AVG Internet Security 2011

Manuale per l'utente

Revisione documento 2011.21 (16.5.2011)

Sommario

1. Introduzione

Questa guida per l'utente fornisce la documentazione completa relativa a **AVG Internet Security 2011**.

Complimenti per l'acquisto di AVG Internet Security 2011!

AVG Internet Security 2011 fa parte della gamma di prodotti pluripremiati AVG progettata per fornire la tranquillità di un'esperienza informatica sicura agli utenti e la protezione completa per il PC. Analogamente a tutti i prodotti AVG, **AVG Internet Security 2011** è stato interamente riprogettato per fornire la protezione nota e accreditata di AVG in una nuova maniera più efficace e intuitiva. Il nuovo prodotto **AVG Internet Security 2011** presenta un'interfaccia semplificata combinata con funzioni di scansione più efficienti 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 specifiche esigenze. Nessun compromesso in termini di utilizzabilità e protezione.

AVG è stato progettato e sviluppato per proteggere le attività svolte con computer e reti. AVG offre agli utenti l'esperienza della protezione completa.

Tutti i prodotti AVG offrono

- Protezione specifica per le attività svolte con computer e Internet. Operazioni bancarie e acquisti, navigazione e ricerca, chat e e-mail oppure download di file e social network: AVG ha il prodotto di protezione giusto
- Protezione ottimizzata scelta da oltre 110 milioni di persone a livello mondiale e gestita da una rete globale di ricercatori altamente specializzati
- Protezione supportata dall'assistenza di esperti 24 ore su 24

2. Requisiti per l'installazione di AVG

2.1. Sistemi operativi supportati

AVG Internet Security 2011 è destinato alla protezione delle workstation che eseguono i seguenti sistemi operativi:

- 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)

(ed eventualmente Service Pack successivi per sistemi operativi specifici)

***Nota**: il componente ID Protection non è supportato in Windows XP x64. Su questo sistema operativo è possibile installare AVG Internet Security 2011, ma solo senza il componente IDP.*

2.2. Requisiti hardware minimi e consigliati

Requisiti hardware minimi per **AVG Internet Security 2011**:

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

Requisiti hardware consigliati per **AVG Internet Security 2011**:

- CPU Intel Pentium da 1,8 GHz
- 512 MB di memoria RAM
- 1400 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/).

Prima di avviare l'installazione di AVG, è consigliabile visitare il sito Web di AVG (http://www.avg.com/) 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 Internet Security 2011.

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

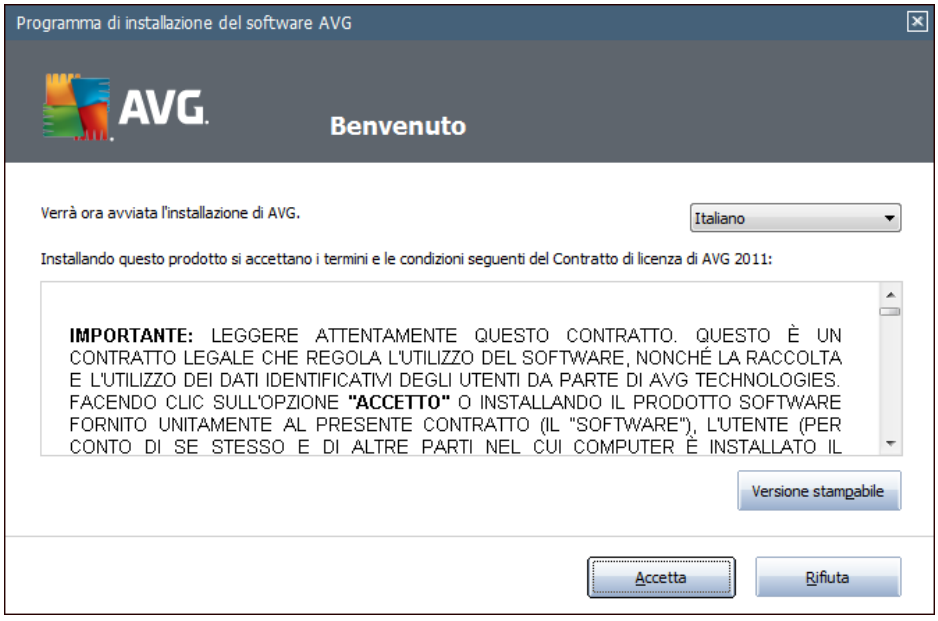
4. Processo di installazione di AVG

Per installare **AVG Internet Security 2011** nel computer è necessario disporre del file di installazione più recente. È possibile utilizzare il file di installazione presente nel CD contenuto nella confezione del 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/), sezione ***Supporto / Download.***

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:

4.1. Pagina di benvenuto

Il processo di installazione viene avviato con la ***pagina di benvenuto***. Qui è possibile selezionare la lingua utilizzata per il processo di installazione e la lingua predefinita dell'interfaccia utente di AVG. Nella sezione superiore della finestra di dialogo è presente il menu a discesa con l'elenco delle lingue disponibili:



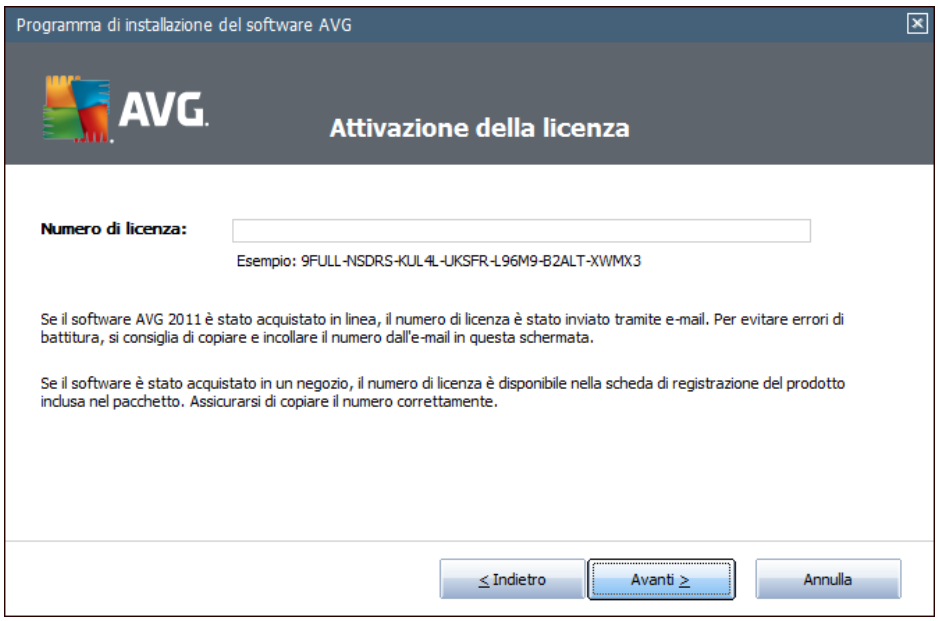
Attenzione: *in questa fase viene selezionata la lingua per il processo di installazione. La lingua selezionata verrà installata come lingua predefinita per l'interfaccia utente di AVG, insieme all'inglese che viene installato automaticamente. Per installare lingue aggiuntive per l'interfaccia utente, specificarle in una delle seguenti finestre di dialogo di impostazione denominate* ***Opzioni personalizzate****.*

In questa finestra di dialogo è inoltre disponibile l'intero contenuto del contratto di licenza di AVG. Leggere attentamente i termini del contratto. Per confermare che il contratto è stato letto e accettato, selezionare il pulsante ***Accetto***. Se non si accettano i termini del contratto di licenza, fare clic sul pulsante ***Rifiuta***. Il processo di installazione verrà interrotto immediatamente.

4.2. Attiva la licenza AVG

Nella finestra di dialogo ***Attiva la licenza AVG*** viene richiesto di immettere il numero di licenza nel campo di testo fornito.

Il numero di vendita è disponibile sulla custodia del CD incluso nella confezione di **AVG Internet Security 2011** . Il numero di licenza sarà contenuto nel messaggio e-mail di conferma ricevuto dopo l'acquisto in linea di **AVG Internet Security 2011**. 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.

4.3. Selezionare il tipo di installazione

La finestra di dialogo ***Selezionare il tipo di installazione*** offre due opzioni di installazione: ***Installazione rapida*** e ***Installazione personalizzata***.

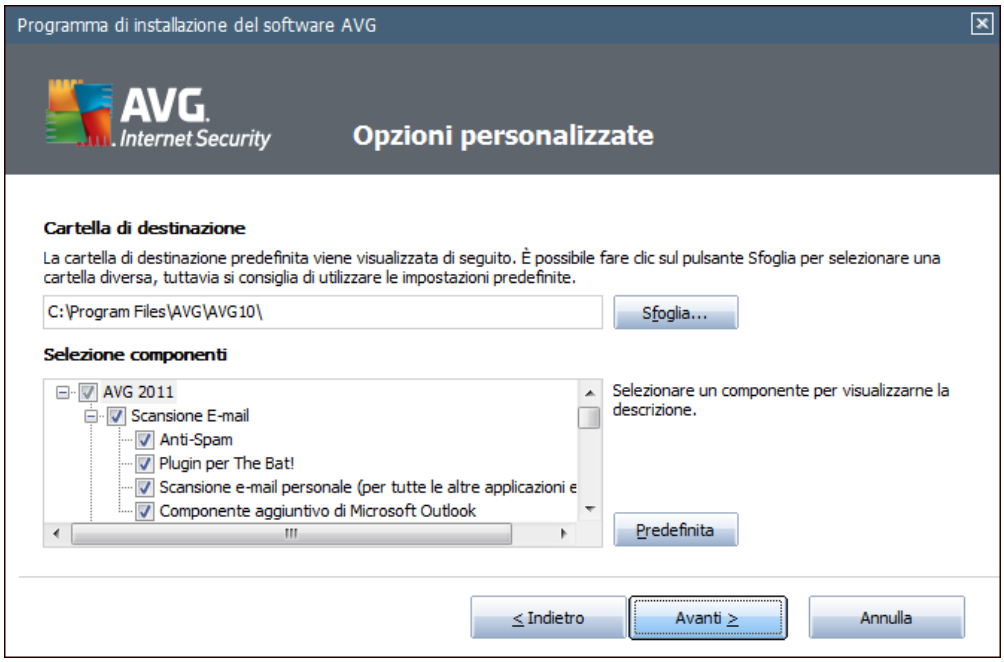
Alla maggior parte degli utenti si consiglia di mantenere l'***installazione rapida*** standard che consente di installare AVG in modalità completamente automatica con le impostazioni predefinite dal produttore del software. La configurazione fornisce la massima protezione combinata con l'utilizzo ottimale delle risorse. In futuro, se ci fosse necessità di modificare la configurazione, sarà possibile farlo direttamente nell'applicazione AVG. Se è stata selezionata l'opzione ***Installazione rapida***, selezionare il pulsante ***Avanti*** per passare alla finestra di dialogo ***Installa AVG Security Toolbar***.

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. Se è stata selezionata questa opzione, selezionare il pulsante ***Avanti*** per passare alla finestra di dialogo ***Opzioni personalizzate***.

Nella sezione destra della finestra di dialogo è disponibile la casella di controllo correlata al ***gadget AVG*** (*supportato in Windows Vista/Windows 7*). Per installare questo gadget, selezionare la relativa casella di controllo. ***Il gadget AVG*** sarà quindi accessibile dalla Sidebar di Windows e fornirà accesso immediato alle funzioni più importanti di **AVG Internet Security 2011**, ossia scansione e aggiornamento.

4.4. Opzioni personalizzate

La finestra di dialogo ***Opzioni personalizzate*** consente di impostare due parametri dell'installazione:



Cartella di destinazione

All'interno della sezione ***Cartella di destinazione*** è possibile specificare la posizione in cui **AVG Internet Security 2011** deve essere installato. Per impostazione predefinita, AVG viene installato nella cartella dei programmi che si trova nell'unità C:. Se si desidera modificare questa posizione, utilizzare il pulsante ***Sfoglia*** per visualizzare la struttura dell'unità e selezionare la cartella pertinente.

Selezione componenti

La sezione ***Selezione componenti*** visualizza una panoramica di tutti i componenti di **AVG Internet Security 2011** che è possibile installare. Se le impostazioni predefinite non sono adeguate alle esigenze specifiche, è possibile rimuovere/aggiungere determinati componenti.

È tuttavia possibile eseguire la selezione solo tra i componenti inclusi nell'edizione di AVG che è stata acquistata.

Evidenziare una voce dell'elenco ***Selezione componenti*** per visualizzare una breve descrizione del relativo componente nella parte destra della sezione. Per informazioni dettagliate sulla funzionalità di ciascun componente, consultare il capitolo ***Panoramica dei componenti*** di questo documento. Per ripristinare la configurazione predefinita dal fornitore del software, utilizzare il pulsante ***Predefinita***.

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

4.5. Installa AVG Security Toolbar

Nella finestra di dialogo ***Installa AVG Security Toolbar*** è possibile decidere se installare o meno ***AVG Security Toolbar***. 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. 3.0 o successiva*) per offrire la protezione in linea completa durante l'esplorazione di Internet.

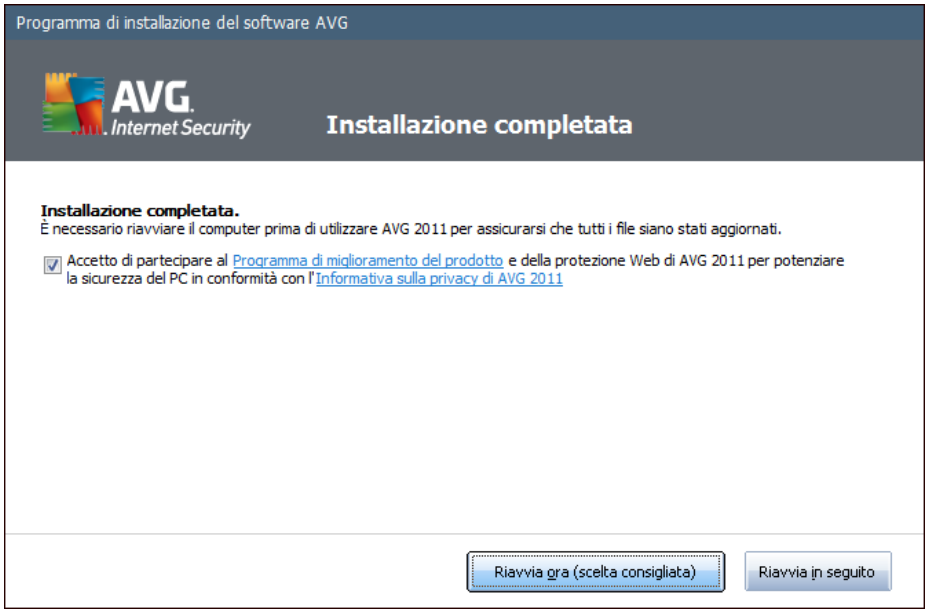
È inoltre possibile scegliere se utilizzare *AVG Secure Search (powered by Google)* come provider di ricerca predefinito. In caso affermativo, mantenere la relativa casella di controllo selezionata.

4.6. Avanzamento dell'installazione

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

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

4.7. Installazione completata



La finestra di dialogo ***Installazione completata*** conferma che **AVG Internet Security 2011** è stato installato e configurato correttamente.

In questa finestra di dialogo fornire le informazioni di contatto per poter ricevere tutte le informazioni e le novità correlate al prodotto. Sotto il modulo di registrazione sono disponibili le due opzioni seguenti:

- ***Sì, voglio essere informato circa notizie sulla protezione e offerte speciali di AVG 2011 via e-mail***: selezionare la casella di controllo per indicare che si desidera essere informati circa novità relative alla protezione Internet e ricevere informazioni su offerte speciali, miglioramenti, aggiornamenti e così via relativi ai prodotti AVG.

- ***Accetto di partecipare al Programma di miglioramento del prodotto e della protezione Web di AVG 2011...***: selezionare la casella di controllo per confermare che si desidera partecipare al Programma di miglioramento del prodotto (*per dettagli, vedere il capitolo Impostazioni avanzate di AVG / Programma di miglioramento del prodotto*) nell'ambito del quale vengono raccolte informazioni anonime sulle minacce rilevate per aumentare il livello di protezione generale in Internet.

Per finalizzare il processo di installazione è necessario riavviare il computer: selezionare ***Riavvia subito*** per riavviare il computer immediatamente oppure ***Riavvia in seguito*** per posticipare l'operazione.

> ***Nota:*** *se si utilizza una licenza aziendale di AVG e si è scelto di installare Amministrazione remota (vedere Opzioni personalizzate), la finestra di dialogo Installazione completata viene visualizzata come segue:*
>
> *È necessario specificare i parametri 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.*** *Per informazioni dettagliate su Amministrazione remota di AVG, consultare il Manuale per l'utente di AVG Business Edition disponibile per il download sul sito Web di AVG (http://www.avg.com/).*

5. Dopo l'installazione

5.1. Registrazione del prodotto

Una volta completata l'installazione di **AVG Internet Security 2011**, registrare il prodotto in linea sul sito Web di AVG (http://www.avg.com/), 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.

5.2. 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
- tramite doppio clic sulla riga dello stato situata nella sezione inferiore del ***gadget AVG*** (*se installato; supportato su Windows Vista/Windows 7*)
- dal menu ***Start/Programmi/AVG 2011/Interfaccia utente di AVG***
- da ***AVG Security Toolbar*** tramite l'opzione ***Avvia AVG***

5.3. Scansione dell'intero computer

Esiste il rischio potenziale che un virus sia stato trasmesso al computer dell'utente prima dell'installazione di **AVG Internet Security 2011**. 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*** .

5.4. Controllo Eicar

Per confermare che **AVG Internet Security 2011** 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 poiché non si tratta di un vero virus e non include frammenti di codice virale. La maggior parte dei prodotti vi reagisce come se si trattasse di un virus, *anche se normalmente lo segnala con un nome ovvio come "EICAR-AV-Test"*. È possibile scaricare il virus EICAR dal sito Web di EICAR all'indirizzowww.eicar.com, in cui si troveranno anche tutte le informazioni necessarie sul controllo EICAR.

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.**

5.5. Configurazione predefinita di AVG

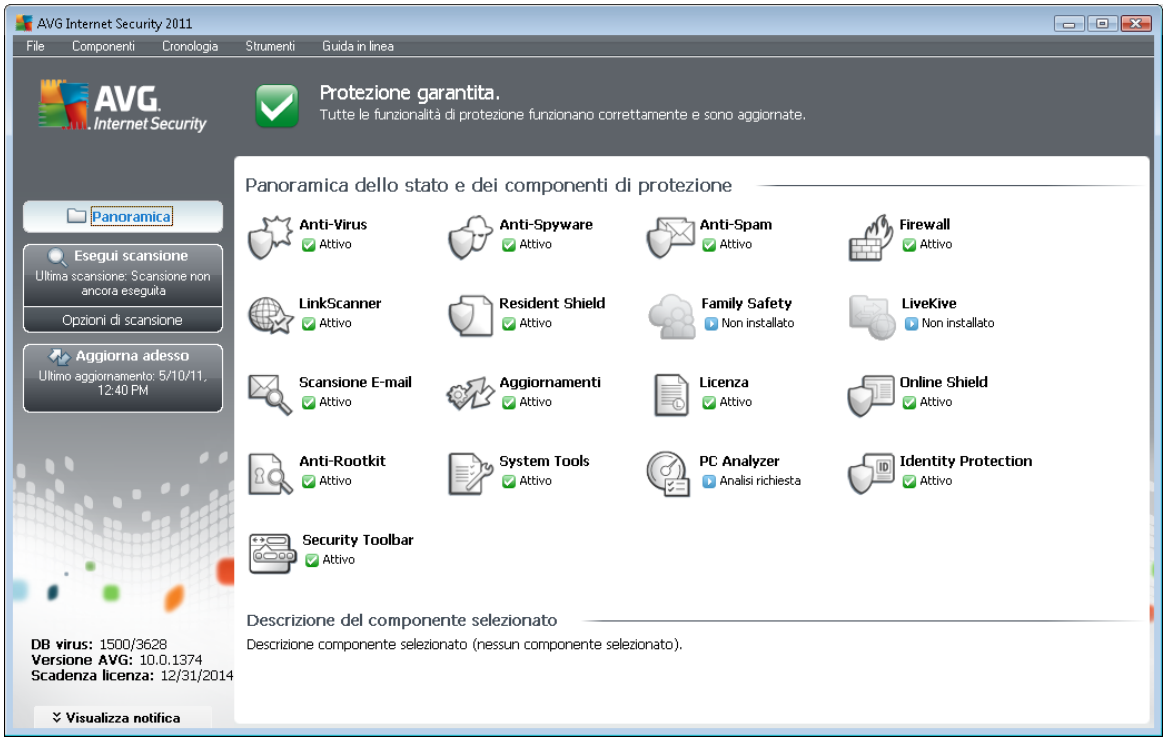
La configurazione predefinita (*ovvero la modalità di impostazione dell'applicazione dopo l'installazione*) di **AVG Internet Security 2011** è impostata dal fornitore del software in modo tale che tutti i componenti e le funzioni offrano un'ottimizzazione massima delle prestazioni.

A meno che non vi sia un motivo valido, si consiglia di non modificare la configurazione di AVG. Le eventuali modifiche alle impostazioni devono essere eseguite solo da utenti esperti.

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

6. Interfaccia utente di AVG

AVG Internet Security 2011 si apre visualizzando la finestra principale:



La finestra principale è suddivisa in diverse sezioni:

- ***Menu di sistema*** *(riga di sistema visualizzata nella parte superiore della finestra)*: è lo strumento di 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*** *(sezione inferiore sinistra della 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 >>
- ***Gadget AVG*** *(sidebar di Windows, supportata in Windows Vista/7)*: consente l'accesso rapido alle scansioni e agli aggiornamenti di AVG - dettagli >>

6.1. 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 Internet Security 2011**. 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:

6.1.1. File

- ***Esci***: consente di chiudere l'interfaccia utente di **AVG Internet Security 2011**. Tuttavia, l'applicazione AVG continuerà a essere eseguita in background e il computer sarà comunque protetto.

