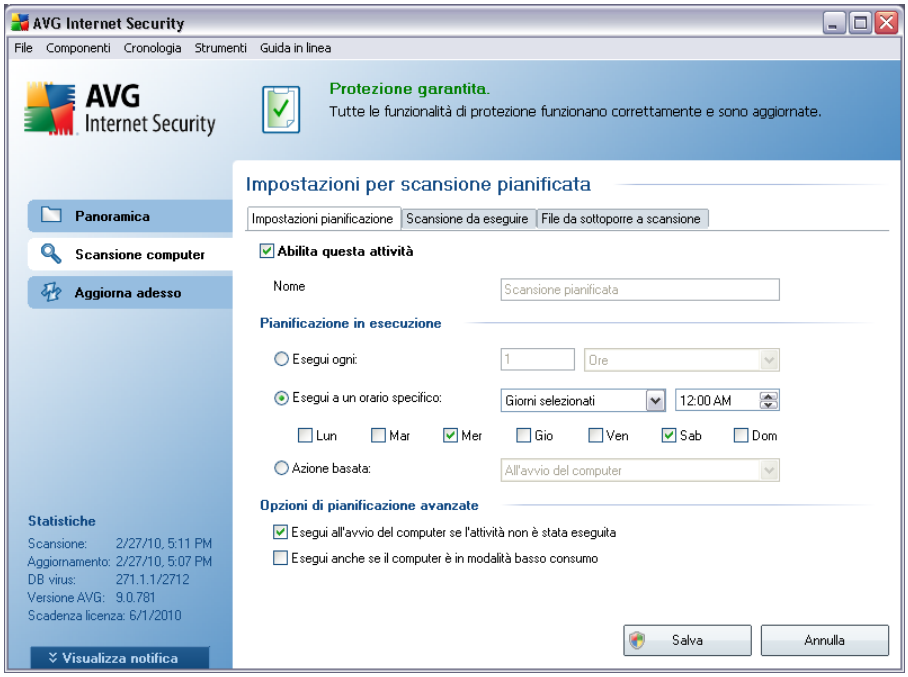
- ***Modifica pianificazione scansione***: il pulsante può essere utilizzato solo se è stato selezionato in precedenza un controllo esistente dall'elenco dei controlli pianificati. In tal caso il pulsante è visualizzato come attivo e, premendolo, si passa alla finestra di dialogo ***Impostazioni per 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.

- ***Indietro***: consente di tornare all'interfaccia di scansione di AVG

11.5.1. Impostazioni pianificazione

Per pianificare un nuovo controllo e il relativo avvio regolare, accedere alla finestra di dialogo ***Impostazioni per il controllo pianificato*** (*fare clic sul pulsante* ***Aggiungi pianificazione scansione*** *nella finestra di dialogo* ***Pianificazione scansioni***). 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 selezionati.

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.

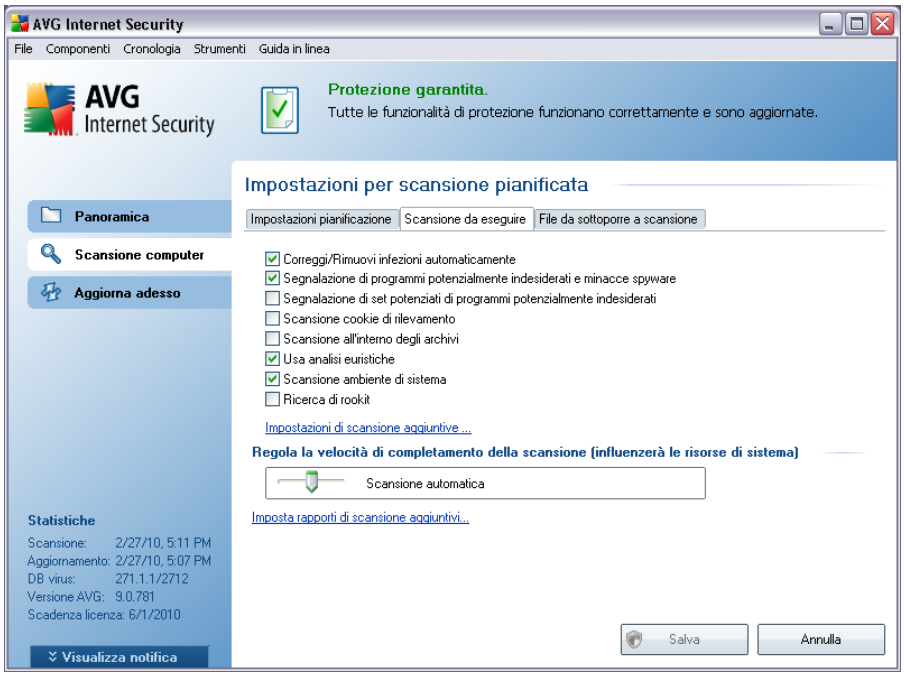
Pulsanti di controllo delle impostazioni per la finestra di dialogo della scansione pianificata