6.1.2. Componenti

Alla voce ***Componenti*** del menu di sistema sono disponibili i collegamenti a tutti i componenti AVG installati che consentono di aprire la rispettiva 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 del relativo stato
- ***Anti-Virus*** assicura che il computer sia protetto dai virus che tentano di accedervi - dettagli >>
- ***Anti-Spyware*** assicura che il computer sia protetto da spyware e adware - dettagli >>
- ***Anti-Spam*** controlla tutti i messaggi e-mail in entrata e contrassegna quelli indesiderati come SPAM - dettagli >>
- ***Firewall*** controlla il modo in cui il computer scambia dati con altri computer in Internet o nella rete locale - dettagli >>
- ***Link Scanner*** controlla i risultati delle ricerche visualizzati nel browser Internet - dettagli >>
- ***Scansione E-mail*** controlla la posta in entrata e in uscita per rilevare eventuali virus - dettagli >>
- ***Family Safety*** aiuta a monitorare le attività in linea dei bambini e li protegge dai contenuti inappropriati presenti nei siti Web - dettagli >>
- ***LiveKive*** fornisce il backup automatico dei dati in linea - 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 >>
- ***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 >>

- ***Anti-Rootkit*** rileva i programmi e le tecnologie che tentano di camuffare i malware - dettagli >>
- ***System Tools*** offre un riepilogo dettagliato dell'ambiente AVG e informazioni sul sistema operativo - dettagli >>
- ***PC Analyzer*** fornisce informazioni sullo stato del computer - dettagli >>
- ***Identity Protection*** è un componente anti-malware destinato alla prevenzione di attacchi da parte di malintenzionati volti a sottrarre preziosi dati digitali personali - dettagli >>
- ***Security Toolbar*** consente di utilizzare funzionalità AVG selezionate direttamente dal browser Internet - dettagli >>
- ***Amministrazione remota*** è disponibile nelle versioni AVG Business Edition se durante il processo di installazione è stato richiesto di installare questo componente

6.1.3. 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 Internet Security 2011** registrate
- ***Firewall***: consente di aprire l'interfaccia di impostazione del Firewall sulla scheda ***Log*** con una panoramica dettagliata di tutte le azioni del componente Firewall

6.1.4. Strumenti

- ***Scansione computer***: consente di passare all'interfaccia di scansione di AVG e di avviare la 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 Internet Security 2011**.

- ***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*** in cui è possibile modificare la configurazione di **AVG Internet Security 2011**. In genere è consigliabile mantenere le impostazioni dell'applicazione predefinite dal fornitore del software.

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

6.1.5. 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/) alla pagina del centro di assistenza clienti

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

- ***Informazioni sui virus e sulle minacce***: consente di aprire l'***Enciclopedia dei virus*** in rete in cui è possibile trovare informazioni dettagliate sul virus identificato

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

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

Nota*: se è in uso la versione Trial di* **AVG Internet Security 2011***, le ultime due voci appaiono come* ***Acquista ora*** *e* ***Attiva****, consentendo di acquistare subito la versione completa del programma. Per* **AVG Internet Security 2011** *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***.

6.2. 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 Internet Security 2011**. Vedere la panoramica delle icone eventualmente visualizzate in questa sezione, con 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 controllare le relative proprietà/impostazioni. Non sono presenti problemi gravi in AVG e probabilmente si è deciso di disattivare alcuni componenti per qualche ragione. La protezione di AVG è comunque attiva. Tuttavia, prestare attenzione alle impostazioni 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 dell'Assistenza tecnica di AVG.

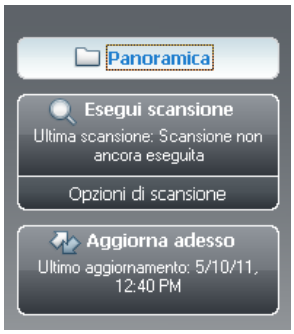
Se AVG non è impostato per prestazioni ottimali, un nuovo pulsante denominato Correggi (oppure Correggi tutto se il problema riguarda più componenti) appare accanto alle informazioni sullo stato della protezione. Selezionare il pulsante per avviare un processo automatico di controllo e configurazione del programma. Questo è un modo rapido per impostare AVG per prestazioni ottimali e ottenere il livello di protezione massimo.

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.*

6.3. Collegamenti rapidi

Collegamenti rapidi *(nella sezione sinistra dell'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*** >>
- ***Esegui scansione adesso***: per impostazione predefinita, il pulsante fornisce informazioni sull'ultima scansione avviata (*tipo di scansione, data dell'ultimo avvio*). È possibile utilizzare il comando ***Esegui scansione adesso*** per avviare di nuovo la stessa scansione oppure seguire il collegamento ***Opzioni di scansione*** per aprire l'interfaccia di scansione di AVG in cui è possibile eseguire o pianificare le scansioni oppure modificarne i parametri; vedere il capitolo ***Scansione AVG*** >>
- ***Aggiorna adesso***: il collegamento fornisce la data dell'ultimo avvio del processo di aggiornamento. Selezionare il pulsante per aprire l'interfaccia di aggiornamento ed eseguire immediatamente il processo di aggiornamento di AVG; vedere il capitolo ***Aggiornamenti 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, ma i collegamenti rimarranno comunque disponibili. Inoltre, il processo in esecuzione viene visualizzato con un'ulteriore rappresentazione grafica.

6.4. Panoramica dei componenti

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

- Panoramica di tutti i componenti installati, costituita da un riquadro con le icone dei componenti e le informazioni sul relativo stato attivo o inattivo
- Descrizione di un componente selezionato

In **AVG Internet Security 2011** la sezione ***Panoramica dei componenti*** contiene informazioni sui seguenti componenti:

- ***Anti-Virus*** assicura che il computer sia protetto dai virus che tentano di accedervi - dettagli >>
- ***Anti-Spyware*** assicura che il computer sia protetto da spyware e adware - dettagli >>
- ***Anti-Spam*** controlla tutti i messaggi e-mail in entrata e contrassegna quelli indesiderati come SPAM - dettagli >>
- ***Firewall*** controlla il modo in cui il computer scambia dati con altri computer in Internet o nella rete locale - dettagli >>
- ***Link Scanner*** controlla i risultati delle ricerche visualizzati nel browser Internet - dettagli >>
- ***Scansione E-mail*** controlla la posta in entrata e in uscita per rilevare eventuali virus - dettagli >>
- ***Resident Shield*** viene eseguito in background ed esegue la scansione dei file mentre questi vengono copiati, aperti o salvati - dettagli >>
- ***Family Safety*** aiuta a monitorare le attività in linea dei bambini e li protegge dai contenuti inappropriati presenti nei siti Web - dettagli >>
- ***LiveKive*** fornisce il backup automatico dei dati in linea - dettagli >>
- ***Gestore aggiornamenti*** controlla tutti gli aggiornamenti AVG - 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 >>
- ***Anti-Rootkit*** rileva i programmi e le tecnologie che tentano di camuffare i malware - dettagli >>
- ***System Tools*** offre un riepilogo dettagliato dell'ambiente AVG e informazioni sul sistema operativo - dettagli >>
- ***PC Analyzer*** fornisce informazioni sullo stato del computer - dettagli >>
- ***Identity Protection*** è un componente anti-malware destinato alla prevenzione di attacchi da parte di malintenzionati volti a sottrarre preziosi dati digitali personali - dettagli >>
- ***Security Toolbar*** consente di utilizzare funzionalità AVG selezionate direttamente dal browser Internet - dettagli >>
- ***Amministrazione remota*** è disponibile nelle versioni AVG Business Edition se durante il processo di installazione è stato richiesto di installare questo componente

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 del

componente 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.

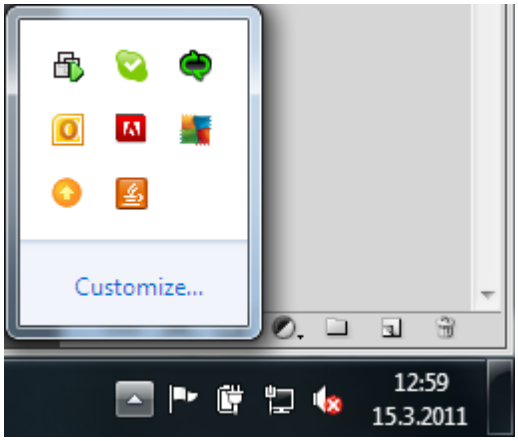
6.5. Statistiche

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

- ***Virus DB***: contiene informazioni sulla versione correntemente installata del database dei virus
- ***Versione AVG***: contiene informazioni sulla versione AVG installata *(il formato del numero è 10.0.xxxx, dove 10.0 indica la versione della linea del prodotto e xxxx indica il numero di build)*
- ***Scadenza licenza:***: indica la data della scadenza della licenza di AVG

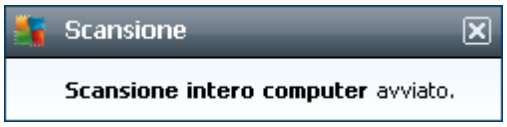
6.6. Icona della barra delle applicazioni

L'icona della barra delle applicazioni (*presente nella barra delle applicazioni di Windows*) indica lo stato corrente di **AVG Internet Security 2011**. 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, attivazione dei profili Firewall, 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
- ***Scansioni***: fare clic per aprire il menu di scelta rapida di
- ***Firewall***: fare clic per aprire il menu di scelta rapida delle opzioni di impostazione del Firewall in cui è possibile modificare i parametri principali: stato del Firewall (*firewall abilitato/firewall disabilitato/modalità di emergenza*), passaggio alla modalità gioco e profili Firewall
- ***Esegui PC Analyzer***: fare clic per avviare il componente PC Analyzer
- ***Esecuzione delle scansioni in corso***: questa voce viene visualizzata solo se una scansione è in esecuzione sul computer. Per questa scansione è possibile impostare la priorità oppure arrestarla o sospenderla. Inoltre, sono accessibili le seguenti azioni: *Imposta priorità per tutte le scansioni, Sospendi tutte le scansioni* o *Arresta tutte le scansioni*.
- ***Aggiorna adesso***: viene avviato un aggiornamento immediato
- ***Guida in linea***: apre il file della Guida alla pagina iniziale

6.7. Gadget AVG

Il ***gadget AVG*** viene visualizzato sul desktop di Windows (*Windows Sidebar*). Questa applicazione è supportata solo sui sistemi operativi Windows Vista e Windows 7. Il ***gadget AVG*** offre l'accesso immediato alle funzionalità più importanti di **AVG Internet Security 2011**, ossia scansione e aggiornamento:

Il ***gadget AVG*** fornisce le seguenti opzioni di accesso rapido:

- ***Esegui scansione adesso***: fare clic sul collegamento ***Esegui scansione adesso*** per avviare direttamente la ***scansione dell'intero computer***. È possibile visualizzare l'avanzamento del processo di scansione nell'interfaccia utente alternativa del gadget. Una breve panoramica delle statistiche fornisce informazioni sul numero di oggetti esaminati, minacce rilevate e minacce corrette. È possibile sospendere o arrestare il processo di scansione in corso in qualsiasi momento. Per dati dettagliati relativi ai risultati di scansione, consultare la finestra di dialogo standard ***Panoramica risultati di scansione*** che può essere aperta direttamente dal gadget tramite l'opzione ***Mostra dettagli*** (i risultati di scansione pertinenti verranno elencati alla voce ***Scansione gadget sidebar***).

- ***Aggiorna adesso***: fare clic sul collegamento ***Aggiorna adesso*** per avviare l'aggiornamento AVG direttamente dal gadget:

- ***Collegamento Twitter***: apre una nuova interfaccia del ***gadget AVG*** che fornisce una panoramica dei feed AVG più recenti pubblicati in Twitter. Seguire il collegamento ***Visualizza tutti i feed Twitter di AVG*** per aprire il browser Internet in una nuova finestra e passare direttamente al sito Web Twitter, in corrispondenza della pagina dedicata alle notizie relative a AVG:

- ***Collegamento Facebook***: apre il browser Internet con il sito Web Facebook, in corrispondenza della pagina dedicata alla ***community AVG***

- ***LinkedIn*** ***:*** questa opzione è disponibile solo nell'installazione di rete (*ossia se AVG è stato installato utilizzando una licenza AVG Business Edition*) e apre il browser Internet in corrispondenza del sito Web ***AVG SMB Community*** all'interno del social network LinkedIn

- ***PC Analyzer*** : apre l'interfaccia utente in corrispondenza del componente ***PC Analyzer***

- ***Casella di ricerca***: digitare una parola chiave per ottenere subito i risultati della ricerca in una nuova finestra del browser Web predefinito

7. Componenti di AVG

7.1. Anti-Virus

7.1.1. Principi dell'Anti-Virus

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 ricercare virus noti. Tutti i virus rilevati verranno bloccati per essere poi corretti o messi in quarantena. La maggior parte dei software antivirus utilizza anche la scansione euristica che consente di rilevare le caratteristiche tipiche dei 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.

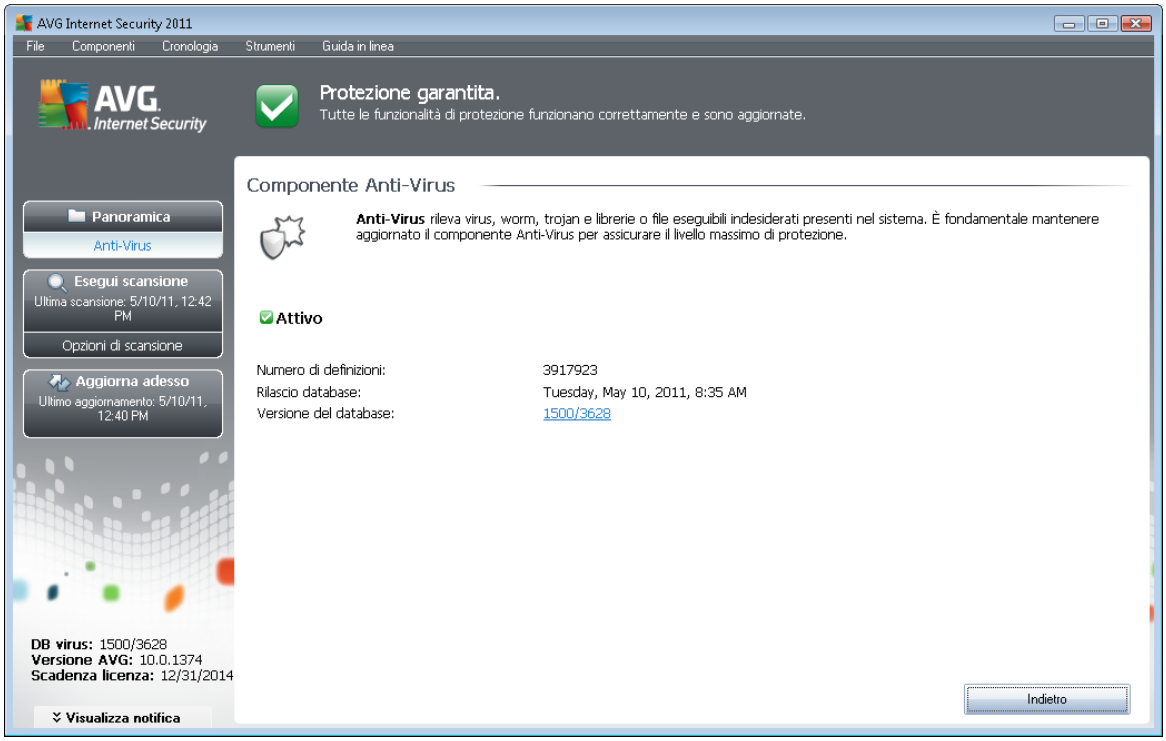
La funzione principale della protezione antivirus è impedire l'esecuzione di virus noti sul computer.

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). AVG esegue inoltre la scansione del Registro di sistema alla ricerca di voci sospette, dei file Internet temporanei e dei cookie di rilevamento e consente di trattare tutti gli elementi potenzialmente dannosi come avviene per le altre infezioni.

7.1.2. Interfaccia dell'Anti-Virus



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

- ***Numero di definizioni***: indica il numero di virus definiti nella versione aggiornata del database dei virus
- ***Rilascio 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 del database dei virus installato. Il numero viene incrementato dopo ogni aggiornamento del database dei virus

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

7.2. Anti-Spyware

7.2.1. Principi dell'Anti-Spyware

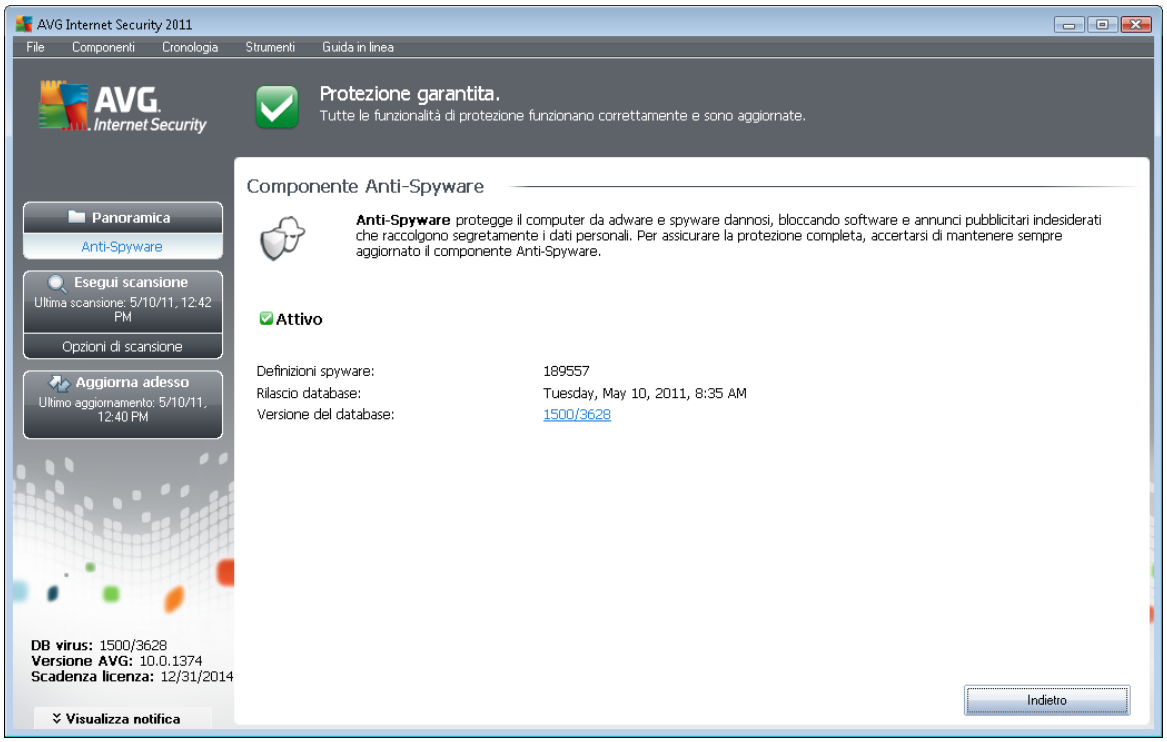
In genere, per spyware si intende un particolare tipo di malware, ovvero un software che raccoglie informazioni dal computer senza informarne l'utente e senza richiederne l'autorizzazione. Alcune applicazioni spyware possono anche essere installate intenzionalmente e spesso contengono

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, ad esempio i messaggi 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 Internet Security 2011** 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. È inoltre possibile rilevare malware inattivo, ovvero malware che è stato scaricato ma non ancora attivato.

7.2.2. Interfaccia dell'Anti-Spyware



L'interfaccia del componente ***Anti-Spyware*** fornisce una breve panoramica della funzionalità del componente, informazioni sullo stato corrente e alcune statistiche di ***Anti-Spyware***:

- ***Definizioni spyware***: indica il numero di campioni di spyware definiti nella versione più recente del database degli spyware
- ***Rilascio database***: specifica in che giorno e a che ora è stato eseguito l'ultimo aggiornamento del database degli spyware
- ***Versione del database***: indica il numero della versione più recente del database degli

spyware. Il numero viene incrementato dopo ogni aggiornamento del database dei virus

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

7.3. Anti-Spam

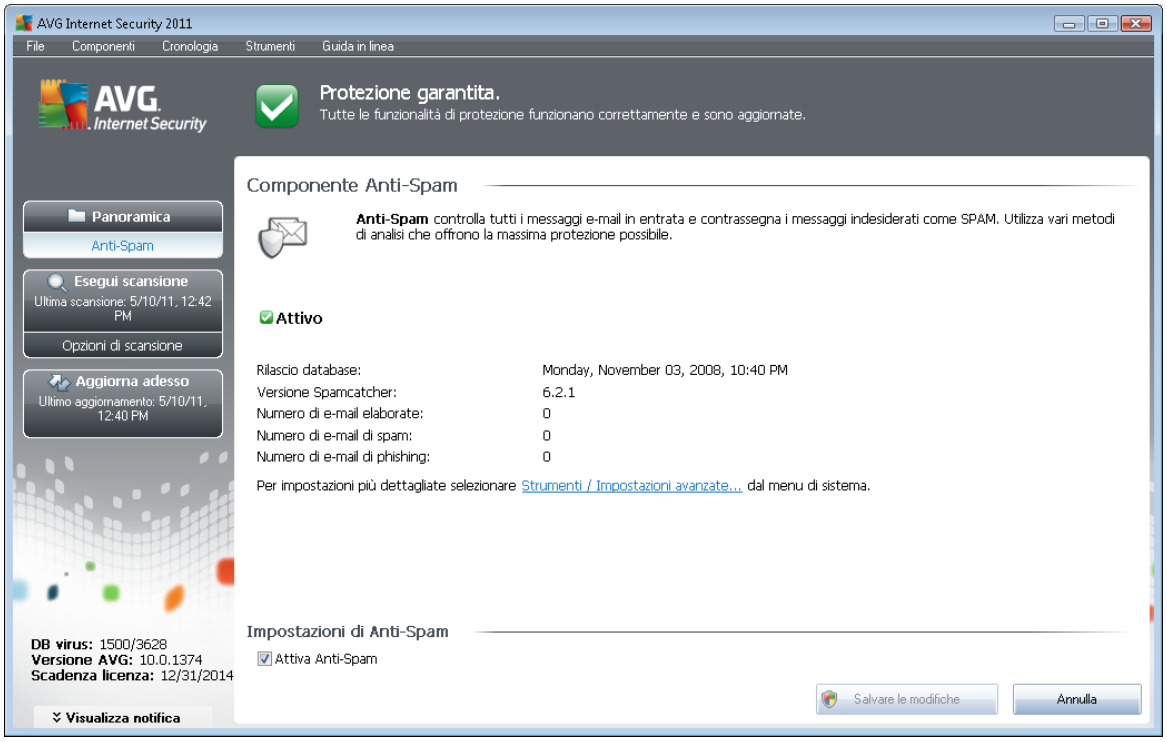
Il termine "spam" indica messaggi di posta indesiderati, per lo più pubblicità di prodotti o servizi, inviati in massa e simultaneamente a un enorme numero di indirizzi di posta elettronica, che intasano le cassette postali dei destinatari. Lo spam non rientra nella categoria dei legittimi messaggi di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

7.3.1. Principi dell'Anti-Spam

AVG Anti-Spam controlla tutti i messaggi e-mail in entrata e contrassegna quelli indesiderati come spam. ***AVG Anti-Spam*** può modificare l'oggetto dell'e-mail (*identificata come spam*) aggiungendo una stringa di testo speciale. Sarà quindi possibile filtrare rapidamente le e-mail nel client e-mail.

Il componente AVG Anti-Spam utilizza diversi metodi di analisi per elaborare ciascun messaggio e-mail, offrendo il massimo livello di protezione possibile contro i messaggi e-mail indesiderati. ***AVG Anti-Spam*** utilizza un database aggiornato regolarmente per il rilevamento dello spam. È inoltre possibile utilizzare i server RBL (*database pubblici di indirizzi e-mail di spammer noti*) e aggiungere manualmente indirizzi e-mail alla whitelist (*indirizzi da non contrassegnare mai come spam*) e alla blacklist (*indirizzi da contrassegnare sempre come spam*).

7.3.2. Interfaccia dell'Anti-Spam



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

- ***Rilascio database***: specifica quando e a che ora il database anti-spam è stato aggiornato e pubblicato
- ***Versione di Spamcatcher***: indica il numero della versione più recente del motore anti-spam
- ***Numero di e-mail elaborate***: indica il numero di messaggi e-mail sottoposti a scansione dall'ultimo avvio del motore anti-spam
- ***Numero di e-mail di spam***: di tutte le e-mail sottoposte a scansione, indica il numero di messaggi contrassegnati come spam
- ***Numero di e-mail di phishing***: di tutte le e-mail sottoposte a scansione, indica il numero di messaggi contrassegnati come attacchi di phishing

La finestra di dialogo ***Anti-Spam*** fornisce inoltre il collegamento a ***Strumenti/Impostazioni avanzate***. Utilizzare il collegamento per passare all'ambiente di configurazione avanzata di tutti i componenti di **AVG Internet Security 2011**.

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. Le eventuali modifiche alle impostazioni devono essere eseguite solo da utenti esperti.*

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

7.4. Firewall

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

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

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

Consiglio: *in genere non è consigliabile utilizzare più di un firewall su un singolo computer. Il livello*

di protezione del computer non è maggiore se si installano più firewall. È più probabile che si verifichino conflitti tra queste applicazioni. Si consiglia, pertanto, di utilizzare un solo firewall nel computer e di disattivare gli altri, eliminando così il rischio di possibili conflitti e problemi correlati.

7.4.1. Principi del Firewall

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

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

Funzionalità di AVG Firewall:

- Consente o blocca automaticamente tentativi di comunicazione di applicazioni note o chiede conferma
- Utilizza profili completi con regole predefinite, in base alle esigenze personali
- Attiva profili automaticamente durante la connessione a varie reti o durante l'utilizzo di diverse schede di rete

7.4.2. Profili Firewall

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

Profili disponibili

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

Questo profilo di sistema non può essere duplicato o eliminato e le relative impostazioni non possono essere modificate.

- ***Profili personalizzati***:

  - ***Direttamente connesso a Internet***: adatto per i normali computer desktop domestici connessi direttamente a Internet o per i notebook che si connettono a Internet fuori dalla rete aziendale protetta. Selezionare questa opzione se si effettua la connessione da casa o dalla rete di una piccola azienda senza controllo centralizzato. Selezionare inoltre questa opzione quando, durante un viaggio, si effettua la connessione con il notebook da vari luoghi sconosciuti e potenzialmente pericolosi (*Internet Point, stanze di albergo e così via*). Verranno create regole più restrittive, poiché si presume che questi computer non abbiano protezione aggiuntiva, quindi richiedano la protezione massima.

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

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

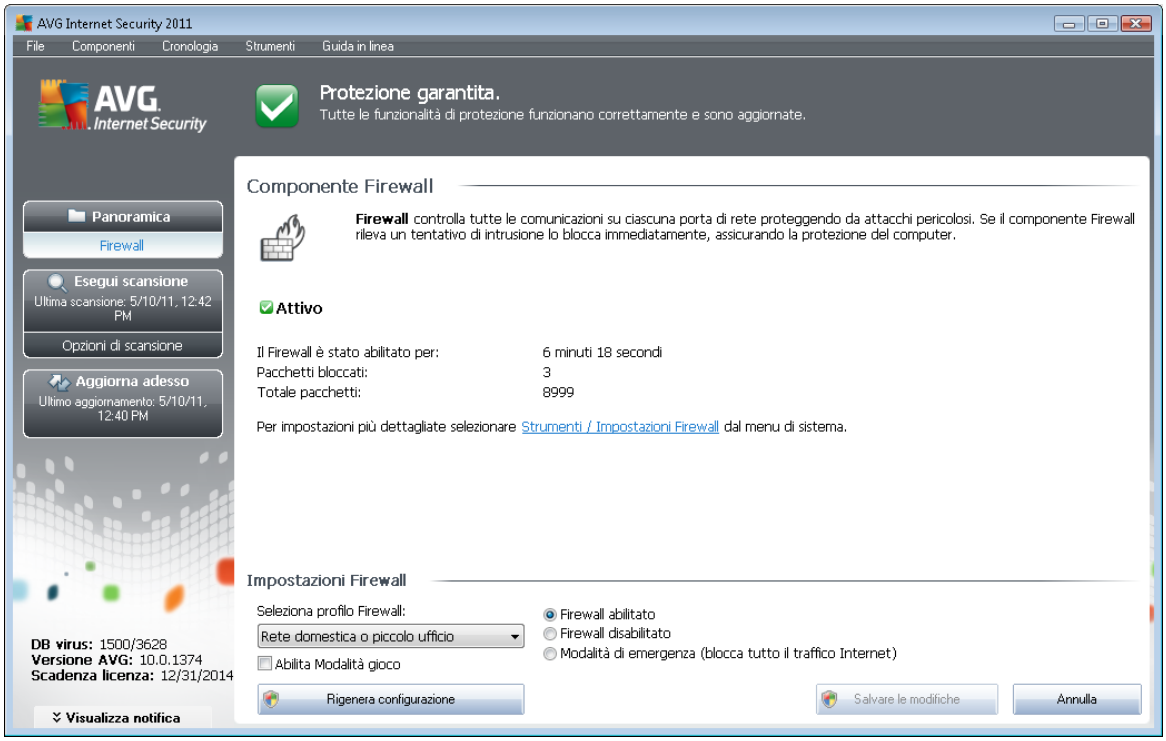
Attivazione profili

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

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

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

7.4.3. Interfaccia del Firewall



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

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

Impostazioni Firewall

- ***Seleziona profilo firewall***: dal menu a discesa scegliere uno dei profili definiti: due profili sono disponibili in ogni momento (i *profili predefiniti denominati* ***Permetti Tutto*** *e* ***Blocca Tutto***), altri profili sono stati aggiunti manualmente mediante la modifica dei profili nella finestra di dialogo ***Profili*** in ***Impostazioni Firewall***.
- ***Abilita modalità gioco***: selezionare questa opzione per assicurare che, durante l'esecuzione di applicazioni a schermo intero (*giochi, presentazioni, film e così via*), il ***Firewall*** non visualizzi finestre di dialogo per richiedere se consentire o bloccare la comunicazione per applicazioni sconosciute. Se un'applicazione sconosciuta tenta di comunicare sulla rete in quel momento, il ***Firewall*** consente o blocca automaticamente il tentativo in base alle impostazioni presenti nel profilo corrente. ***Nota:*** se la modalità gioco è attivata, tutte le attività pianificate (scansioni e aggiornamenti) vengono posticipate finché

l'applicazione non viene chiusa.

- ***Stato del firewall***:
  - ***Firewall abilitato***: selezionare questa opzione per consentire la comunicazione alle applicazioni contrassegnate come 'consentite' nell'insieme di regole definito all'interno del profilo ***Firewall*** selezionato
  - ***Firewall disabilitato***: questa opzione consente di disattivare completamente il componente ***Firewall***. Tutto il traffico di rete viene consentito ma non controllato.
  - ***Modalità di emergenza (blocca tutto il traffico Internet)***: selezionare questa opzione per bloccare tutto il traffico su ogni singola porta di rete; il ***Firewall*** è ancora in esecuzione ma tutto il traffico di rete viene interrotto

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. Le eventuali modifiche alle impostazioni devono essere eseguite solo da utenti esperti. Se è necessario modificare la configurazione del Firewall, selezionare la voce di menu di sistema* ***Strumenti / Impostazioni Firewall*** *e modificare la configurazione del Firewall nella finestra di dialogo* ***Impostazioni Firewall*** *visualizzata.*

Pulsanti di controllo

- ***Rigenera configurazione***: selezionare questo pulsante per sovrascrivere la configurazione corrente del ***Firewall*** e ripristinare la configurazione predefinita basata sul rilevamento automatico.
- ***Salva modifiche***: selezionare questo pulsante per salvare e applicare le eventuali modifiche eseguite in questa finestra di dialogo
- ***Annulla***: selezionare questo pulsante per tornare all'***interfaccia utente di AVG*** predefinita (*panoramica dei componenti*).

7.5. Link Scanner

7.5.1. Principi di Link Scanner

LinkScanner protegge dal numero sempre crescente di minacce transitorie presenti sul Web. Queste minacce possono nascondersi in qualsiasi tipo di sito Web, da quelli degli enti governativi, a quelli di grandi marchi famosi, a quelli di piccole aziende, e raramente restano in questi siti per più di 24 ore. ***LinkScanner*** protegge gli utenti analizzando le pagine Web dietro a tutti i collegamenti presenti sulla pagina Web visualizzata e garantendo che le pagine siano sicure nel momento cruciale, ovvero nell'attimo in cui si sta per fare clic sul collegamento.

La tecnologia ***LinkScanner*** è costituita da due funzionalità, ***Search-Shield*** e ***Surf-Shield***:

- ***Search-Shield*** contiene un elenco di siti Web (*indirizzi URL*) notoriamente pericolosi.

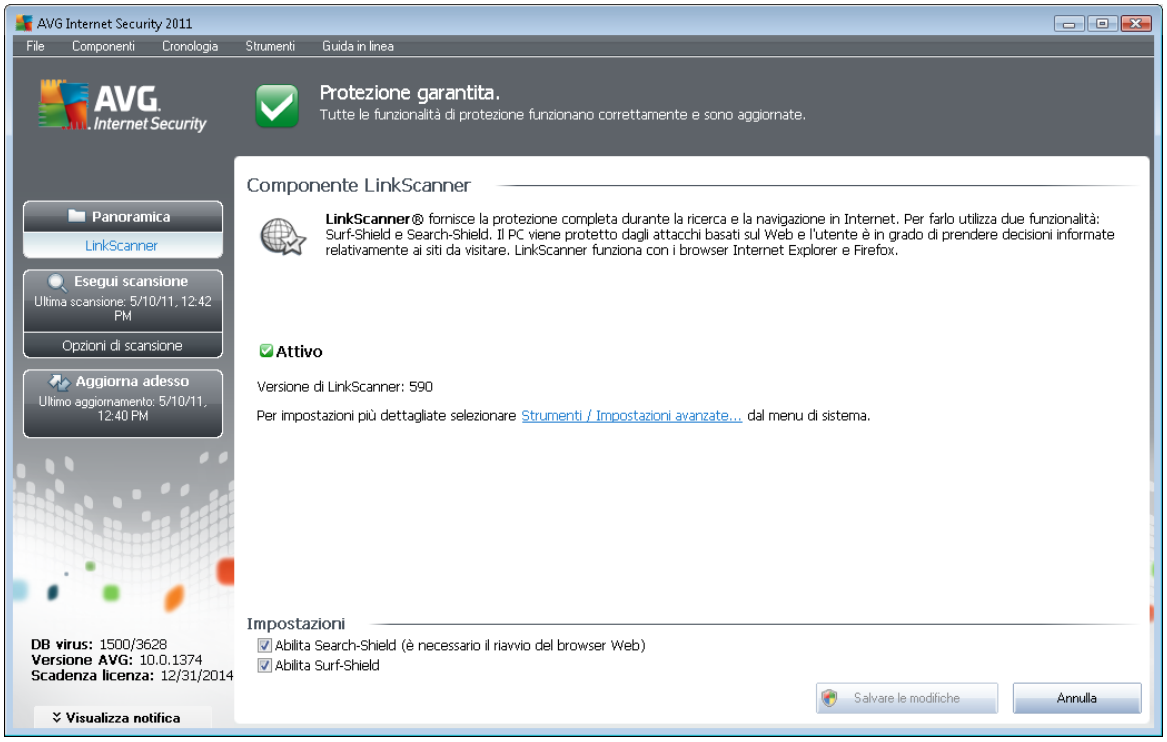
Quando si effettuano ricerche con Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg o SlashDot, tutti i risultati delle ricerche vengono controllati in base a questo elenco e viene visualizzata un'icona relativa al livello di sicurezza (*per Yahoo vengono visualizzate solo le icone relative ai siti Web dannosi*).

- ***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 ***Search-Shield*** (*ad esempio quando viene creato un nuovo sito dannoso o quando un sito in precedenza sicuro contiene ora un malware*), verrà rilevato e bloccato da ***Surf-Shield*** una volta che si tenterà di accedervi.

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

7.5.2. Interfaccia di Link Scanner

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



Impostazioni LinkScanner

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

- ***Abilita Search-Shield*** (*attivata per impostazione predefinita*): icone informative relative ai siti restituiti dalle ricerche eseguite in Google, Yahoo! JP, WebHledani, Yandex, Baidu,

Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg o SlashDot il cui contenuto è stato precedentemente controllato.

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

7.5.3. Search-Shield

Quando si eseguono ricerche in Internet con ***Search-Shield*** attivato, tutti i risultati di ricerca restituiti dai motori di ricerca più comuni (*Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg e SlashDot*) vengono controllati per rilevare l'eventuale presenza di 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 (*questa icona non verrà visualizzata per i risultati della ricerca Yahoo! JP*).

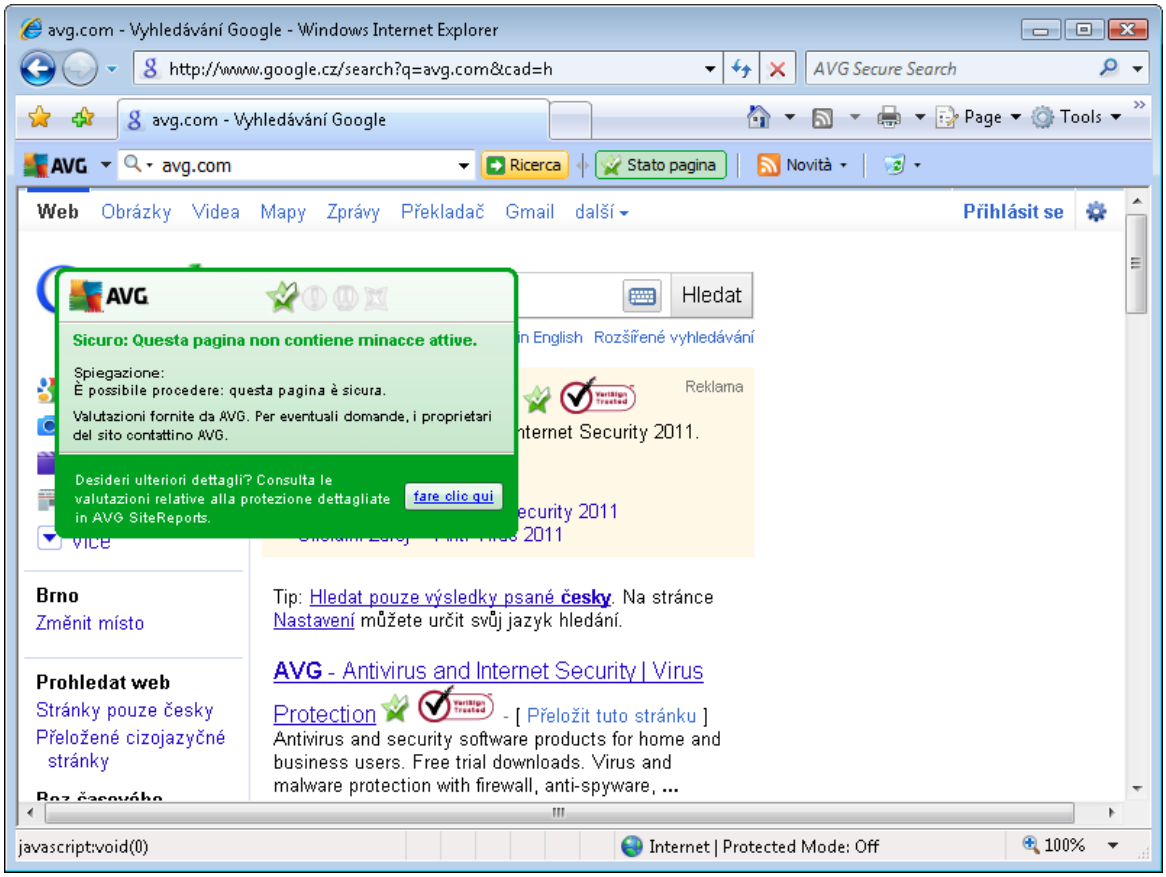
 La pagina alla quale fa riferimento il collegamento non contiene minacce ma risulta sospetta (*origine o motivazione dubbia, pertanto non è consigliabile utilizzarla per l'e-shopping e così via*).

 La pagina 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 sicurezza, non sarà consentito visitare questa pagina.

 La pagina collegata non è accessibile, pertanto non è stato possibile eseguirne la scansione.

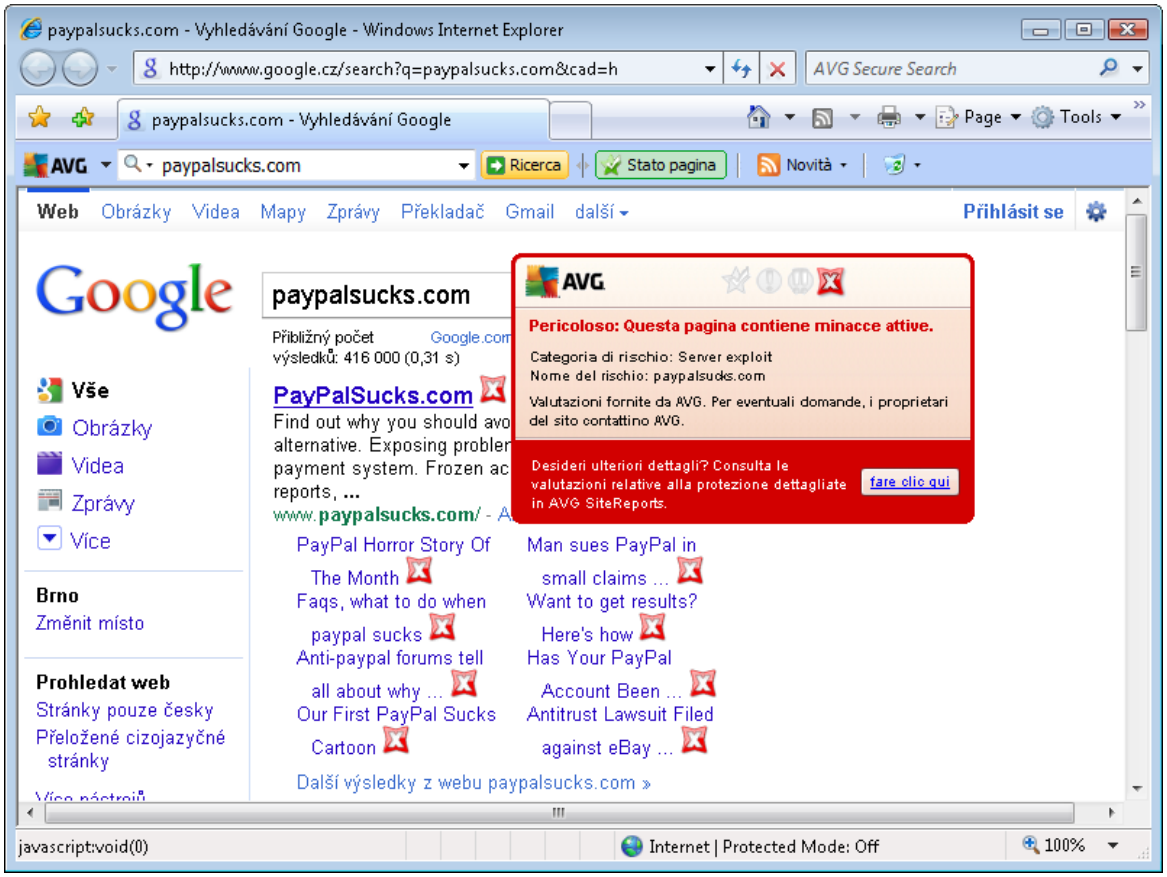
Se si passa il mouse sopra una singola icona che indica la valutazione verranno visualizzati i dettagli relativi al collegamento specifico. Le informazioni includono dettagli aggiuntivi relativi alla minaccia (*se presenti*):



7.5.4. 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.