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***). Ciascun pulsante mantiene 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, selezionare 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.

11.5.2. 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***.

- ***Segnalazione di programmi potenzialmente indesiderati e minacce spyware*** – (*attivata per impostazione predefinita*) selezionare questa casella di controllo per attivare il motore ***Anti-Spyware*** ed eseguire la scansione per ricercare spyware e virus. Gli spyware rappresentano una categoria di malware anomala: anche se solitamente costituiscono un rischio per la sicurezza, alcuni di questi programmi possono essere installati intenzionalmente. Si consiglia di mantenere questa funzionalità attivata in

quanto consente di aumentare la protezione del computer

- ***Segnalazione di set potenziati di programmi potenzialmente indesiderati*** – se la precedente opzione è attivata, è inoltre possibile selezionare questa casella per rilevare pacchetti estesi di spyware: programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita.

- ***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*);

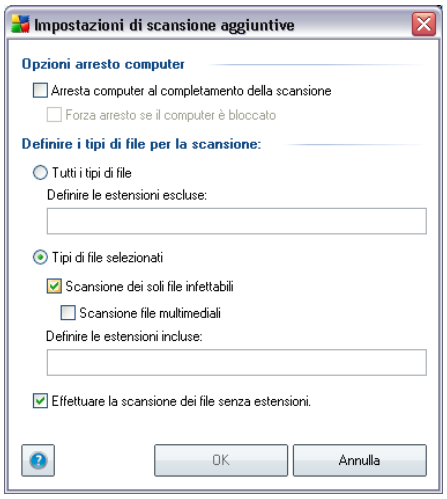
- ***Scansione all'interno degli archivi*** : (*attivata per impostazione predefinita*) questo parametro stabilisce che la scansione deve controllare tutti i file anche se inclusi all'interno di un archivio, ad esempio ZIP, RAR e così via.

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

Quindi, è possibile modificare la configurazione della scansione come segue:

- ***Impostazioni di scansione aggiuntive***: il collegamento consente di aprire una nuova finestra di dialogo ***Impostazioni di scansione aggiuntive*** in cui è possibile specificare i seguenti parametri:



- ***Opzioni arresto computer***: consente di decidere se il computer deve essere arrestato automaticamente 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***).

- ***Definire i tipi di file per la scansione***: specificare se si desidera sottoporre a scansione:

  - ***Tutti i tipi di file*** con la possibilità di definire le eccezioni fornendo un elenco di estensioni di file separate da virgola da non sottoporre a scansione;

  - ***Tipi di file selezionati***: è possibile specificare che si desidera sottoporre a scansione solo file potenzialmente infettabili (*i file che non possono essere infettati non verranno sottoposti a scansione, ad esempio alcuni file di testo normale o altri file non eseguibili*), inclusi i file multimediali (*file video e audio; se non si seleziona questa casella, il tempo di scansione risulterà ulteriormente ridotto, poiché questi file sono spesso di grandi dimensioni e non facilmente infettabili dai virus.*). Anche in questo caso, è possibile specificare tramite le estensioni quali file devono essere sempre sottoposti a scansione.

  - Facoltativamente, è possibile sottoporre a scansione i file senza estensione tramite ***Effettuare la scansione dei file senza estensioni***: questa opzione è attivata per impostazione predefinita e si consiglia di non modificare questa impostazione a meno che non

siano presenti motivi validi per farlo. I file senza estensione sono piuttosto sospetti e devono essere sempre sottoposti a 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 più lentamente così da ridurre al minimo il carico delle risorse di sistema (*utile quando è necessario lavorare al computer ma la durata della scansione non influisce*) o più velocemente con requisiti delle risorse di sistema più elevati (*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:

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

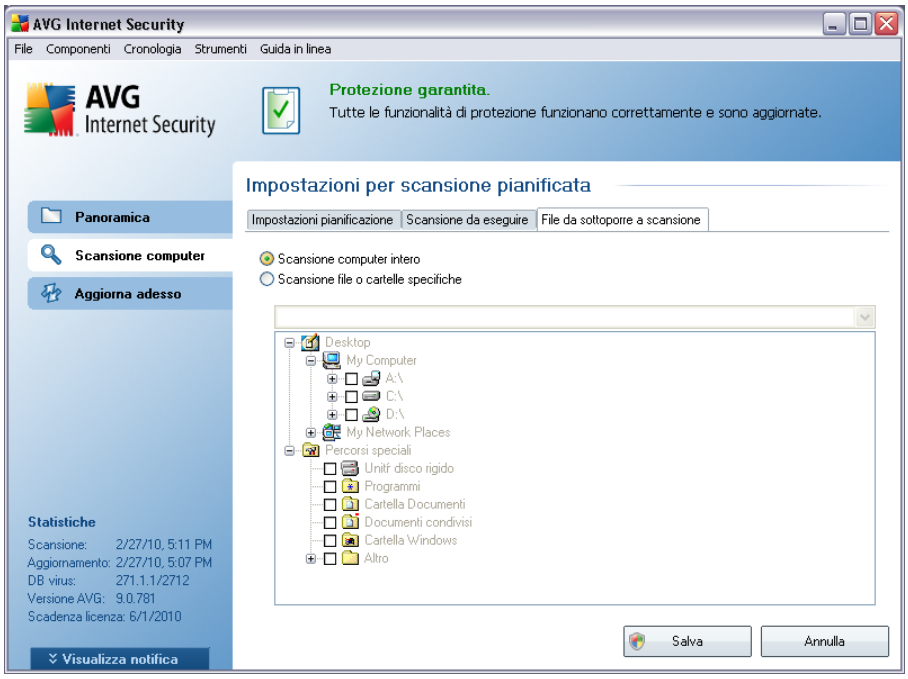
Sono disponibili due pulsanti di controllo sulle tre schede della finestra di dialogo ***Impostazioni per scansione pianificata*** (***Impostazioni pianificazione***, ***Scansione da eseguire*** e***File da sottoporre a scansione***). Ciascun pulsante mantiene la stessa funzionalità indipendentemente 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, selezionare 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.

11.5.3. 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 cartelle o file specifici, nella parte inferiore di questa finestra di dialogo viene attivata la struttura visualizzata che consente di specificare le cartelle da sottoporre a scansione (*espandere le voci facendo clic sul nodo "+" finché non viene individuata la cartella da sottoporre a scansione*). È possibile selezionare più cartelle facendo clic sulle rispettive caselle. Le cartelle selezionate verranno visualizzate nel campo di testo nella parte superiore della finestra di dialogo e nel menu a discesa verrà mantenuta la cronologia delle scansioni selezionate per riferimento futuro. In alternativa, è possibile immettere manualmente il percorso completo della cartella desiderata (*se si immettono più percorsi, è necessario separarli con un punto*

e virgola senza ulteriori spazi).

All'interno della struttura è inoltre possibile visualizzare un ramo denominato ***Percorsi speciali***. Di seguito è disponibile un elenco delle posizioni che verranno sottoposte a scansione se verrà selezionata la relativa casella di controllo:

- ***Dischi rigidi locali***: tutti i dischi rigidi del computer
- ***Programmi***: C:\Programmi\
- ***Cartella Documenti***: C:\Documents and Settings\utente\Documenti\
- ***Documenti condivisi***: C:\Documents and Settings\All Users\Documenti condivisi\
- ***Cartella Windows***: C:\Windows\
- ***Altro***
  - *Unità di sistema*: disco rigido su cui è installato il sistema operativo (solitamente C:)
  - *Cartella di sistema*: Windows/System32
  - *Cartella dei file temporanei*: Documents and Settings/utente/Local Settings/Temp
  - *File temporanei di Internet*: Documents and Settings/utente/Local Settings/Temporary Internet Files

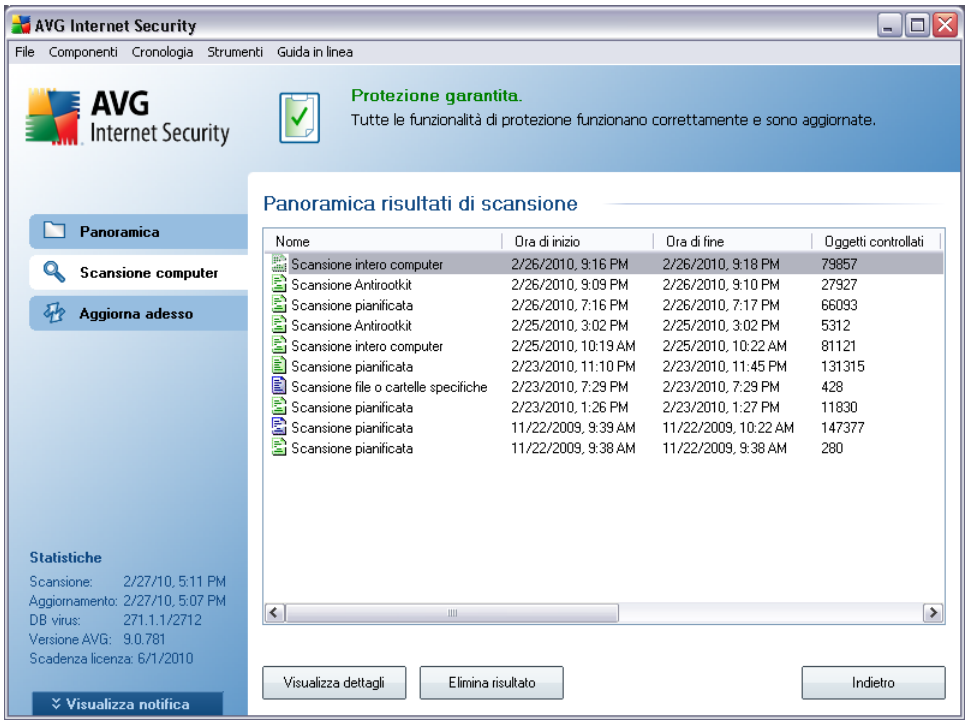
Pulsanti di controllo delle impostazioni per la finestra di dialogo della scansione pianificata

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***). Ciascun pulsante mantiene 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, selezionare 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.

11.6. 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

- ***Avvisi***: numero di oggetti sospetti
- ***Rootkit***: numero di rootkit
  - ***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***: selezionare questa opzione per accedere alla finestra di dialogo ***Risultati scansione*** e visualizzare dati dettagliati relativi alla scansione selezionata
- ***Elimina risultato***: selezionare questa opzione per rimuovere la voce selezionata dalla panoramica dei risultati di scansione
- ***Indietro***: consente di tornare alla finestra di dialogo predefinita dell'interfaccia di scansione di AVG

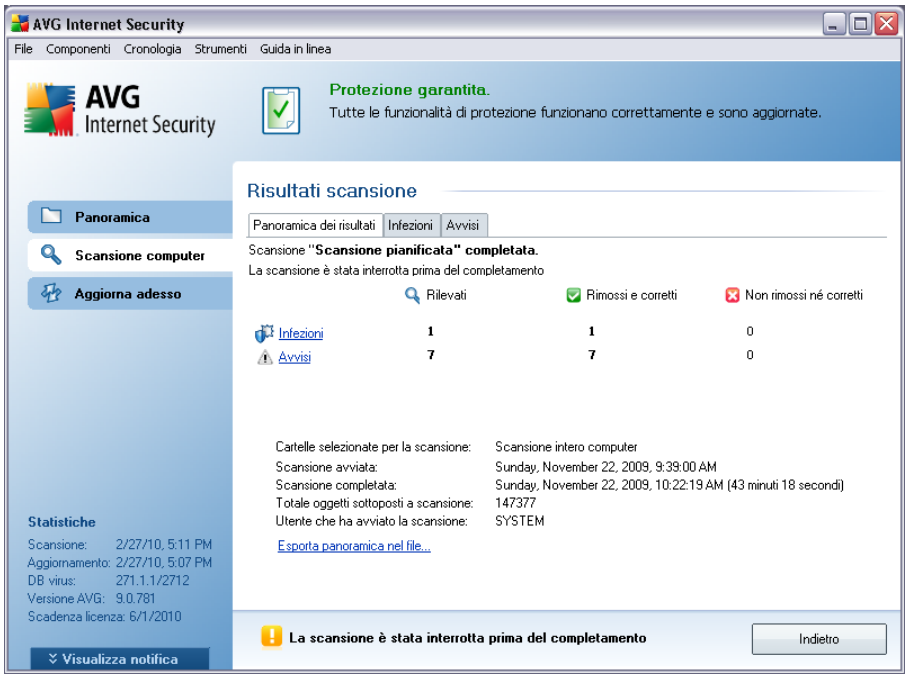
11.7. Dettagli di Risultati scansione

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, ad esempio, se sono stati rilevati cookie durante la scansione
- ***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. Inoltre, qui sono disponibili informazioni sugli oggetti che non è stato possibile sottoporre a scansione (ad esempio archivi protetti da password).