7.6. Resident Shield

7.6.1. Principi di Resident Shield

Il componente ***Resident Shield*** fornisce al computer una protezione continua. Esegue la scansione di ogni singolo file che viene 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.

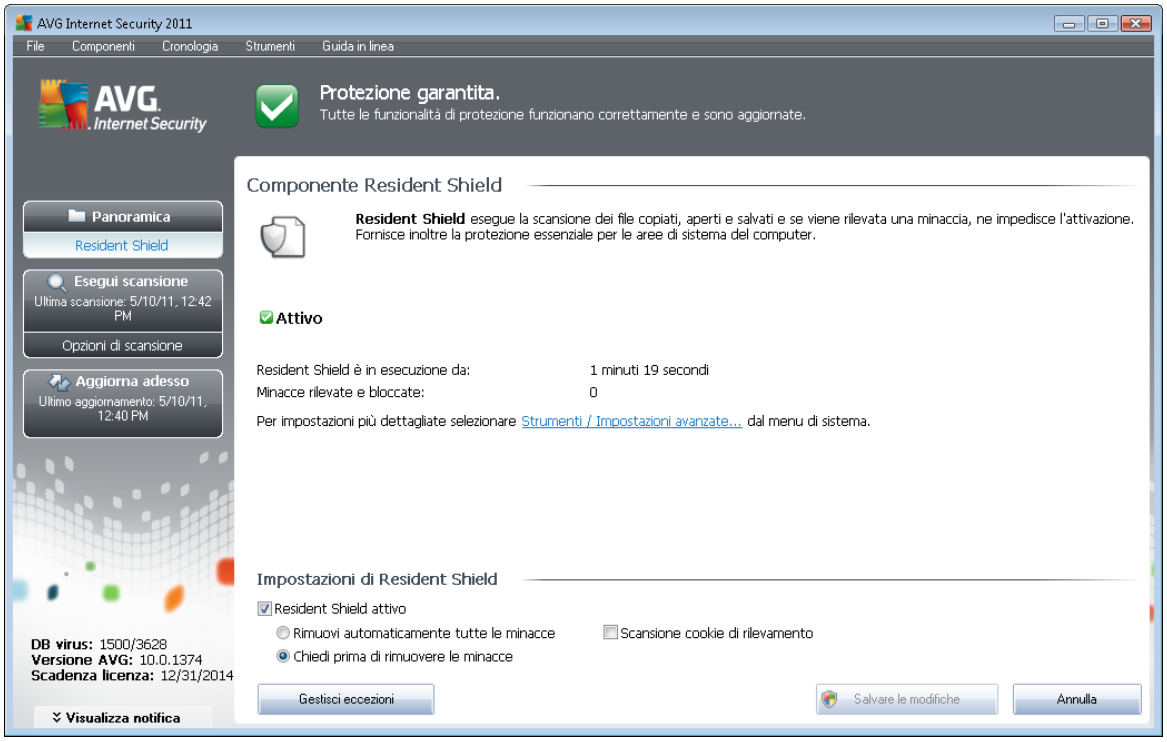
Funzionalità di ***Resident Shield***:

- Esegue la scansione alla ricerca di tipi specifici di possibili minacce
- Esegue la scansione di supporti rimovibili (*unità di memoria flash e così via*)
- Esegue la scansione di file con estensioni specifiche o senza alcuna estensione

- Consente eccezioni alla scansione; è possibile impostare alcuni file o cartelle che non devono mai essere sottoposti a scansione

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

7.6.2. Interfaccia di Resident Shield



Oltre a una panoramica della funzionalità di ***Resident Shield*** e alle informazioni sullo stato del componente, l'interfaccia di ***Resident Shield*** fornisce alcuni dati statistici:

- ***Resident Shield è in esecuzione da***: 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*)

Impostazioni Resident Shield

Nella parte inferiore della finestra di dialogo è presente la sezione ***Impostazioni Resident Shield*** in cui 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 comunque possibile scegliere di 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 questo 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 esista un motivo valido per farlo, si consiglia di non modificare la configurazione di AVG. Le eventuali modifiche alle impostazioni devono essere eseguite solo da utenti esperti. 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 - Elementi esclusi*** in cui è possibile definire le cartelle da escludere dalla scansione di ***Resident Shield***
- ***Salva modifiche***: selezionare questo pulsante per salvare e applicare le eventuali modifiche eseguite in questa finestra di dialogo
- ***Annulla***: selezionare questo pulsante per tornare all'***interfaccia utente di AVG*** predefinita (*panoramica dei componenti*).

7.6.3. 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:

In questa finestra di dialogo di avviso sono disponibili dati sul file rilevato e giudicato infetto (*Nome file*), il nome dell'infezione riconosciuta (*Nome minaccia*) e un collegamento all'***Enciclopedia dei virus*** che include informazioni dettagliate sull'infezione rilevata, se nota (*Ulteriori informazioni*).

Inoltre, è necessario decidere quale azione effettuare. Sono disponibili le seguenti opzioni:

Tenere presente che, in base a condizioni specifiche (tipo e posizione del file infetto), non tutte le opzioni sono sempre disponibili.

- ***Rimuovi minaccia come Power User***: selezionare la casella di controllo se si ritiene di non disporre di diritti sufficienti per rimuovere la minaccia come utente normale. I Power User dispongono di diritti di accesso estesi. Se la minaccia si trova in una determinata cartella di sistema, potrebbe essere necessario utilizzare questa casella di controllo per procedere alla rimozione.

- ***Correggi***: questo pulsante viene visualizzato solo se l'infezione rilevata può essere corretta. Quindi, il pulsante rimuove l'infezione dal file e ripristina il file allo stato originale. Se il file è un virus, utilizzare questa funzione per eliminarlo (*ossia spostarlo in **Quarantena virus***)

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

- ***Vai al file***: questa opzione reindirizza alla posizione esatta dell'oggetto sospetto (*apre una nuova finestra di Esplora risorse*)

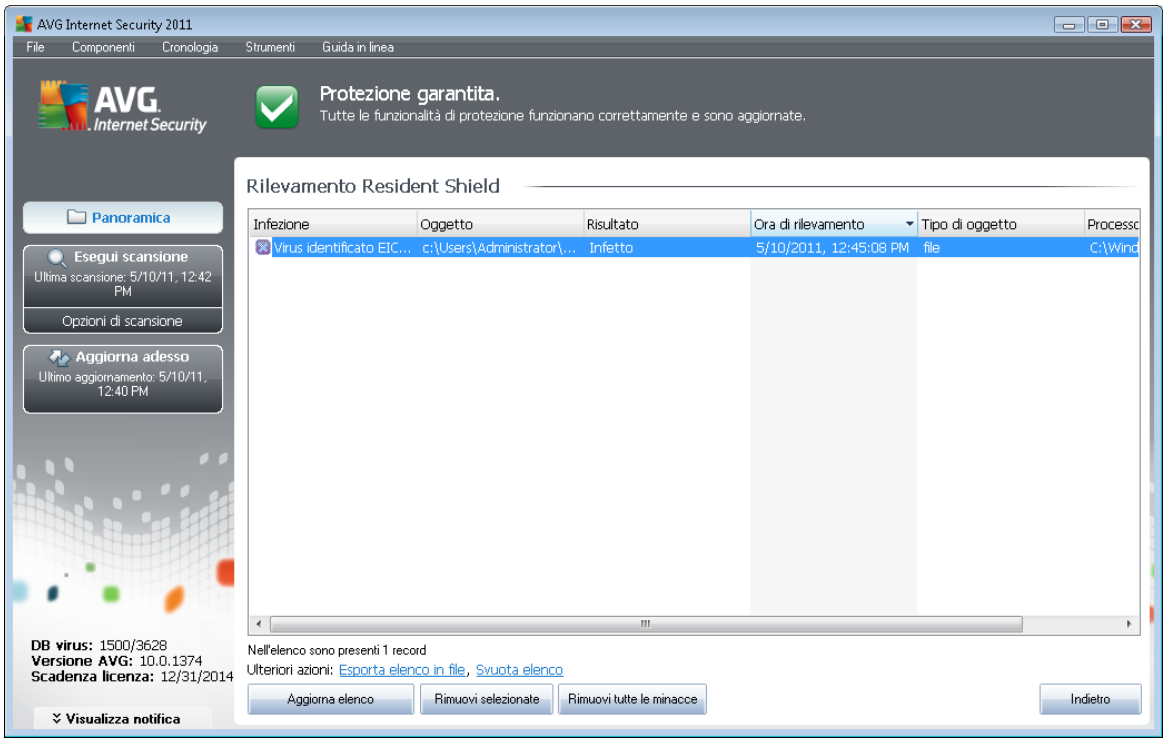
- ***Ignora***: si consiglia di NON utilizzare questa opzione a meno che non sussista un motivo valido per farlo

Nota: *potrebbe accadere che le dimensioni dell'oggetto rilevato superino il limite di spazio libero in Quarantena virus. In tal caso, verrà visualizzato un avviso relativo al problema quando si tenterà di spostare l'oggetto infetto in Quarantena virus. Tuttavia, le dimensioni di Quarantena virus possono essere modificate. Tali dimensioni vengono definite come percentuale regolabile delle dimensioni effettive del disco rigido. Per aumentare le dimensioni di Quarantena virus, nella finestra di dialogo Quarantena virus, accessibile tramite Impostazioni AVG avanzate, è disponibile l'opzione Limite*

dimensione per Quarantena virus.

Nella parte inferiore della finestra di dialogo è disponibile il collegamento ***Mostra dettagli***. Fare clic su di esso per aprire una finestra popup con informazioni dettagliate sul processo in esecuzione quando l'infezione è stata rilevata e i dati identificativi del processo.

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 / Rilevamento 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 (eventualmente 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*).

7.7. Family Safety

AVG Family Safety aiuta a proteggere i bambini da siti Web, ricerche in linea e contenuti multimediali inappropriati e fornisce rapporti relativi alle attività che essi svolgono in linea. È possibile impostare il livello di protezione che meglio si adatta a ciascun bambino e controllarne l'attività separatamente tramite dati di accesso univoci.

Il componente è attivo solo se il prodotto ***AVG Family Safety*** è installato nel computer. Se il prodotto ***AVG Family Safety*** non è installato, fare clic sulla relativa icona presente nell'interfaccia utente di **AVG Internet Security 2011** per accedere al sito Web del prodotto in cui sono disponibili tutte le informazioni necessarie.

7.8. AVG LiveKive

AVG LiveKive esegue il backup automatico di tutti i file, le foto e la musica in una posizione sicura, consentendo di condividerli con familiari e amici e di accedervi da qualsiasi dispositivo abilitato per il Web, inclusi dispositivi Android e iPhone.

Il componente è attivo solo se il prodotto ***AVG LiveKive*** è installato nel computer. Se il prodotto ***AVG LiveKive*** non è installato, fare clic sulla relativa icona presente nell'interfaccia utente di **AVG Internet Security 2011** per accedere al sito Web del prodotto in cui sono disponibili tutte le informazioni necessarie.

7.9. 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.

7.9.1. Principi di Scansione E-mail

Scansione e-mail personale 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 (*ma può essere utilizzato inoltre per esaminare i messaggi e-mail per i client e-mail supportati da AVG con un plug-in specifico, ossia Microsoft Outlook e The Bat*). Principalmente, è destinato all'uso con applicazioni e-mail quali 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).

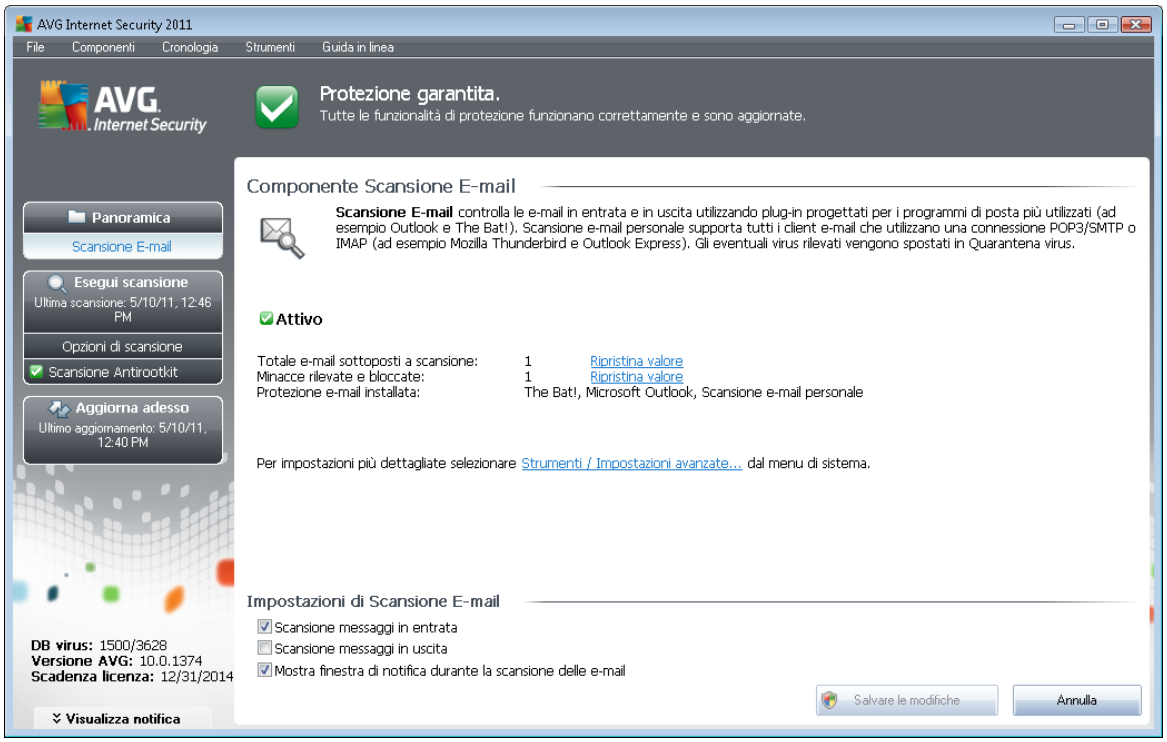
Scansione E-mail funziona come interfaccia tra il client e-mail e i server e-mail in Internet.

- ***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.*

7.9.2. Interfaccia di Scansione E-mail



Nella finestra di dialogo del componente Scansione E-mail sono contenuti un breve testo che descrive la funzionalità del componente, le informazioni sullo stato corrente 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

Impostazioni di Scansione E-mail

Nella parte inferiore della finestra di dialogo è contenuta una sezione relativa alle ***impostazioni di Scansione E-mail*** che consente di modificare alcune funzionalità di base 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 finestra di notifica durante la scansione delle 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 delle 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 ai soli 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. Le eventuali modifiche alle impostazioni devono essere eseguite solo da utenti esperti. 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.*

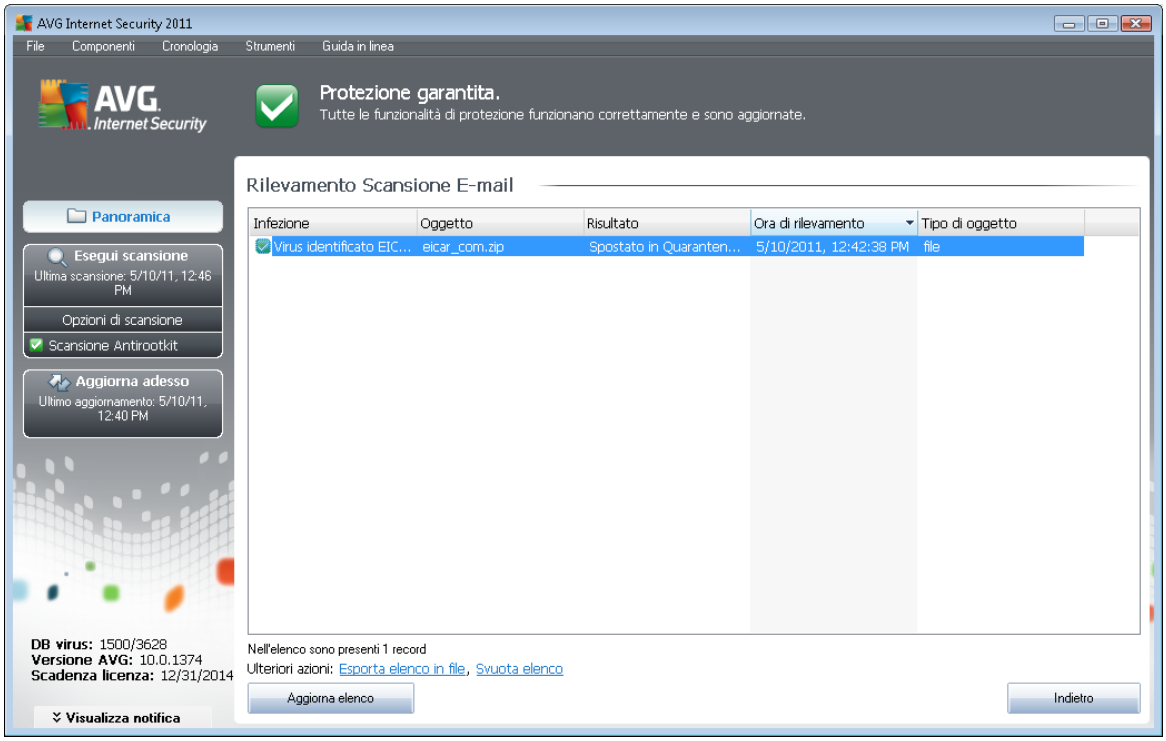
Pulsanti di controllo

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

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

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

7.9.3. 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 (eventualmente 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***: torna alla finestra di dialogo visualizzata in precedenza

7.10. Gestore aggiornamenti

7.10.1. Principi di Gestore aggiornamenti

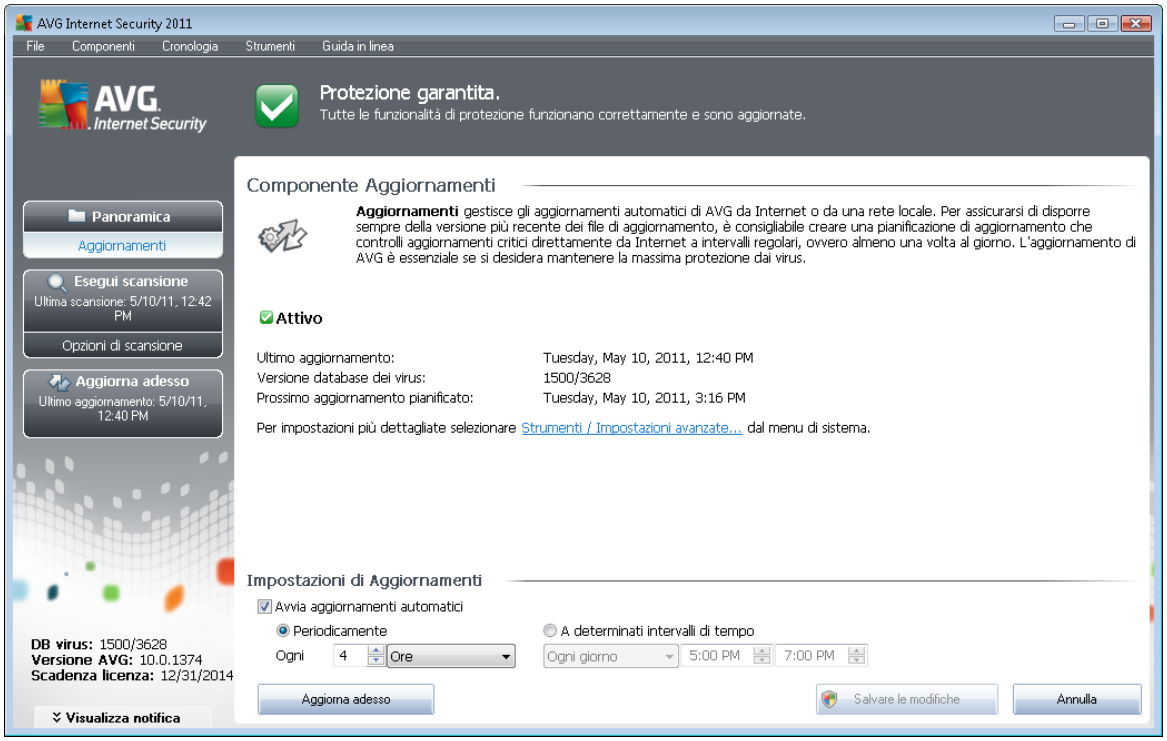
Nessun software per la protezione è in grado di garantire una vera protezione dai vari tipi di minacce se non viene aggiornato con regolarità. Gli autori dei virus ricercano di continuo nuove imperfezioni da sfruttare sia nei sistemi operativi che nel software. Tutti i giorni si presentano nuovi virus,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

È fondamentale aggiornare AVG con regolarità.

Gestore aggiornamenti consente di controllare la regolarità degli aggiornamenti. All'interno di questo componente è possibile pianificare download automatici dei file di aggiornamento da Internet o dalla rete locale. Gli aggiornamenti delle definizione dei virus principali dovrebbero essere eseguiti ogni giorno, se possibile. Gli aggiornamenti del programma meno urgenti possono essere eseguiti settimanalmente.