11.7.1. Scheda Panoramica dei risultati



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

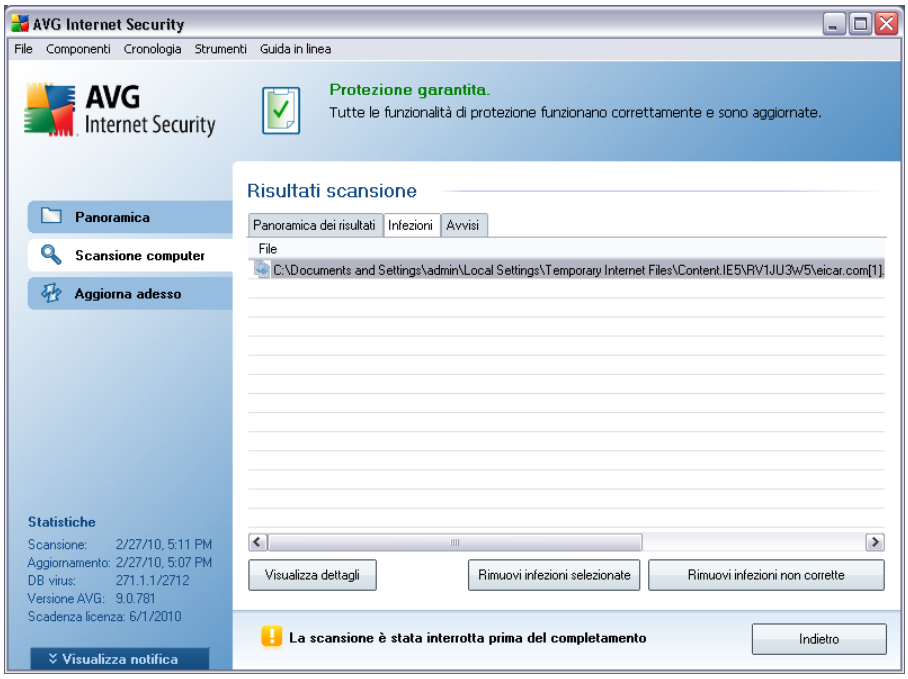
- infezioni da virus / spyware rilevate
- infezioni da virus / spyware rimosse
- numero di infezioni da virus / spyware che non è possibile rimuovere o correggere

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***.

11.7.2. Scheda Infezioni



La scheda ***Infezioni*** viene visualizzata nella finestra di dialogo ***Risultati scansione*** solo 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:

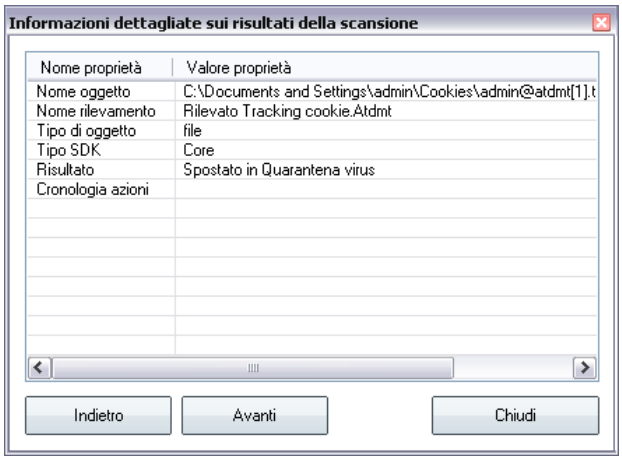
- ***File***: percorso completo della posizione originale dell'oggetto infetto
- ***Infezioni***: nome del virus rilevato (*per informazioni dettagliate su virus specifici, consultare l'Enciclopedia dei virus in linea*)
- ***Risultato***: definisce lo stato corrente dell'oggetto infetto rilevato durante 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 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***