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

7.10.2. Interfaccia di Gestore aggiornamenti



L'interfaccia del componente ***Gestore aggiornamenti*** fornisce informazioni sulla funzionalità del componente e sul relativo stato e i relativi dati statistici:

- ***Ultimo aggiornamento***: specifica la data e l'ora dell'aggiornamento del database più recente
- ***Versione del database***: indica il numero della versione del database dei virus installato. Il numero viene incrementato dopo ogni aggiornamento del database dei virus
- ***Prossimo aggiornamento pianificato***: specifica la data e l'ora del successivo aggiornamento del database

Impostazioni di Gestore aggiornamenti

Nella parte inferiore della finestra di dialogo è contenuta la sezione delle ***impostazioni di 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
- ***A determinati intervalli di tempo***: definisce l'ora esatta in cui l'aggiornamento deve essere avviato

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 esista un motivo valido per farlo, si consiglia di non modificare la configurazione di AVG. Le eventuali modifiche alle impostazioni devono essere eseguite solo da utenti esperti. 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.*

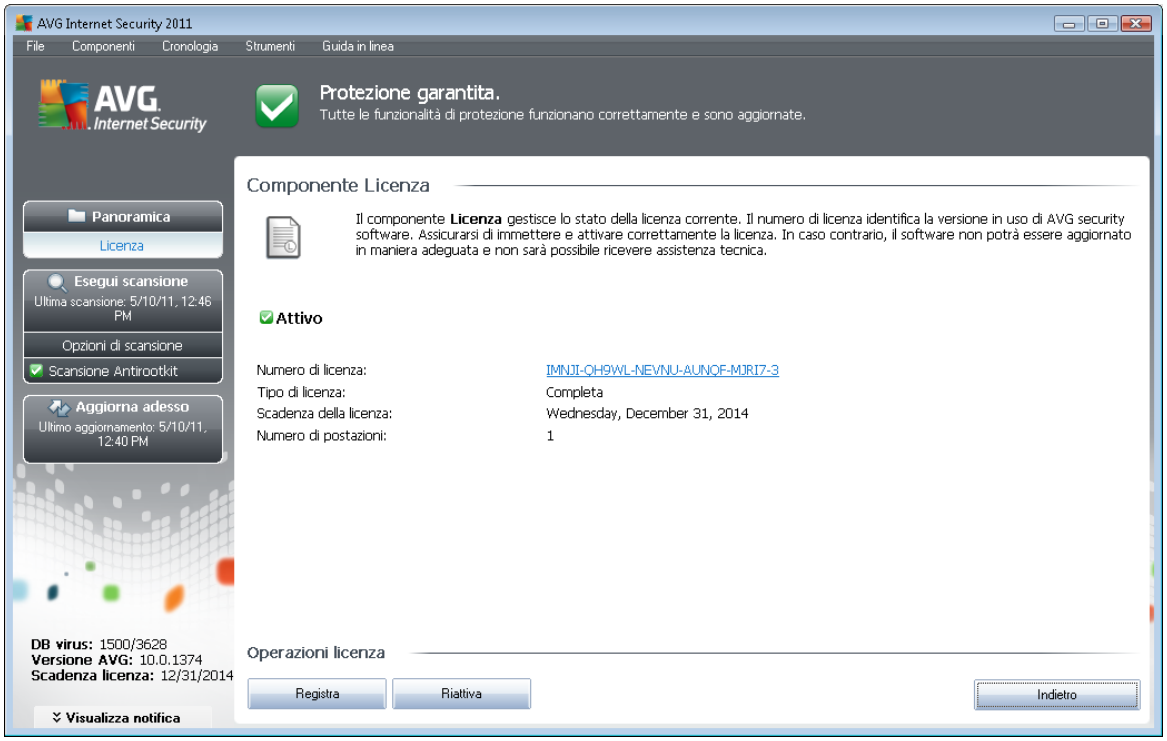
Pulsanti di controllo

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

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

7.11. Licenza



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

- ***Numero di licenza***: fornisce il numero di licenza in forma abbreviata (*per motivi di sicurezza gli ultimi quattro simboli vengono omessi*). Quando si immette il numero di licenza, è necessario essere precisi e digitarlo esattamente come viene indicato. Si consiglia pertanto 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 Internet Security 2011** dopo questa data, sarà necessario rinnovare la licenza. Il rinnovo della licenza può essere effettuato in linea sul sito Web di AVG.

- ***Numero di postazioni***: indica il numero di workstation nelle quali è possibile installare **AVG Internet Security 2011**.

Pulsanti di controllo

- ***Registra***: consente di aprire la pagina relativa alla registrazione del sito Web di AVG (http://

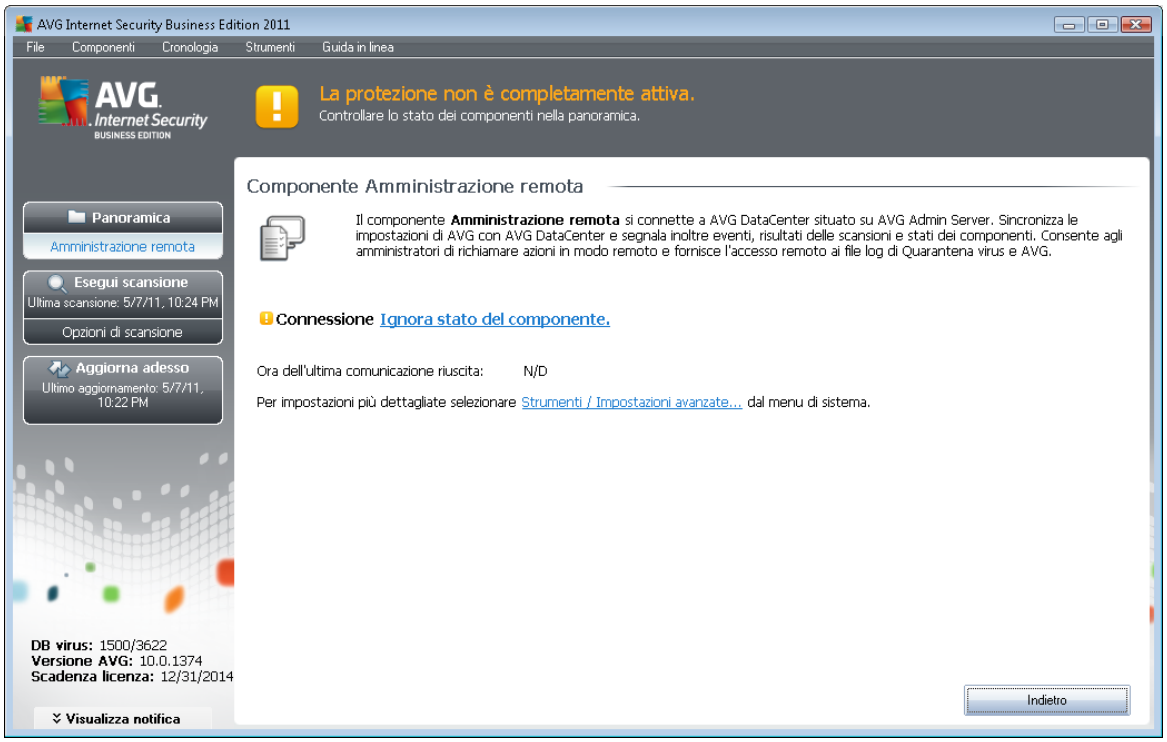
www.avg.com/). Immettere i dati di registrazione; solo i clienti che registrano il prodotto AVG possono ricevere assistenza tecnica gratuita.

- ***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 Internet Security 2011*, **i pulsanti appaiono come** *Acquista ora* **e** *Attiva, consentendo di acquistare subito la versione completa del programma. Per* **AVG Internet Security 2011** *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*).

7.12. Amministrazione remota



Il componente ***Amministrazione remota*** viene visualizzato nell'interfaccia utente di **AVG Internet Security 2011** solo se è stata installata la versione Business Edition del prodotto (*vedere il componente* ***Licenza***). Nella finestra di dialogo ***Amministrazione remota*** viene indicato se il componente è attivo e connesso al server. Tutte le impostazioni del componente ***Amministrazione remota*** vengono regolate in ***Impostazioni avanzate / Amministrazione remota***.

Per la descrizione dettagliata di opzioni e funzionalità del componente all'interno del sistema AVG Amministrazione remota, consultare la documentazione specifica dedicata esclusivamente a questo

argomento. Questa documentazione è disponibile per il download sul sito Web di AVG (www.avg.com), nella sezione ***Centro di assistenza / Download / Documentazione***.

Pulsanti di controllo

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

7.13. Online Shield

7.13.1. Principi di Online Shield

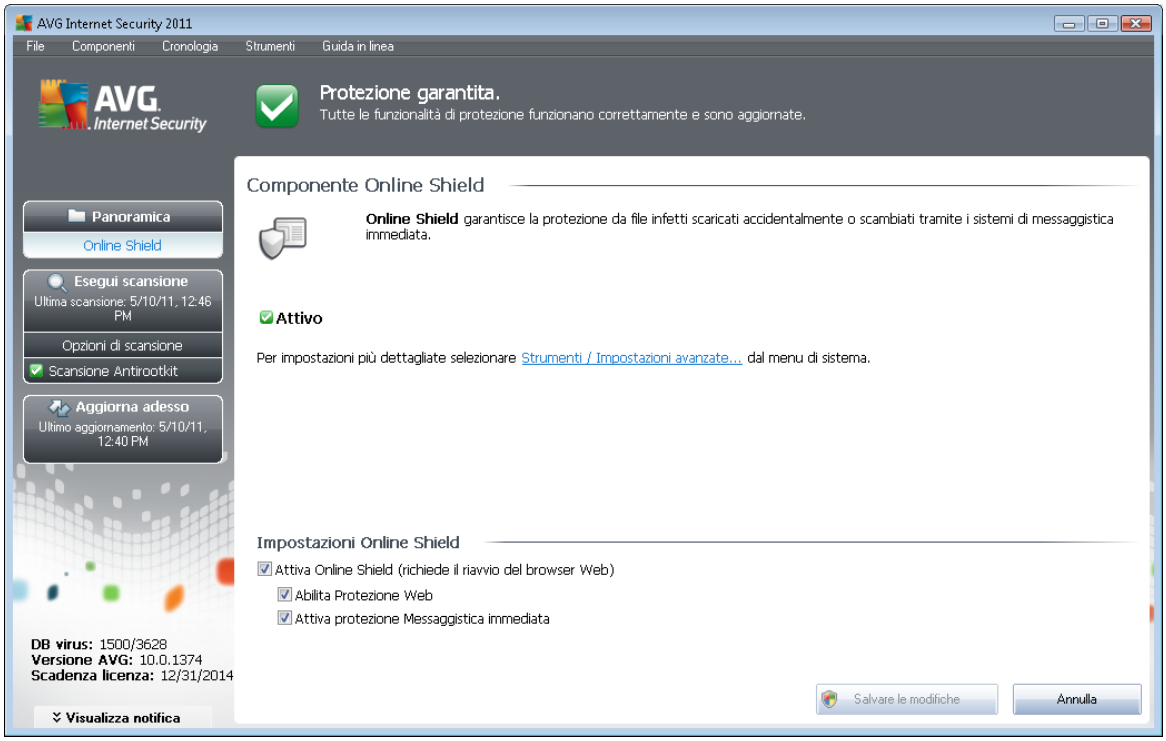
Online Shield è un tipo di protezione permanente in tempo reale; esegue la scansione del contenuto delle pagine Web visitate (*e dei possibili file in esse contenuti*) persino prima che vengano visualizzate nel browser Web o scaricate nel computer.

Online Shield rileva se la pagina che sta per essere aperta contiene javascript dannosi e ne impedisce la visualizzazione. 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.*

7.13.2. Interfaccia di Online Shield

L'interfaccia del componente ***Online Shield*** descrive il comportamento di questo tipo di protezione. Sono inoltre disponibili informazioni sullo stato corrente del componente. Nella parte inferiore della finestra di dialogo sono presenti le opzioni di modifica di base della funzionalità del componente:



Impostazioni di Online Shield

Innanzitutto, è disponibile l'opzione per attivare/disattivare immediatamente ***Online Shield*** selezionando la voce ***Abilita Online Shield***. Questa opzione è attivata 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, due ulteriori opzioni di configurazione vengono attivate:

- ***Abilita protezione Web***: questa opzione conferma l'esecuzione della scansione del contenuto dei siti Web da parte del componente ***Online Shield***.
- ***Attiva protezione Messaggistica immediata***: selezionare questa voce se si desidera che ***Online Shield*** verifichi che le comunicazioni di messaggistica immediata (*ad esempio ICQ, MSN Messenger e così via*) sono prive di virus.

Nota: il *fornitore del software ha impostato tutti i componenti AVG per fornire prestazioni ottimali. A meno che non esista un motivo valido per farlo, si consiglia di non modificare la configurazione di AVG. Le eventuali modifiche alle impostazioni devono essere eseguite solo da utenti esperti. 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***: selezionare questo pulsante per salvare e applicare le eventuali modifiche eseguite in questa finestra di dialogo
- ***Annulla***: selezionare il pulsante per tornare all'***interfaccia utente AVG predefinita*** (*panoramica dei componenti*)

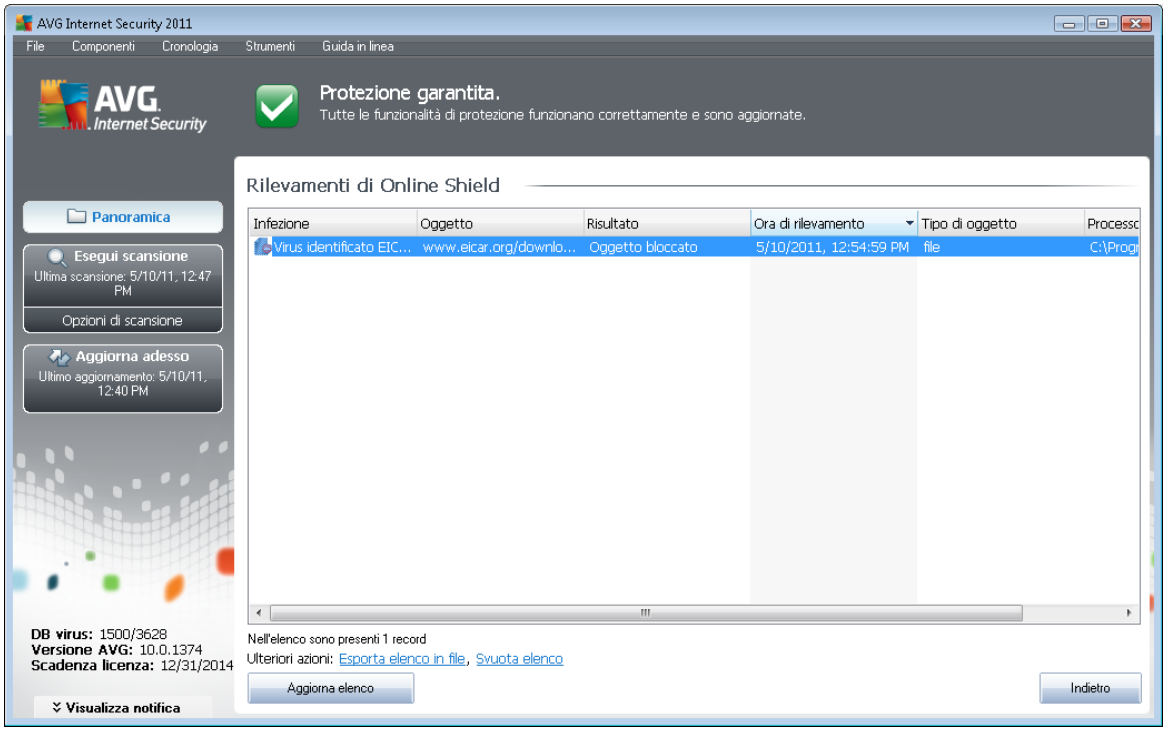
7.13.3. Rilevamenti di Online Shield

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:

In questa finestra di dialogo di avviso sono disponibili dati sul file rilevato e giudicato infetto (*Nome file*), il nome dell'infezione riconosciuta (*Nome minaccia*) e un collegamento all'***Enciclopedia dei virus*** che include informazioni dettagliate sull'infezione rilevata (*se nota*). La finestra di dialogo fornisce i seguenti pulsanti:

- ***Mostra dettagli***: fare clic sul pulsante ***Mostra dettagli*** per aprire una finestra popup con informazioni sul processo in esecuzione quando l'infezione è stata rilevata e i dati identificativi del processo.
- ***Chiudi***: fare clic sul pulsante per chiudere la finestra di dialogo di avviso.

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 *eventualmente 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*).

7.14. Anti-Rootkit

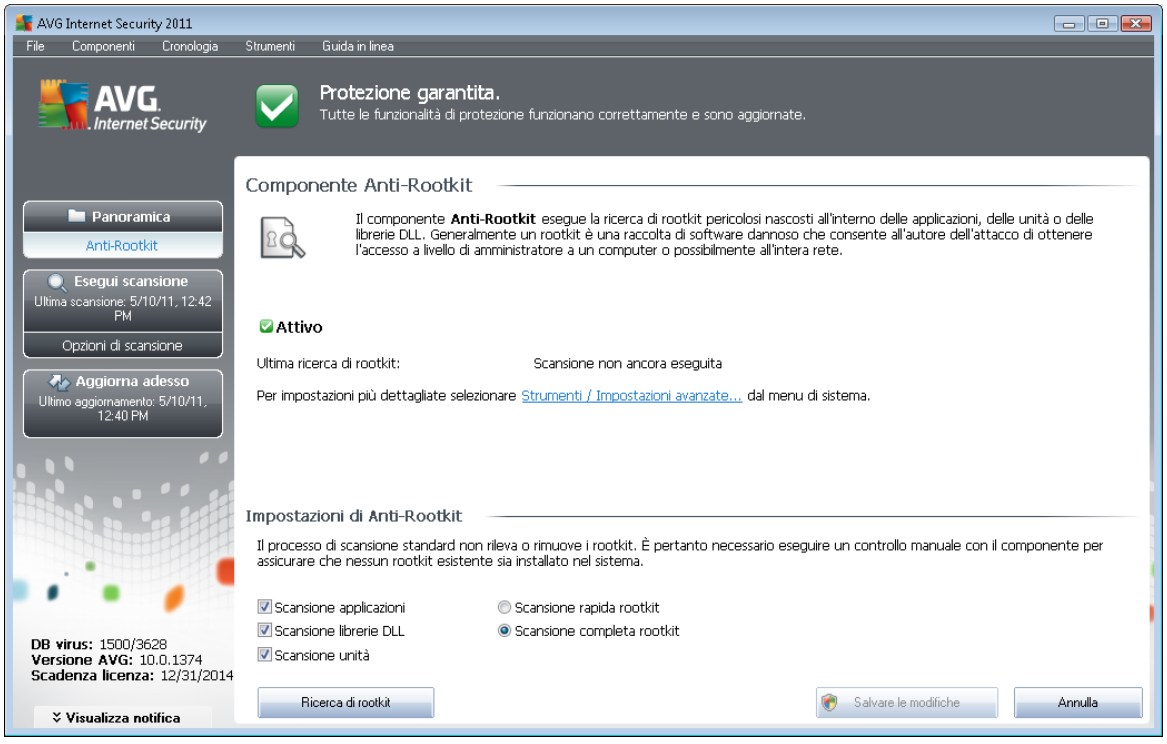
Un rootkit è un programma progettato per assumere il controllo di base di un sistema senza autorizzazione da parte dei proprietari e dei gestori legittimi del sistema. L'accesso all'hardware è raramente necessario poiché un rootkit dovrà assumere il controllo del sistema operativo in esecuzione sull'hardware. 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 di poter essere eseguiti in tutta sicurezza sui sistemi. Le tecniche utilizzate a questo scopo possono includere l'occultamento di processi in esecuzione dai programmi di monitoraggio oppure di file o dati di sistema dal sistema operativo.

7.14.1. Principi dell'Anti-Rootkit

AVG Anti-Rootkit è uno strumento specializzato per il rilevamento e la rimozione efficace di rootkit dannosi, ossia programmi e tecnologie che possono camuffare la presenza di software dannoso sul computer. ***AVG Anti-Rootkit*** è in grado di rilevare i rootkit in base a un gruppo di regole predefinito. Tenere presente che vengono rilevati tutti i rootkit (*non solo quelli infetti*). Se ***AVG Anti-Rootkit*** rileva un rootkit, ciò non significa necessariamente che il rootkit sia infetto. Talvolta i rootkit vengono utilizzati come driver o fanno parte di applicazioni regolari.

7.14.2. Interfaccia dell'Anti-Rootkit



L'interfaccia utente di ***Anti-Rootkit*** fornisce una breve descrizione della funzionalità del componente, informa sullo stato corrente del componente e indica l'ultimo avvio del controllo ***Anti-Rootkit*** (***Ultima ricerca di rootkit***). La finestra di dialogo ***Anti-Rootkit*** fornisce inoltre il collegamento a ***Strumenti/ Impostazioni avanzate***. Utilizzare il collegamento per passare all'ambiente di configurazione avanzata del componente ***Anti-Rootkit***.

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. Le eventuali modifiche alle impostazioni devono essere eseguite solo da utenti esperti.*

Impostazioni di Anti-Rootkit

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

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

Quindi, è possibile selezionare la modalità di scansione anti-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*)

Pulsanti di controllo

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

7.15. System Tools

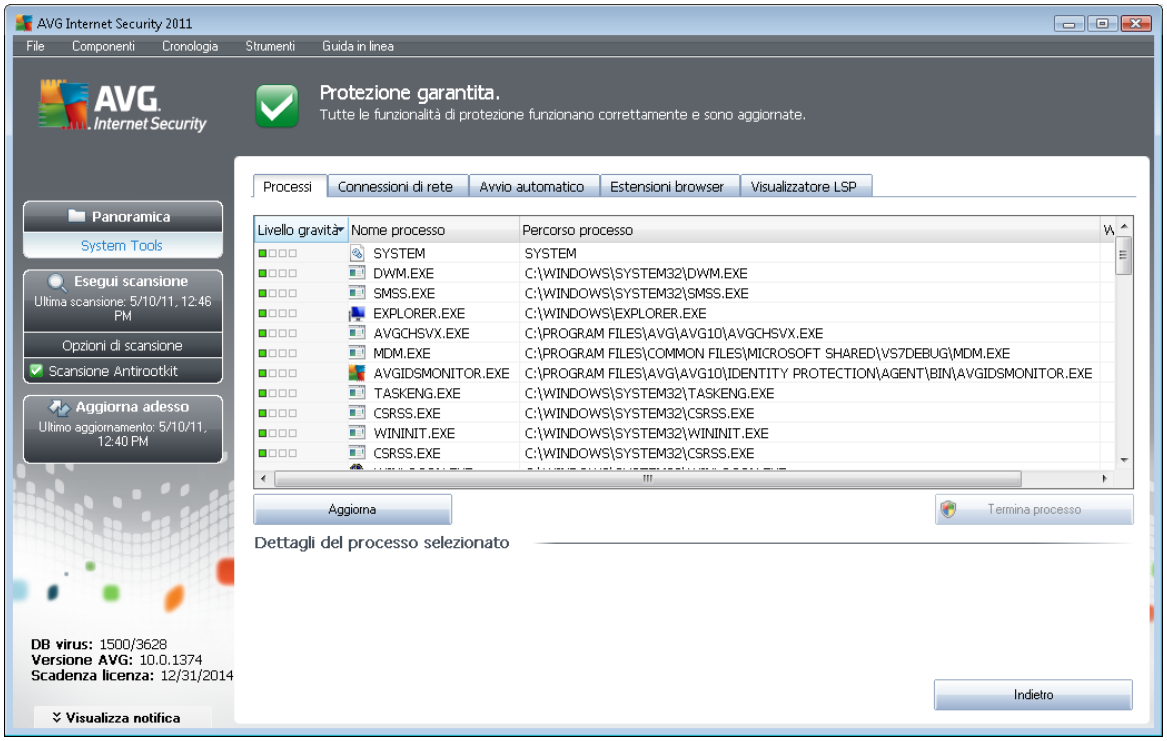
System Tools si riferisce a strumenti che offrono un riepilogo dettagliato dell'ambiente **AVG Internet Security 2011** e del sistema operativo. Il componente visualizza una panoramica degli elementi seguenti:

- Processi: elenco dei processi (*ossia le applicazioni in esecuzione*) attivi nel computer
- Connessioni di rete: elenco delle connessioni attive
- Avvio automatico: elenco di tutte le applicazioni eseguite durante l'avvio del sistema Windows

- Estensioni browser: elenco dei plug-in (*ossia le applicazioni*) installate nel browser Internet
- Visualizzatore LSP: elenco dei Layered Service Provider (*LSP*)

È anche possibile modificare panoramiche specifiche, ma questa operazione è consigliabile solo a utenti molto esperti.