11.7.3. 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

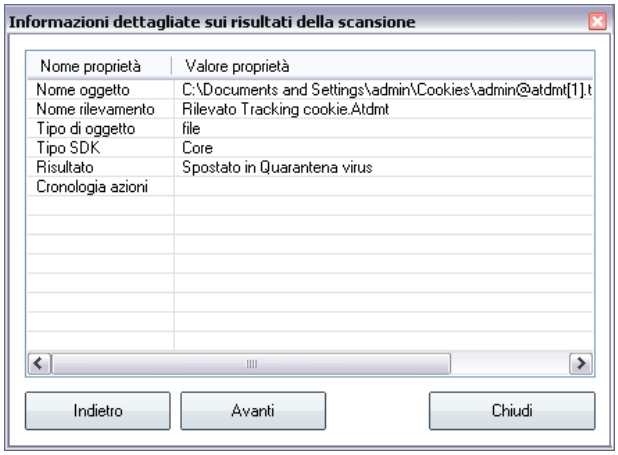
- o ***Oggetto potenzialmente pericoloso***: l'oggetto è stato rilevato come potenzialmente pericoloso ma non infetto (potrebbe contenere macro, ad esempio); l'informazione deve essere considerata solo come un avviso

- o ***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.

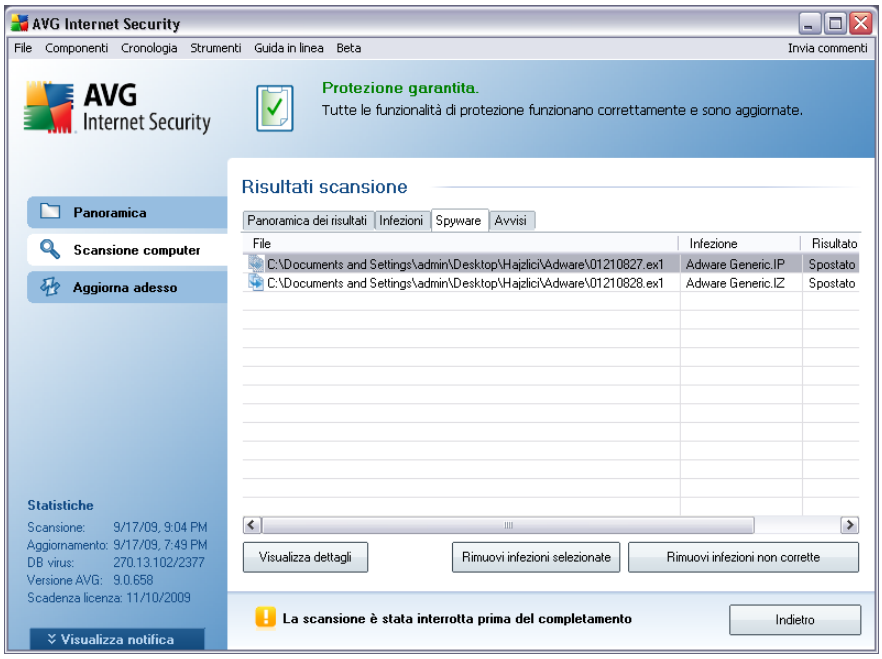
- ***Rimuovi infezioni selezionate***: utilizzare il pulsante per spostare l'oggetto rilevato selezionato in ***Quarantena virus***

- ***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***

11.7.4. 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. Tali file non presentano minacce dirette per il computer o la sicurezza. Le informazioni su questi file sono generalmente utili in caso venga individuato adware o spyware sul computer. Se vengono individuati solo Avvisi durante un test AVG, non è richiesto alcun intervento.



Questa è una breve descrizione degli esempio più comuni di tali oggetti:

- ***File nascosti***: i file nascosti, per impostazione predefinita, non sono visibili in Windows e alcuni virus o altre minacce potrebbero tentare di evitare il rilevamento memorizzando i propri file con questo attributo. Se AVG segnala un file nascosto che si ritiene dannoso, è possibile spostarlo in ***Quarantena virus di AVG***.

- ***Cookie***: i cookie sono file di testo che vengono utilizzati dai siti Web per

memorizzare informazioni specifiche dell'utente, che vengono in seguito utilizzate per caricare layout personalizzati del sito Web, pre-immettere il nome utente e così via.