7.15.1. Processi



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

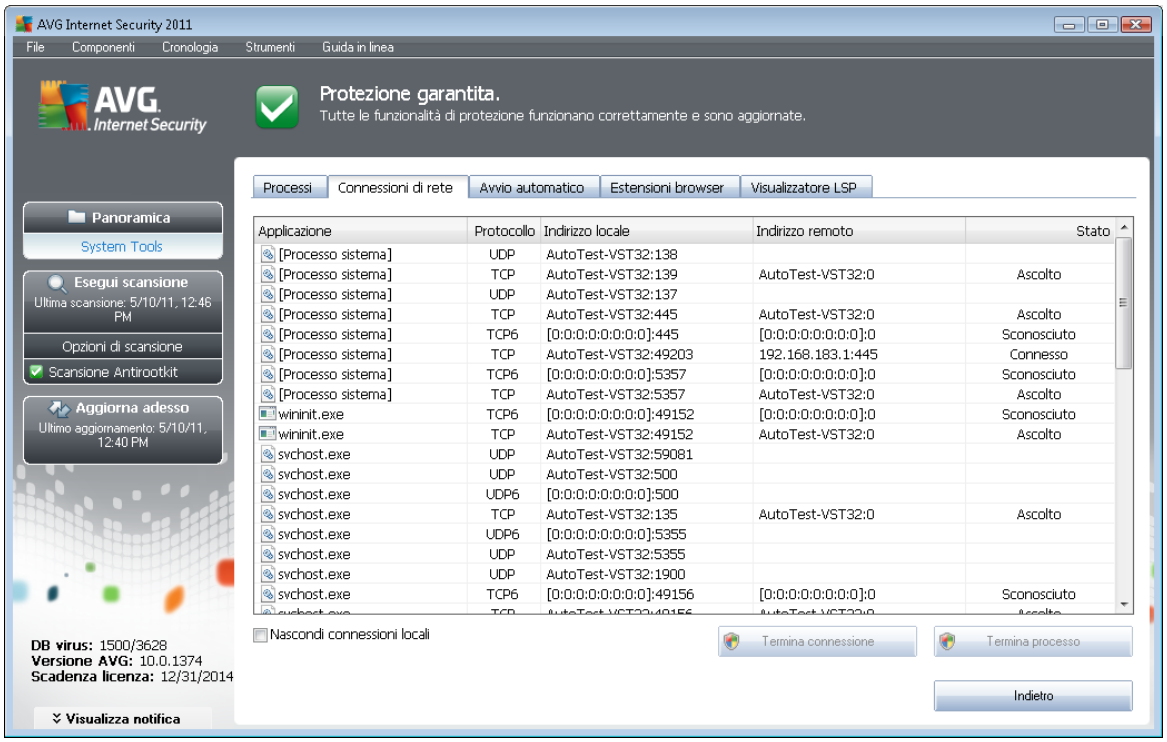
- ***Livello gravità***: identificazione grafica della gravità di un determinato processo valutata su una scala di quattro livelli dal meno grave (■□□□) al più grave (■■■■)
- ***Nome processo***: nome del processo in esecuzione.
- ***Percorso processo***: percorso fisico del processo in esecuzione
- ***Finestra***: se applicabile, indica il nome della finestra dell'applicazione in Windows
- ***PID***: il numero di identificazione del processo è un numero interno di Windows univoco

Pulsanti di controllo

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

- ***Aggiorna***: aggiorna l'elenco dei processi in base allo stato corrente
- ***Termina processo***: è possibile selezionare una o più applicazioni, quindi terminarle facendo clic su questo pulsante. ***Si consiglia di non terminare alcuna applicazione se non si è assolutamente sicuri che rappresenti una reale minaccia.***
- ***Indietro***: consente di tornare all'Interfaccia utente di AVG predefinita (*panoramica dei componenti*)

7.15.2. Connessioni di rete



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

- ***Applicazione***: nome dell'applicazione correlata alla connessione (*con l'eccezione di Windows 2000 in cui le informazioni non sono disponibili*)
- ***Protocollo***: il tipo di protocollo di trasmissione utilizzato per la connessione:
  - TCP: protocollo utilizzato assieme al protocollo IP (Internet Protocol) per trasmettere le informazioni in Internet
  - UDP: protocollo alternativo al protocollo TCP.
- ***Indirizzo locale***: indirizzo IP del computer locale e numero della porta utilizzata.
- ***Indirizzo remoto***: indirizzo IP del computer remoto e numero della porta a cui viene

eseguita la connessione. Se possibile, verrà cercato anche il nome host del computer remoto.

- ***Stato***: indica lo stato corrente più probabile (*Connesso, Il server deve essere chiuso, Ascolto, Chiusura attiva terminata, Chiusura passiva, Chiusura attiva*).

Per visualizzare solo le connessioni esterne, selezionare la casella di controllo ***Nascondi connessioni locali*** nella sezione inferiore della finestra di dialogo sotto l'elenco.

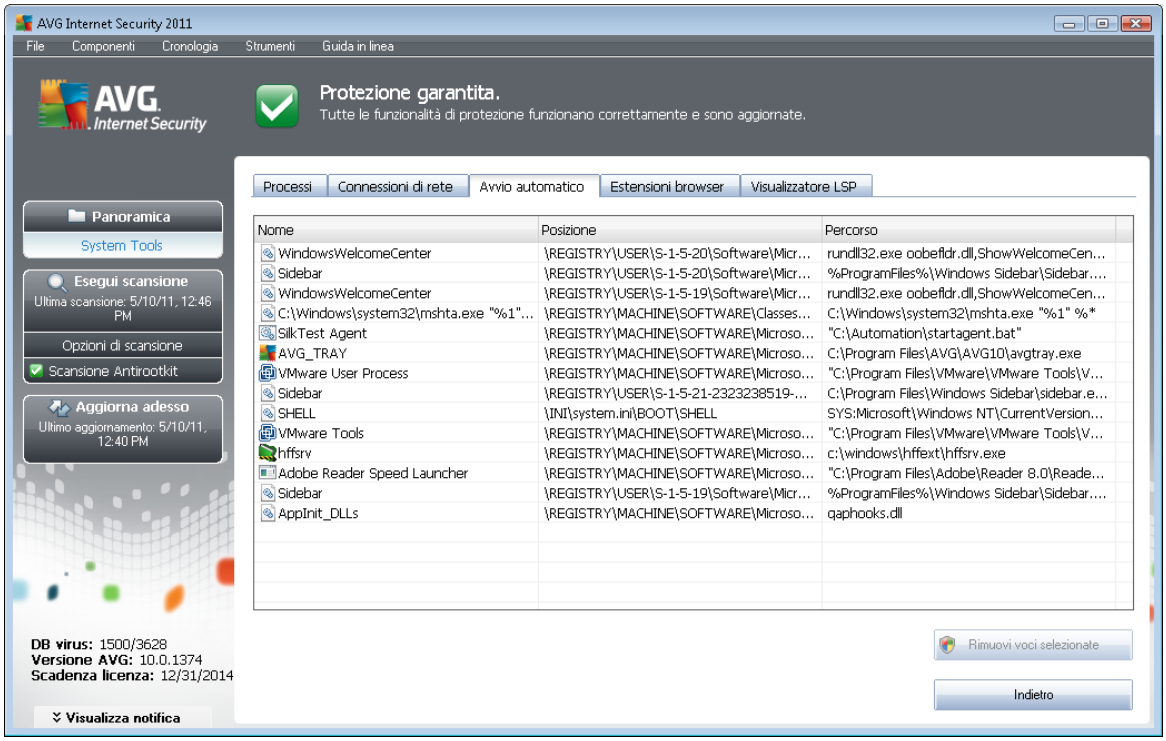
Pulsanti di controllo

Sono disponibili i seguenti pulsanti di controllo:

- ***Termina connessione***: consente di chiudere una o più connessioni selezionate nell'elenco.
- ***Termina processo***: consente di chiudere una o più applicazioni correlate alle connessioni selezionate nell'elenco
- ***Indietro***: consente di tornare all'*interfaccia utente di AVG* predefinita (panoramica dei componenti).

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

7.15.3. Avvio automatico

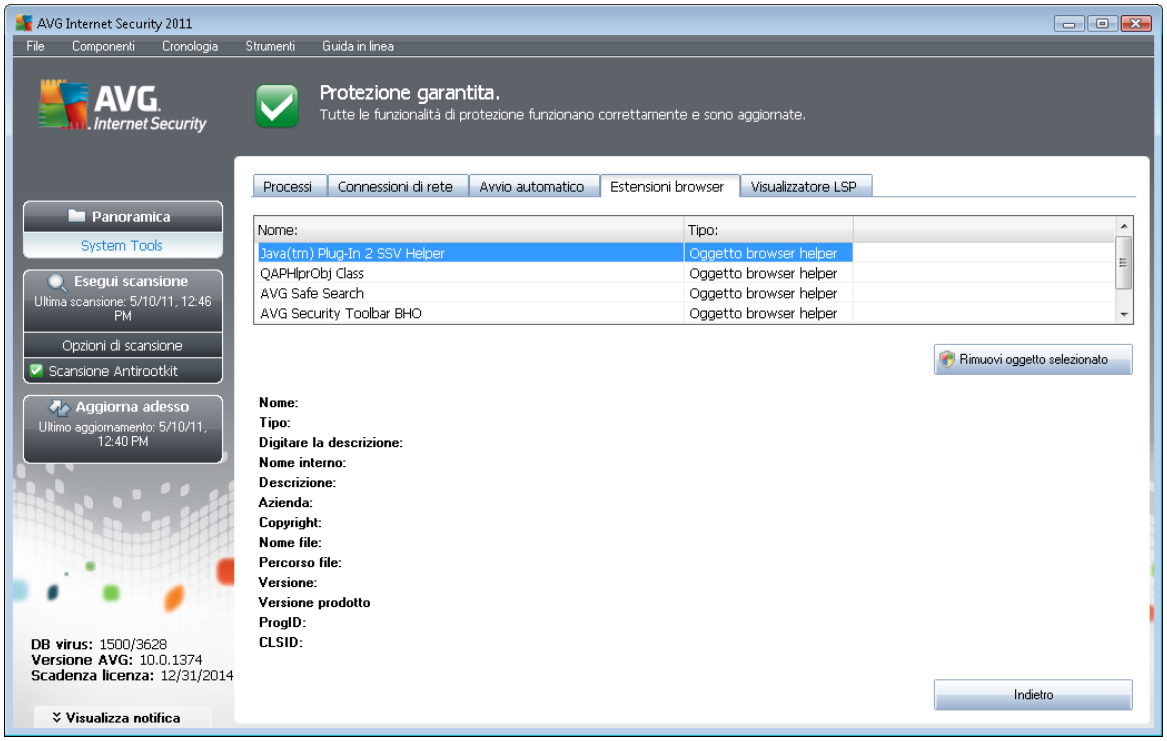


Nella finestra di dialogo ***Avvio automatico*** è visualizzato un elenco di tutte le applicazioni eseguite durante l'avvio del sistema Windows. Molto spesso diverse applicazioni malware si aggiungono automaticamente alle voci del Registro di sistema di avvio.

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

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

7.15.4. Estensioni browser



Nella finestra di dialogo ***Estensioni browser*** è presente l'elenco dei plug-in (*applicazioni*) installati nel browser Web. L'elenco può includere normali plug-in delle applicazioni, ma anche potenziali programmi malware. Fare clic su un oggetto dell'elenco per ottenere informazioni dettagliate sul plug-in selezionato, che verranno visualizzate nella sezione inferiore della finestra di dialogo.

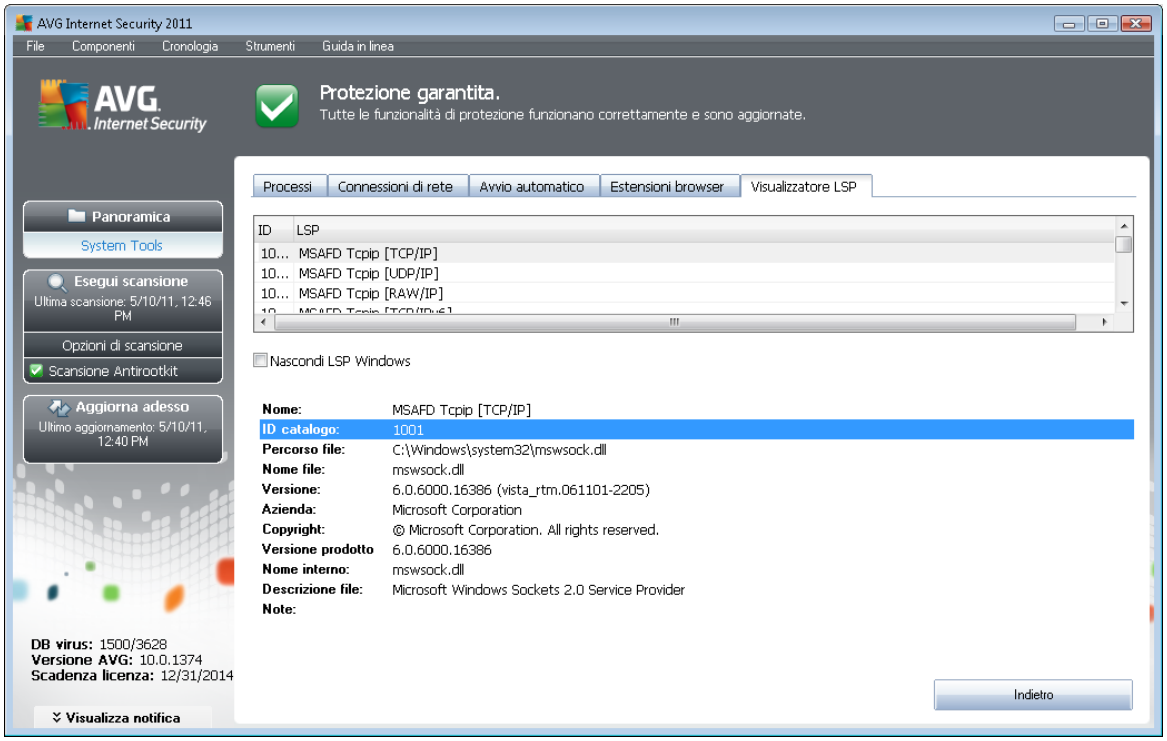
Pulsanti di controllo

I pulsanti di controllo disponibili nella scheda ***Estensioni browser*** sono:

- ***Rimuovi oggetto selezionato***: rimuove il plug-in evidenziato nell'elenco. ***Se non si è assolutamente sicuri che un plug-in rappresenti una reale minaccia, si consiglia di non eliminarlo dall'elenco.***

- ***Indietro***: consente di tornare all'***Interfaccia utente di AVG*** predefinita (panoramica dei componenti)

7.15.5. Visualizzatore LSP



Nella finestra di dialogo ***Visualizzatore LSP*** viene visualizzato un elenco di LSP (Layered Service Provider).

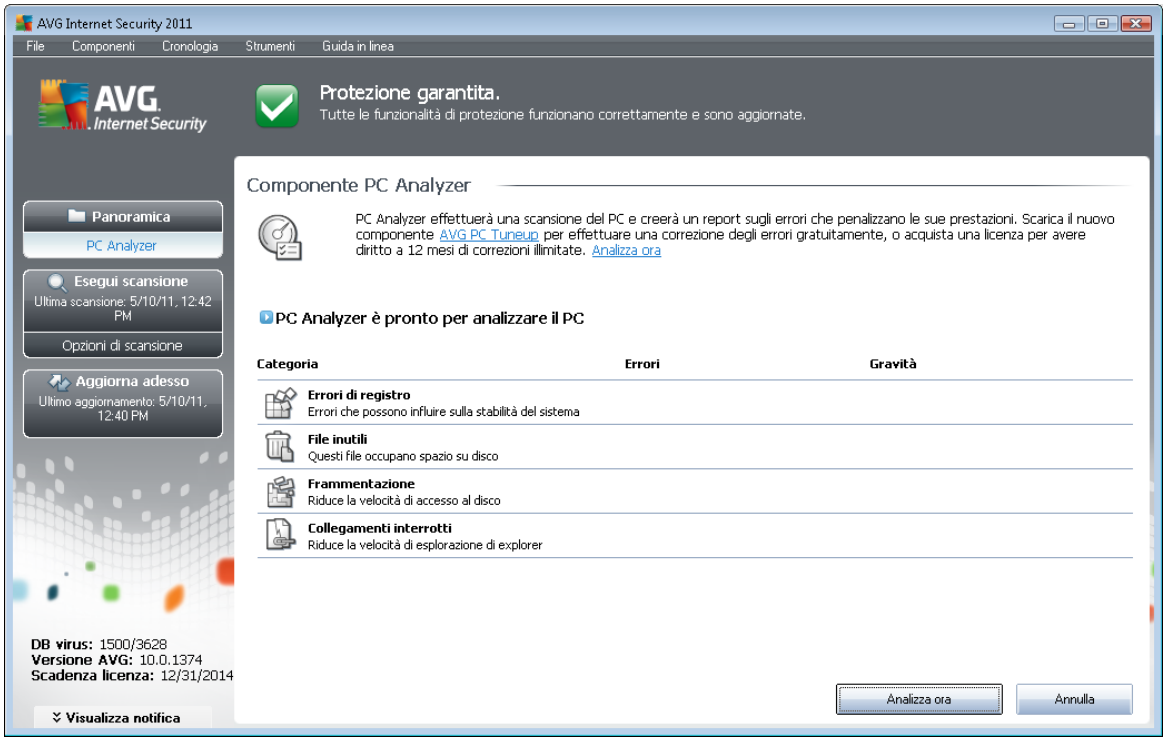
Un ***LSP*** è un driver di sistema collegato ai servizi di rete del sistema operativo Windows. È in grado di accedere a tutti i dati in entrata e in uscita dal computer e di modificare tali dati. Alcuni LSP sono necessari per consentire a Windows di connettere il computer dell'utente ad altri computer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

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

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

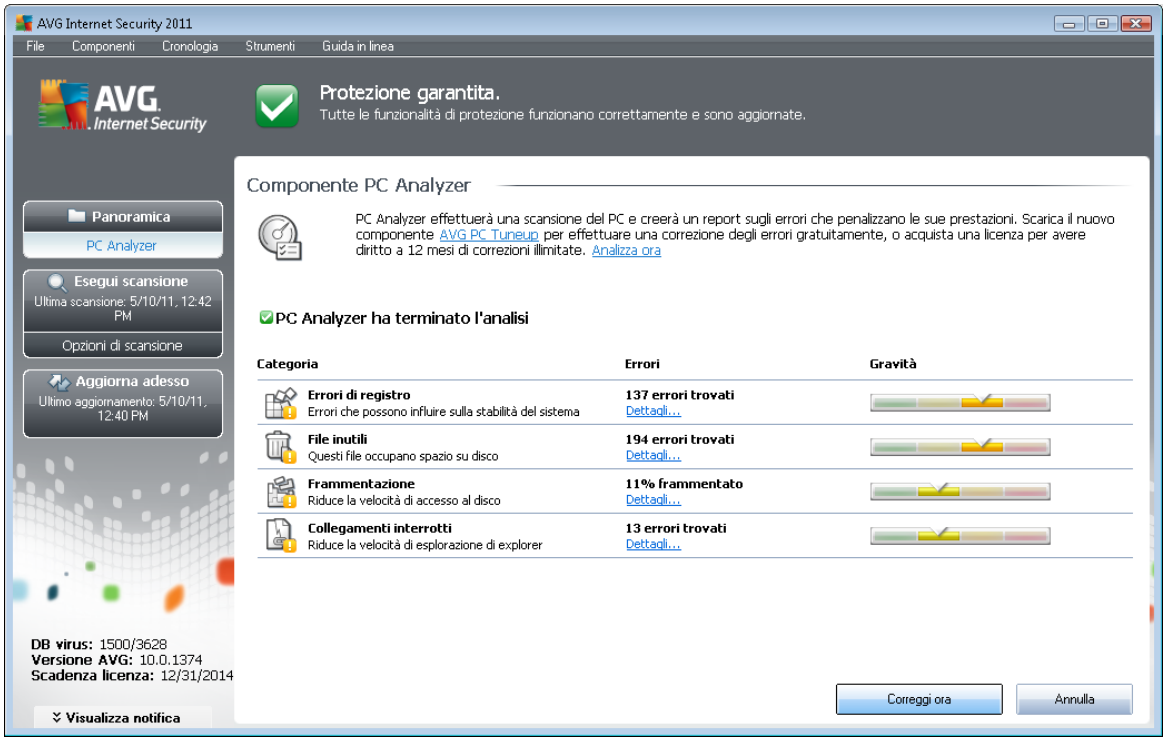
7.16. PC Analyzer

Il componente ***PC Analyzer*** esamina il computer per rilevare problemi di sistema e fornisce una panoramica dettagliata di ciò che potrebbe ridurre le prestazioni globali del computer. Nell'interfaccia utente del componente è possibile visualizzare un grafico diviso in quattro righe relative alle seguenti categorie: errori di registro, file inutili, frammentazione e collegamenti interrotti:



- ***Errori di registro*** fornisce il numero di errori nel Registro di Windows. Poiché la correzione del registro richiede particolare esperienza, non è consigliabile correggere il registro personalmente.
- ***File inutili*** fornisce il numero di file che sono molto probabilmente superflui. In genere si tratta di file temporanei di vario tipo e dei file presenti nel Cestino.
- ***Frammentazione*** consente di calcolare la percentuale di disco rigido frammentata, ovvero utilizzata per molto tempo per cui al momento i file si trovano sparsi in diverse parti del disco fisico. È possibile utilizzare strumenti per la deframmentazione per correggere questa situazione.
- ***Collegamenti interrotti*** indica all'utente collegamenti non più funzionanti, che conducono a posizioni inesistenti e così via.