- ***Chiavi del Registro di sistema sospette***: alcuni tipi di malware memorizzano le proprie informazioni nel Registro di sistema di Windows per garantire che vengano caricate all'avvio del computer o per estenderne gli effetti al sistema operativo.

11.7.5. Scheda Rootkit

La scheda ***Rootkit*** visualizza informazioni sui rootkit rilevati durante la scansione se è stata avviata la ***scansione Anti-Rootkit*** o è stata aggiunta manualmente l'opzione relativa alla scansione anti-rootkit a ***Scansione intero computer*** (*questa opzione è disattivata per impostazione predefinita*).

Un rootkit è un programma progettato per assumere il controllo di base di un sistema senza autorizzazione da parte dei proprietari e dei gestori legittimi del sistema. *** 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.

La struttura di questa scheda corrisponde sostanzialmente a quella della ***scheda Infezioni*** o della ***scheda Spyware***.

11.7.6. 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. Con la scansione di AVG è possibile che vengano rilevati file non infetti, ma sospetti Questo tipo di file viene segnalato come ***Avviso*** oppure ***Informazioni***.

Le ***Informazioni*** sul livello di gravità possono essere segnalate per uno dei motivi seguenti:

- ***Run-time compresso***: il file è stato compresso con uno dei compressori run-time meno comuni. Questa situazione può indicare un tentativo di impedire la scansione del file. Non tutte le segnalazioni di file di questo tipo indicano tuttavia la presenza di un virus.

- ***Run-time compresso ricorsivo***: la situazione è simile a quella descritta sopra, ma meno frequente tra i programmi software di uso comune. Questo tipo di file è sospetto ed è consigliabile rimuoverlo o inviarlo per l'analisi.

- ***Archivio o documento protetto da password***: i file protetti da password non possono essere sottoposti a scansione da AVG (*o da altri programmi anti-malware*).

- ***Documenti con macro***: il documento segnalato contiene macro che possono essere dannose.

- ***Estensione nascosta***: i file con estensioni nascoste potrebbero sembrare, ad esempio, immagini, ma in realtà sono file eseguibili (*ad esempio immagine.jpg.exe*). La seconda estensione non è visibile in Windows per impostazione predefinita e AVG segnala tali file per impedirne l'apertura accidentale.

- ***Percorso di file non appropriato***: se un file di sistema importante viene eseguito da un percorso diverso da quello predefinito (*ad esempio winlogon.exe eseguito da una cartella diversa da Windows*), AVG segnala questa discrepanza. In alcuni casi, i virus utilizzano nomi di processi di sistema standard per rendere meno visibile la propria presenza nel sistema.

- ***File bloccato***: il file segnalato è bloccato, pertanto non può essere sottoposto a scansione da AVG. Ciò significa solitamente che il file viene costantemente utilizzato dal sistema (*ad esempio un file di scambio*).

11.8. 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. Lo scopo principale di ***Quarantena virus*** è quello di conservare ciascun file eliminato per un periodo di tempo sufficiente ad accertare che il file non sia più necessario nella posizione originale. Se l'assenza del file dovesse causare problemi, è possibile inviare il file in questione per l'analisi o ripristinarlo nella posizione originale.

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

- ***Gravità***: informazioni sul tipo di infezione (*in base al livello di infezione; tutti gli oggetti elencati possono essere decisamente o potenzialmente infetti*)
- ***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.
- ***Dettagli***: questo pulsante è applicabile alle sole minacce rilevate da ***Identity Protection***. Una volta selezionato, visualizza una panoramica sinottica dei dettagli della minaccia (*file/processi interessati, caratteristiche del processo e così via*). Tenere presente che per tutti gli elementi non rilevati da IDP questo pulsante è disattivato e inattivo!
- ***Elimina***: consente di rimuovere definitivamente il file infetto da ***Quarantena virus***
- ***Svuota Quarantena***: elimina completamente tutto il contenuto di ***Quarantena Virus***. I file rimossi da Quarantena virus vengono eliminati in modo definitivo dal disco (non vengono spostati nel Cestino).

12. Aggiornamenti di AVG

Mantenere AVG aggiornato è fondamentale per assicurare che tutti gli ultimi virus scoperti vengano rilevati nel più breve tempo possibile.