Per avviare l'analisi del sistema, selezionare il pulsante ***Analizza ora***. Sarà quindi possibile visualizzare l'avanzamento dell'analisi e i relativi risultati direttamente nel grafico:



La panoramica dei risultati fornisce il numero di problemi del sistema rilevati (***Errori***) divisi in base alle categorie controllate. I risultati dell'analisi verranno inoltre visualizzati graficamente nella colonna ***Gravità***.

Pulsanti di controllo

- ***Analizza ora*** (*visualizzato prima dell'avvio dell'analisi*): selezionare questo pulsante per avviare immediatamente l'analisi del computer
- ***Correggi ora*** (*visualizzato al completamento dell'analisi*): selezionare il pulsante per visualizzare il sito Web di AVG (http://www.avg.com/) alla pagina contenente informazioni dettagliate e aggiornate correlate al componente ***PC Analyzer***
- ***Annulla***: selezionare il pulsante per arrestare l'analisi in corso o tornare all'interfaccia utente di AVG predefinita (*panoramica dei componenti*) al completamento dell'analisi

7.17. ID Protection

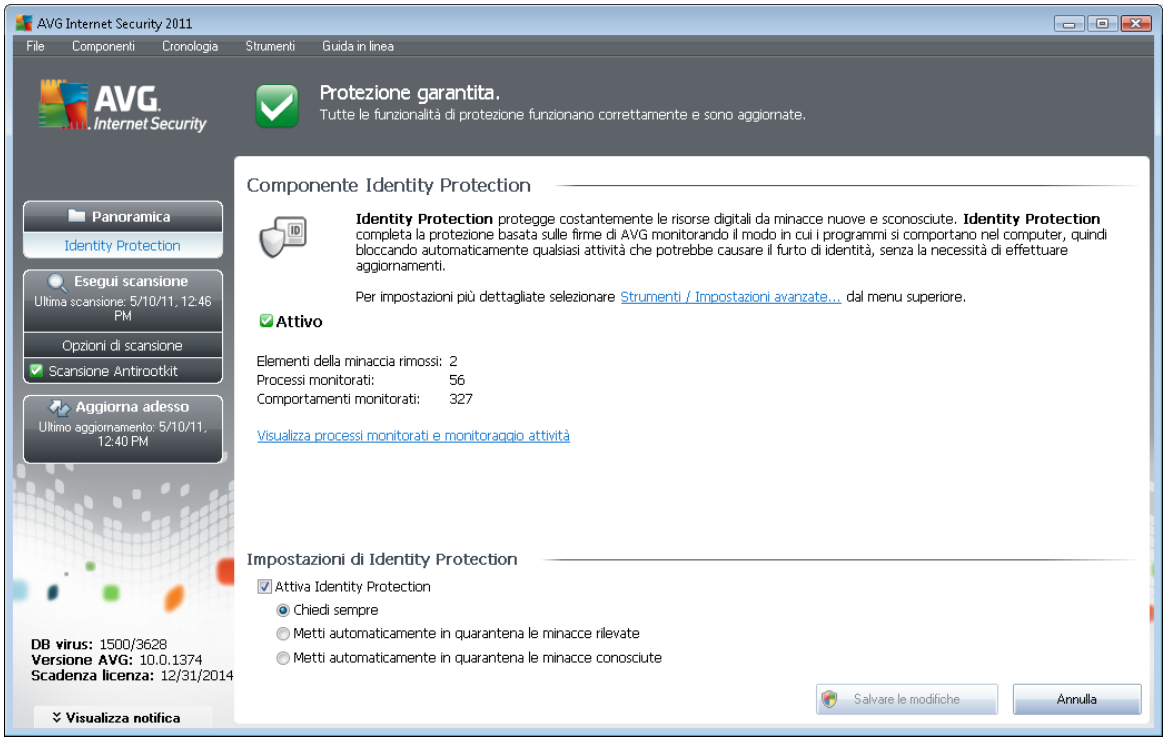
AVG Identity Protection è un prodotto anti-malware destinato alla prevenzione di attacchi da parte di malintenzionati volti a sottrarre password, dati dei conti bancari, numeri delle carte di credito e altri importanti dati digitali tramite qualsiasi tipo di software dannoso (*malware*) in grado di colpire il PC. L'applicazione assicura che tutti i programmi eseguiti sul PC funzionino correttamente. ***AVG Identity Protection*** rileva e blocca i comportamenti sospetti in modo continuo e protegge il computer da tutti i nuovi malware.

7.17.1. Principi di ID Protection

AVG Identity Protection è un componente anti-malware che protegge da tutti i tipi di malware (*spyware, bot, furto di identità e così via*) utilizzando tecnologie basate sul comportamento e fornisce la protezione zero day per i nuovi virus. I malware diventano sempre più sofisticati e assumono la forma di normali programmi per aprire il PC a malintenzionati che in remoto mirano al furto di identità. ***AVG Identity Protection*** protegge da questi nuovi malware basati sull'esecuzione. Rappresenta la protezione complementare di ***AVG Anti-Virus***, che protegge da virus conosciuti e basati su file utilizzando la scansione e il meccanismo delle firme.

È consigliabile installare sia AVG Anti-Virus che AVG Identity Protection per disporre della protezione completa per il PC.

7.17.2. Interfaccia di ID Protection



L'interfaccia del componente ***Identity Protection*** fornisce una breve descrizione delle funzionalità di base del componente, informazioni sul relativo stato e alcuni dati statistici:

- ***Elementi malware rimossi***: numero di applicazioni rilevate come malware e rimosse
- ***Processi monitorati***: numero di applicazioni in esecuzione monitorate da IDP
- ***Comportamenti monitorati***: numero di azioni specifiche in esecuzione all'interno delle applicazioni monitorate

Di seguito è disponibile il collegamento ***Visualizza processi monitorati e monitoraggio attività*** che consente di accedere all'interfaccia utente del componente ***System Tools*** che include una panoramica dettagliata di tutti i processi monitorati.

Impostazioni di Identity Protection

Nella parte inferiore della finestra di dialogo è presente la sezione ***Impostazioni di Identity Protection*** che consente di modificare alcune caratteristiche di base del funzionamento del componente:

- ***Attiva Identity Protection*** (*attivata per impostazione predefinita*): selezionare questa opzione per attivare il componente IDP e accedere a opzioni di modifica aggiuntive.

In alcuni casi, ***Identity Protection*** potrebbe segnalare che un file legittimo è sospetto o pericoloso. Poiché ***Identity Protection*** rileva le minacce in base al comportamento, ciò solitamente accade quando un programma tenta di monitorare la pressione dei tasti o di installare altri programmi oppure quando un nuovo driver viene installato nel computer. Pertanto, selezionare una delle seguenti opzioni specificando il comportamento del componente ***Identity Protection*** in caso di rilevamento di attività sospette:

  - ***Chiedi sempre***: se un'applicazione viene rilevata come malware verrà richiesto se dovrà essere bloccata (*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*)

  - ***Metti automaticamente in quarantena le minacce rilevate***: tutte le applicazioni rilevate come malware verranno bloccate automaticamente

  - ***Metti automaticamente in quarantena le minacce conosciute***: solo le applicazioni rilevate come malware con assoluta certezza verranno bloccate

Pulsanti di controllo

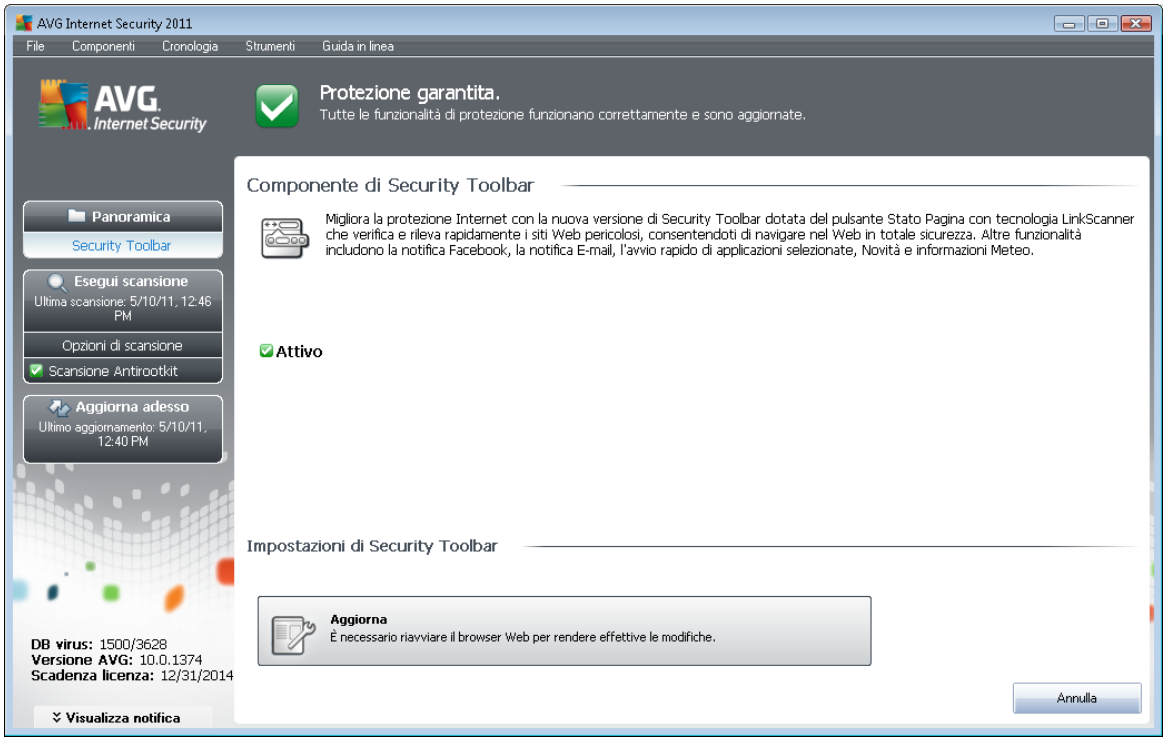
I pulsanti di controllo disponibili nell'interfaccia di ***Identity Protection*** sono i seguenti:

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

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

7.18. Security Toolbar

Security Toolbar è una barra degli strumenti opzionale per il browser Web che rende disponibili la protezione avanzata di AVG e vari strumenti e funzionalità durante la navigazione nel Web. Al momento, ***Security Toolbar*** è supportata dai browser Web Internet Explorer (*6.0 o versione successiva)* e Mozilla Firefox *(3.0 o versione successiva*):



Tutte le impostazioni del componente ***Security Toolbar*** sono accessibili direttamente dalla stessa ***Security Toolbar*** all'interno del browser Web.

8. AVG Security Toolbar

AVG Security Toolbar è un nuovo strumento che funziona insieme al componente ***LinkScanner***. ***AVG Security Toolbar*** può essere utilizzata per controllare le funzioni di ***LinkScanner*** e regolarne il comportamento.

Se si seleziona l'opzione che consente di installare la barra degli strumenti durante l'installazione di **AVG Internet Security 2011**, essa sarà aggiunta automaticamente al browser Web (Internet Explorer 6.0 o versione successiva e Mozilla Firefox 3.0 o versione successiva). Altri browser Internet non sono attualmente supportati.

Nota: *se si utilizza un browser Internet alternativo (ad esempio Avant Browser) potrebbero verificarsi comportamenti inattesi.*

8.1. Interfaccia di AVG Security Toolbar

AVG Security Toolbar è progettata per funzionare con ***MS Internet Explorer*** (*versione 6.0 o superiore*) e ***Mozilla Firefox*** (*versione 3.0 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:

AVG Security Toolbar si compone di quanto segue:

8.1.1. Pulsante del logo AVG

Questo pulsante consente di accedere alle voci della barra degli strumenti generale. Fare clic sul pulsante del logo per essere reindirizzati al sito Web di AVG. Se si fa clic 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 offerta dalla barra degli strumenti***
- ***Avvia AVG***: consente di aprire ***l'interfaccia utente di*****AVG Internet Security 2011**
- ***Informazioni su AVG***: apre un menu di scelta rapida con i seguenti collegamenti relativi a importanti informazioni sulla protezione correlate a **AVG Internet Security 2011**:
  - *Informazioni sulle minacce*: apre il sito Web di AVG in corrispondenza della pagina che fornisce i dati più importanti sulle minacce principali, consigli per la rimozione dei virus, informazioni sugli aggiornamenti AVG, accesso al database dei virus e altre informazioni pertinenti
  - *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

- *AVG Threat Labs*: apre il sito Web AVG Site Reports in cui è possibile ricercare minacce specifiche tramite il relativo nome e ottenere informazioni dettagliate su ciascuna di esse

- ***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***: direttamente da ***AVG Security Toolbar*** consente di eliminare la cronologia completa oppure, distintamente, la cronologia delle ricerche, la cronologia del browser, la cronologia dei download e i cookie.

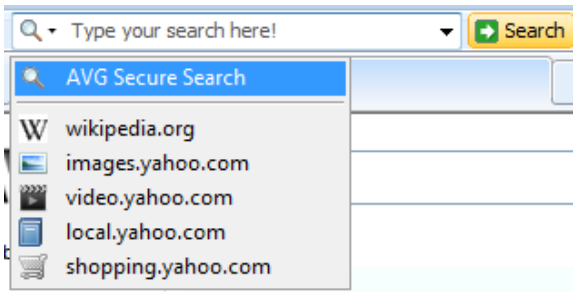
- ***Aggiorna***: consente di controllare la disponibilità di nuovi aggiornamenti per ***AVG Security Toolbar***

- ***Guida***: fornisce le opzioni per aprire il file della guida, contattare l'Assistenza tecnica AVG, inviare commenti relativi ai prodotti oppure visualizzare i dettagli della versione corrente della barra degli strumenti

8.1.2. Casella di ricerca con tecnologia AVG Secure Search (powered by Google)

La casella ***AVG Secure Search (powered by Google)*** rappresenta un modo semplice e sicuro per eseguire ricerche nel Web utilizzando AVG Secure Search (powered by Google). Immettere una parola o una frase nella casella di ricerca e selezionare il pulsante ***Ricerca*** o premere il tasto ***Invio*** per avviare la ricerca direttamente sul server AVG Secure Search (powered by Google), indipendentemente dalla pagina al momento visualizzata. Nella casella di ricerca viene inoltre elencata la cronologia della ricerca. Le ricerche eseguite dalla casella di ricerca vengono analizzate da ***Search-Shield.***

In alternativa, dal campo di ricerca è possibile accedere a Wikipedia o ad altri servizi per la ricerca specifici - vedere la figura:



8.1.3. Stato pagina

Direttamente nella barra degli strumenti, questo pulsante mostra la valutazione della pagina Web visualizzata in base ai criteri del componente ***Surf-Shield***:

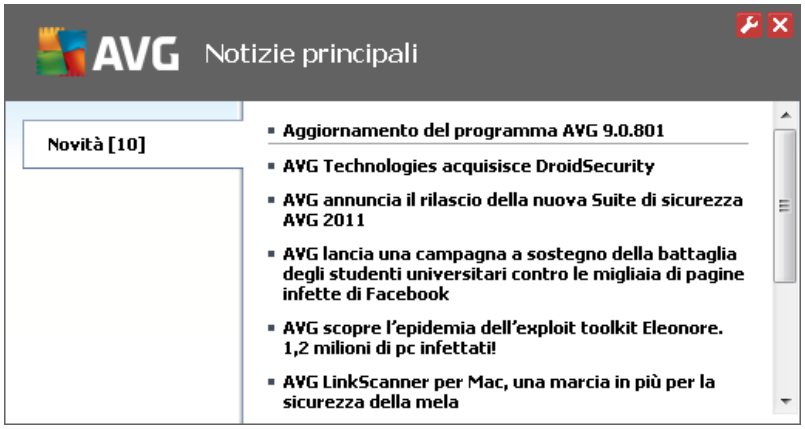
- - La pagina collegata è sicura.

-  - La pagina è sospetta.
-  - La pagina contiene collegamenti a pagine sicuramente pericolose.
-  - La pagina collegata contiene minacce attive. Per motivi di sicurezza, non sarà consentito visitare questa pagina.
-  - La pagina non è accessibile, pertanto non è stato possibile eseguirne la scansione.

Fare clic sul pulsante per aprire un riquadro informativo con dati dettagliati sulla pagina Web specifica.

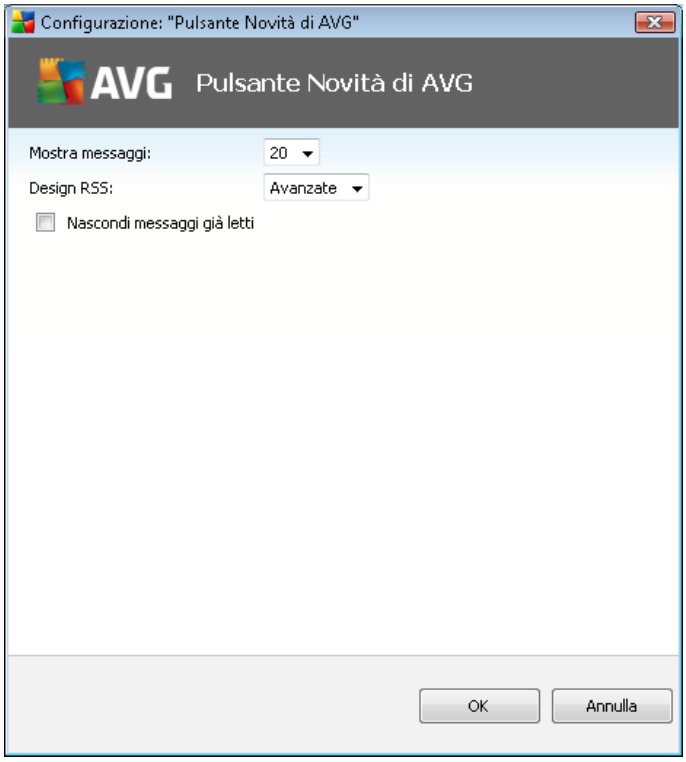
8.1.4. Novità di AVG

Direttamente da ***AVG Security Toolbar***, questo pulsante apre una panoramica delle ultime ***notizie principali*** correlate a AVG, sia notizie della stampa che comunicati stampa della società:



Nell'angolo superiore destro sono disponibili due pulsanti di controllo rossi:

-  - il pulsante apre la finestra di dialogo di modifica in cui è possibile specificare i parametri del pulsante ***Novità di AVG*** visualizzato in ***AVG Security Toolbar***:

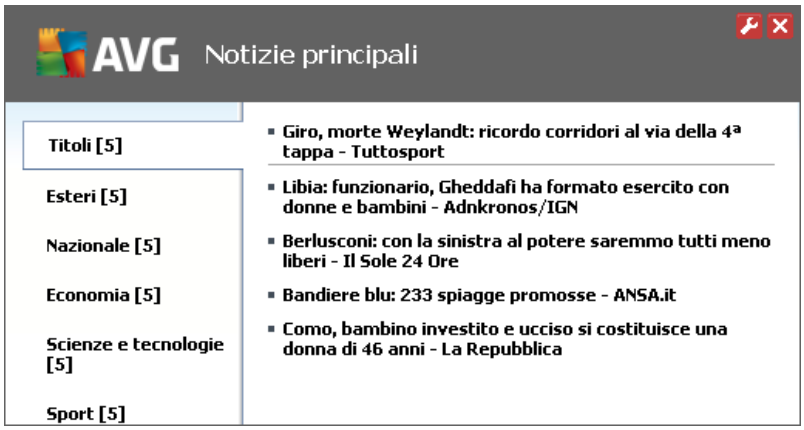


- o ***Mostra messaggi***: consente di modificare il numero desiderato di messaggi da visualizzare contemporaneamente
- o ***Design RSS***: consente di selezionare le modalità avanzata/di base della visualizzazione corrente della panoramica delle notizie (*per impostazione predefinita, è selezionata la modalità avanzata; vedere figura in alto*)
- o ***Nascondi messaggi già letti***: selezionare questa voce per confermare che i messaggi letti non devono più essere visualizzati, in modo che possano essere pubblicati i messaggi nuovi