Durante il processo di installazione di AVG è stato richiesto di specificare la frequenza di aggiornamento di AVG. Le opzioni disponibili sono ***Ogni 4 ore*** oppure ***Ogni giorno*** (vedere la finestra di dialogo ***Pianificazione di scansioni e aggiornamenti regolari***). Poiché gli aggiornamenti di AVG non vengono rilasciati in base a una pianificazione fissa, ma in rapporto alla quantità e alla gravità di nuove minacce, si consiglia di verificare la disponibilità di nuovi aggiornamenti almeno una volta al giorno. Il controllo effettuato ogni 4 ore assicura che **AVG 9 Anti-Virus** venga mantenuto aggiornato anche durante una stessa giornata.

12.1. Livelli di aggiornamento

AVG fornisce due livelli di aggiornamento che è possibile selezionare:

- ***In Aggiornamento definizioni*** sono contenute le modifiche necessarie per una protezione anti-virus 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.

Nota: *se gli orari di un aggiornamento del programma pianificato e di una scansione pianificata dovessero coincidere, il processo di aggiornamento acquista priorità e la scansione viene interrotta.*

12.2. 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.

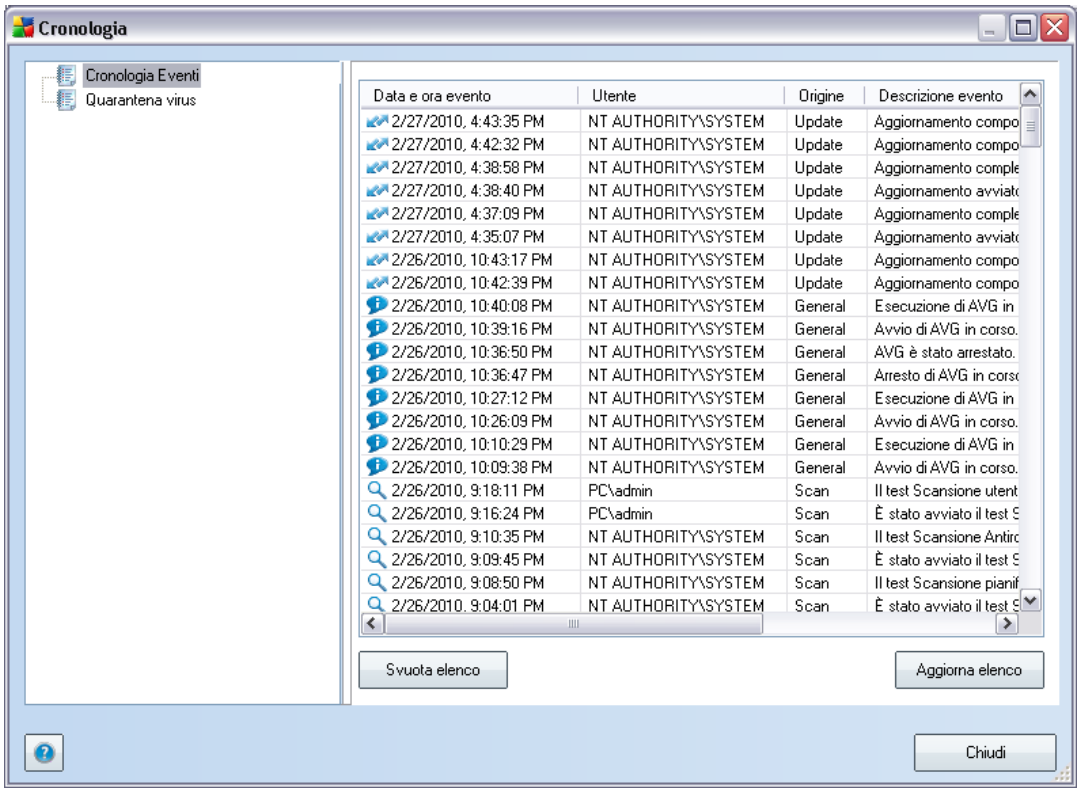
12.3. Processo di aggiornamento

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'avvio 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. L'uso è consigliato ai soli utenti esperti.*

13. 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 9 Anti-Virus**. 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 Resident Shield 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

14. FAQ e assistenza tecnica

Se si verificano problemi con AVG, di tipo commerciale o tecnico, consultare la sezione delle ***Domande frequenti*** del sito Web di AVG (http://www.avg.com/it).

Se non si riesce a risolvere il problema in questo modo, contattare il team dell'Assistenza tecnica via e-mail. Utilizzare il modulo di contatto accessibile dal menu di sistema tramite ***Guida in linea / Utilizza Guida in linea***.