- - fare clic su questo pulsante per chiudere la panoramica delle notizie aperta

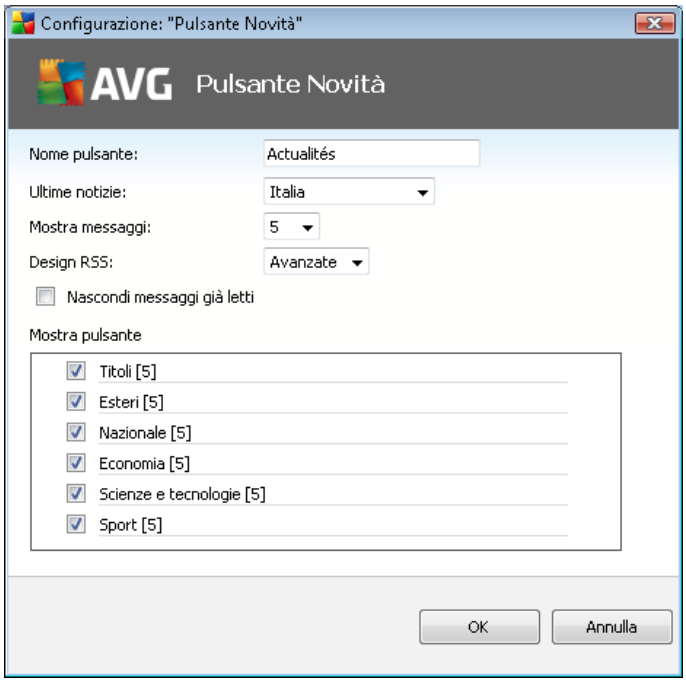
8.1.5. Novità

Analogamente, direttamente da ***AVG Security Toolbar***, questo pulsante apre una panoramica delle ultime notizie fornite da media selezionati suddivise in varie sezioni:



Nell'angolo superiore destro sono disponibili due pulsanti di controllo rossi:

- - il pulsante apre la finestra di dialogo di modifica in cui è possibile specificare i parametri del pulsante ***Novità*** visualizzato in ***AVG Security Toolbar***:



o ***Nome pulsante***: è possibile modificare il nome del pulsante visualizzato in ***AVG Security Toolbar***

o ***Ultime notizie***: scegliere un paese dall'elenco per visualizzare le notizie relative alla regione selezionata

o ***Mostra messaggi***: consente di specificare il numero desiderato di messaggi da visualizzare

contemporaneamente

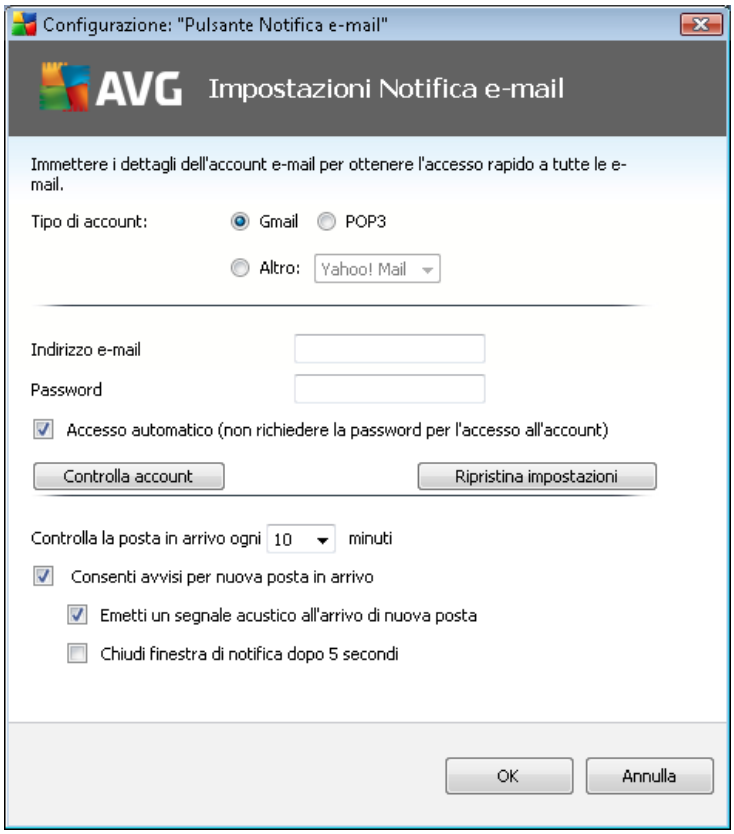
- **_Design RSS_**: consente di selezionare le opzioni Avanzate/Base per impostare la visualizzazione della panoramica delle notizie (**_per impostazione predefinita, è selezionata la modalità avanzata; vedere figura in alto_**)
- **_Nascondi messaggi già letti_**: selezionare questa voce per confermare che i messaggi letti non devono più essere visualizzati nella panoramica delle notizie e possono essere sostituiti dai nuovi titoli
- **_Mostra pulsante_**: in questo campo è possibile selezionare il tipo di notizie da visualizzare nella panoramica delle notizie di **_AVG Security Toolbar_**
  - - fare clic su questo pulsante per chiudere la panoramica delle notizie aperta

8.1.6. Elimina cronologia

Tramite questo pulsante è possibile eliminare la cronologia del browser come avviene tramite l'opzione **_logo AVG -> Elimina cronologia_**.

8.1.7. Notifica e-mail

Il pulsante **_Notifica e-mail_**consente di attivare l'opzione di notifica di nuovi messaggi e-mail ricevuti direttamente dall'interfaccia di ***AVG Security Toolbar***. Il pulsante apre la seguente finestra di dialogo di modifica, in cui è possibile definire i parametri dell'account e-mail e le regole di visualizzazione delle e-mail. Seguire le istruzioni fornite nella finestra di dialogo:



- **_Tipo di account_**: specifica il tipo di protocollo utilizzato dall'account e-mail. È possibile selezionare una delle seguenti alternative: *Gmail*, *POP3* oppure selezionare il nome del

server dal menu a discesa attivabile tramite la voce *Altro* (*al momento, è possibile selezionare questa opzione se si utilizza un account Yahoo! JP Mail o Hotmail*). Se non si è certi del tipo di server e-mail utilizzato dall'account, provare a recuperare le informazioni dal provider e-mail o dall'Internet Service Provider.

- ***Accesso***: nella sezione seguente fornire l'*indirizzo e-mail* e la relativa *password*. Mantenere selezionata l'opzione *Accesso automatico* in modo da non dover immettere i dati ripetutamente.
- ***Controlla account***: utilizzare questo pulsante per controllare i dati immessi.
- ***Ripristina impostazioni***: rimuove rapidamente l'indirizzo e-mail immesso in precedenza.
- ***Controlla la posta in arrivo ogni ... minuti***: definire l'intervallo di tempo da utilizzare per controllare i nuovi messaggi e-mail in arrivo (*da 5 a 120 minuti*) e specificare se e come si desidera essere informati circa l'arrivo di nuovi messaggi.
- ***Consenti avvisi per nuova posta in arrivo***: deselezionare questa casella per disattivare le notifiche visive dell'arrivo di nuovi messaggi e-mail.
    - ***Emetti un segnale acustico all'arrivo di nuova posta***: deselezionare questa casella per disattivare le notifiche sonore dell'arrivo di nuovi messaggi e-mail.
    - ***Chiudi finestra di notifica dopo 5 secondi***: selezionare questa casella per chiudere automaticamente dopo 5 secondi la finestra di notifica visiva dell'arrivo di nuovi messaggi e-mail.

8.1.8. Meteo

Il pulsante ***Meteo*** consente di visualizzare informazioni sulla temperatura corrente (*aggiornate ogni 3-6 ore*) nella località selezionata direttamente dall'interfaccia di ***AVG Security Toolbar***. Fare clic sul pulsante per aprire un nuovo riquadro informativo con una panoramica dettagliata del meteo:

Sono disponibili le seguenti opzioni di modifica:

- ***Cambia località***: fare clic sul testo ***Cambia località*** per visualizzare una nuova finestra di dialogo denominata ***Ricerca la località***. Immettere il nome della località desiderata nel campo di testo e confermare facendo clic sul pulsante ***Ricerca***. Quindi, all'interno dell'elenco delle località con lo stesso nome selezionare quella ricercata. Infine, il riquadro informativo verrà visualizzato di nuovo con le informazioni meteorologiche relative alla località selezionata.

- ***Convertitore Fahrenheit/Celsius***: nell'angolo superiore destro del riquadro informativo è possibile scegliere tra le scale Fahrenheit e Celsius. In base alla selezione, le informazioni sulla temperatura verranno fornite nella scala desiderata.

- ***Previsioni complete***: se si è interessati alle previsioni complete e dettagliate, utilizzare il collegamento ***Previsioni complete*** per passare al sito Web specializzato in previsioni meteorologiche.

8.1.9. Facebook

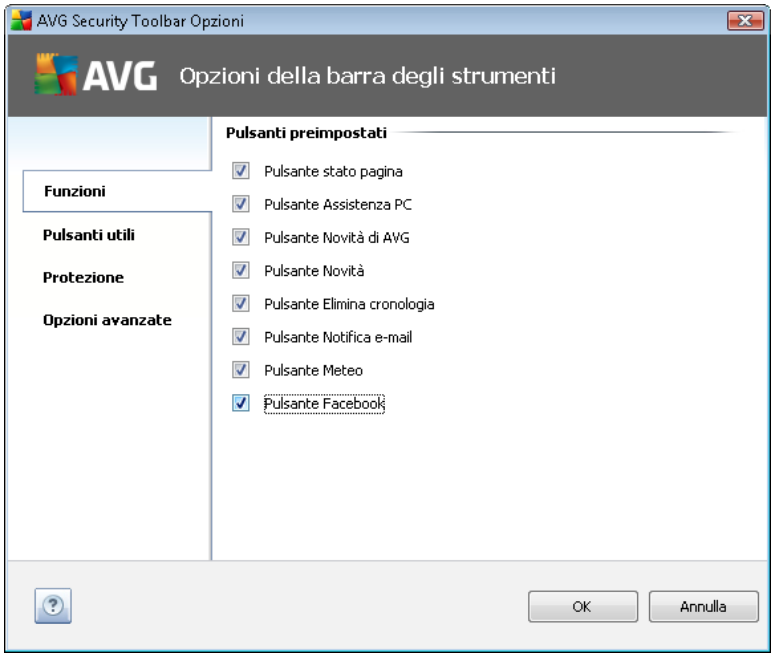
Il pulsante ***Facebook*** consente di connettersi al social network Facebook direttamente da ***AVG Security Toolbar***. Fare clic sul pulsante per visualizzare l'opzione di accesso, quindi fare clic su tale opzione per aprire la finestra di dialogo ***Accedi a Facebook***. Immettere i dati di accesso, quindi fare clic sul pulsante ***Accedi***. Se non si dispone ancora di un account Facebook, è possibile crearne uno direttamente utilizzando il collegamento ***Iscriviti a Facebook***.

All'interno del processo di registrazione di Facebook viene richiesto di autorizzare l'applicazione ***AVG Social Extension***. La funzionalità dell'applicazione è essenziale per la connessione barra degli strumenti - Facebook, pertanto accertarsi di autorizzare tale funzionalità. La connessione a Facebook verrà quindi attivata e il pulsante ***Facebook*** all'interno di ***AVG Security Toolbar*** offrirà le opzioni di menu Facebook standard.

8.2. 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:

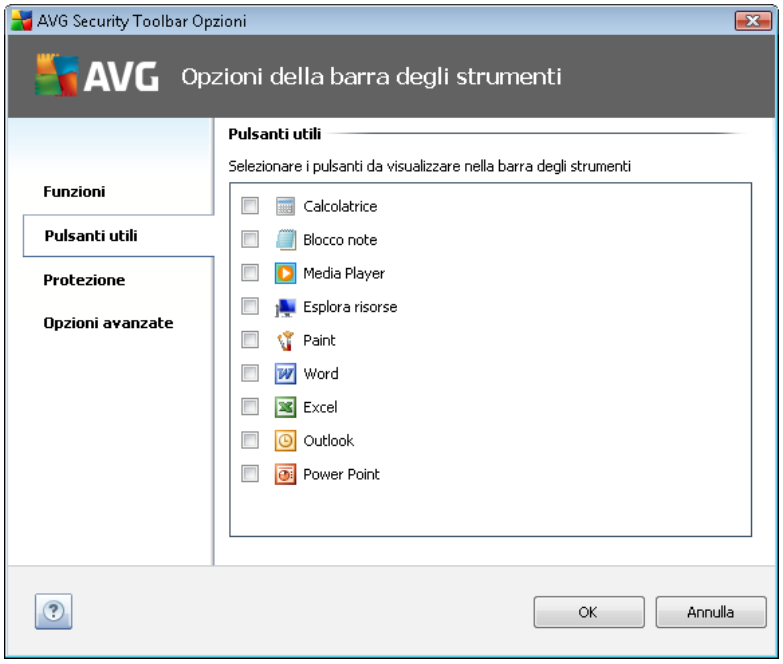
8.2.1. Scheda Generale



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:

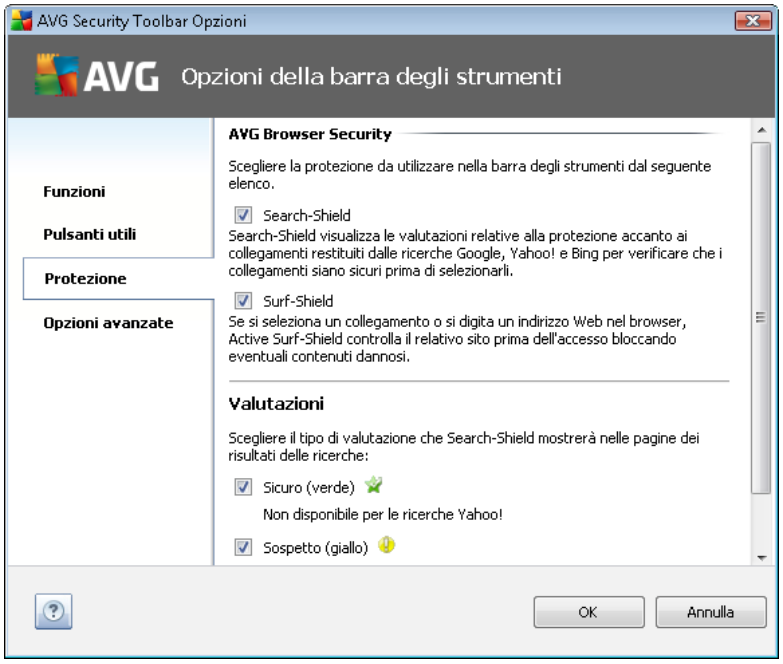
- ***Pulsante Stato pagina***: questo pulsante consente di visualizzare le informazioni sullo stato di protezione della pagina aperta al momento in ***AVG Security Toolbar***
- ***Pulsante Novità di AVG***: questo pulsante consente di aprire la pagina Web contenente i comunicati stampa più recenti relativi a AVG
- ***Pulsante Novità***: questo pulsante fornisce una panoramica articolata delle ultime notizie presenti sui vari quotidiani
- ***Pulsante Elimina cronologia***: questo pulsante consente di utilizzare le opzioni Elimina cronologia completa oppure Elimina cronologia ricerche, Elimina cronologia browser, Elimina cronologia download o Elimina cookie direttamente dal riquadro AVG Security Toolbar
- ***Pulsante Notifica e-mail***: questo pulsante consente di visualizzare la notifica dei nuovi messaggi e-mail ricevuti direttamente dall'interfaccia di ***AVG Security Toolbar***
- ***Pulsante Meteo***: questo pulsante fornisce informazioni immediate sulla situazione meteorologica in una località selezionata
- ***Pulsante Facebook***: questo pulsante fornisce la connessione diretta al social network Facebook

8.2.2. 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.

8.2.3. Scheda Protezione



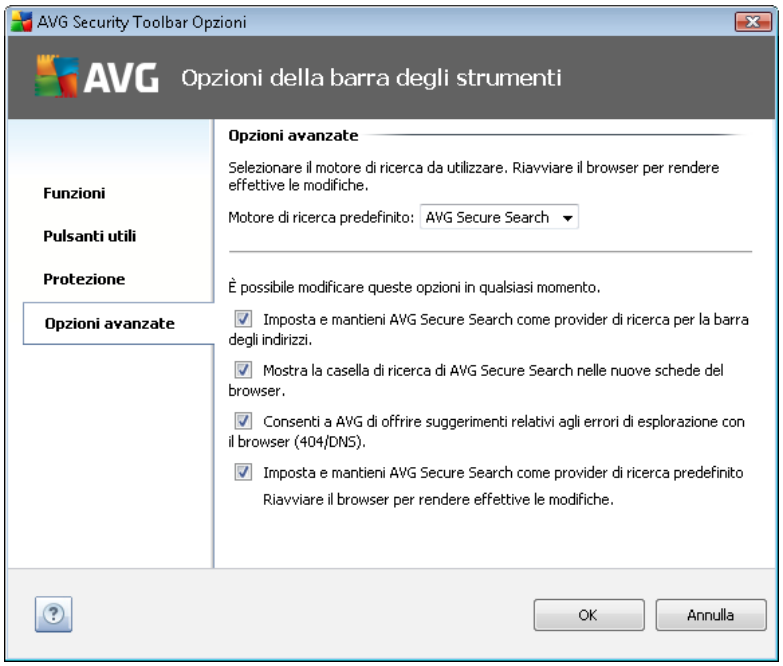
La scheda ***Protezione*** è divisa in due sezioni, ***AVG Browser Security*** e ***Valutazioni***, in cui è

possibile selezionare caselle di controllo specifiche per determinare la funzionalità di ***AVG Security Toolbar*** da utilizzare:

- ***Browser Security***: selezionare questa voce per attivare o disattivare i servizi ***AVG Search-Shield*** e/o ***Surf-Shield***
- ***Valutazioni***: selezionare i simboli grafici utilizzati per le valutazioni dei risultati di ricerca dal componente ***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.***

8.2.4. Scheda Opzioni avanzate



Nella scheda ***Opzioni avanzate*** selezionare innanzitutto il motore di ricerca predefinito da utilizzare. È possibile scegliere tra *AVG Secure Search (powered by Google), Baidu, WebHledani*, *Yandex e Yahoo! JP*. 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*** *(il titolo indicato si riferisce alle impostazioni AVG Secure Search (powered by Google) predefinite)*:

- ***Imposta e mantieni AVG Secure Search (powered by Google) come provider di ricerca per la barra degli indirizzi***: se selezionata, questa opzione consente di digitare una parola chiave per la ricerca direttamente nella barra degli indirizzi del browser Internet: il servizio Google verrà utilizzato automaticamente per ricercare i siti Web pertinenti.

- ***Consenti ad AVG di fornirti suggerimenti relativi agli errori di navigazione con il browser (404/DNS)***: 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.

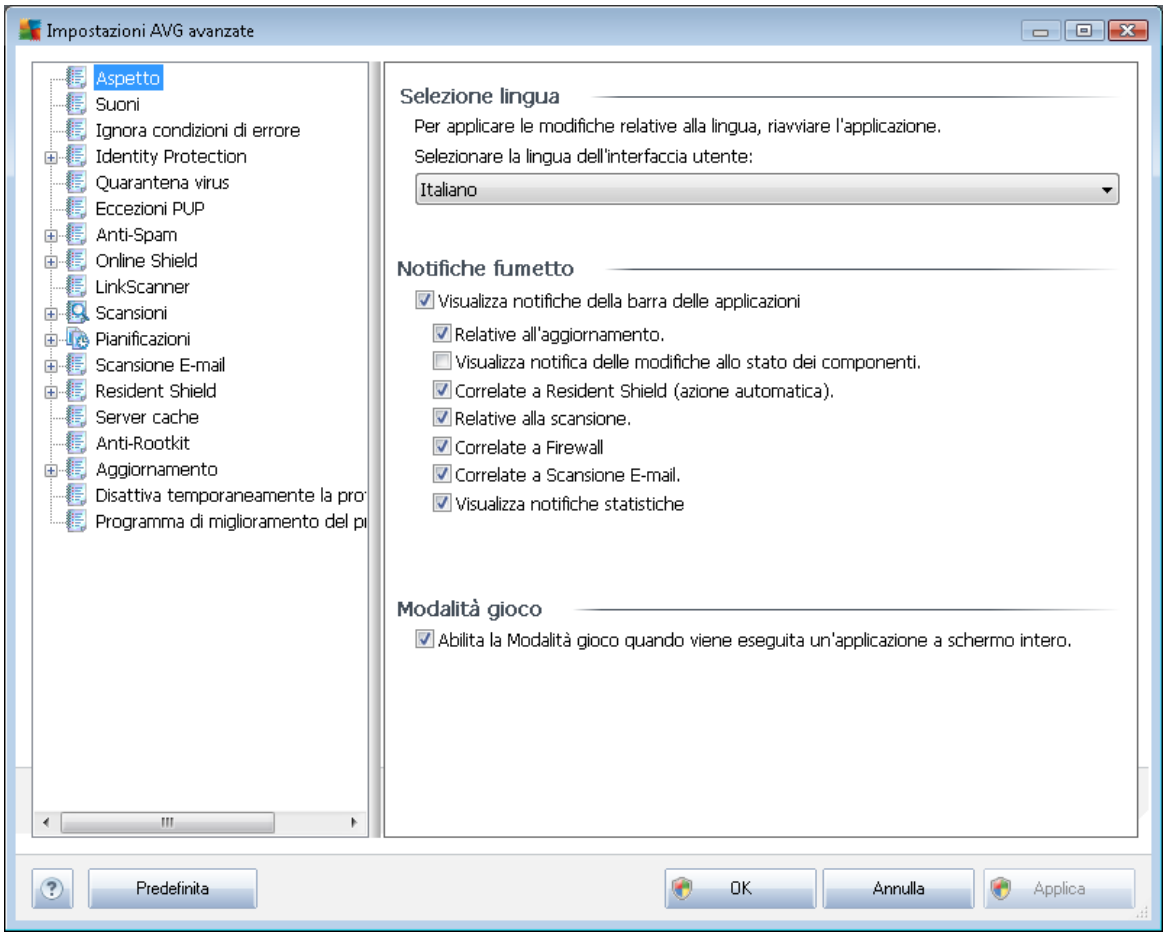
- ***Imposta e mantieni AVG Secure Search (powered by Google) come provider di ricerca predefinito***: Google è il motore di ricerca predefinito per la ricerca Web in ***AVG Security Toolbar***; attivando questa opzione, Google può diventare inoltre il motore di ricerca predefinito per il browser Web.

9. Impostazioni AVG avanzate

Le opzioni di configurazione avanzata di **AVG Internet Security 2011** 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.

9.1. Aspetto

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

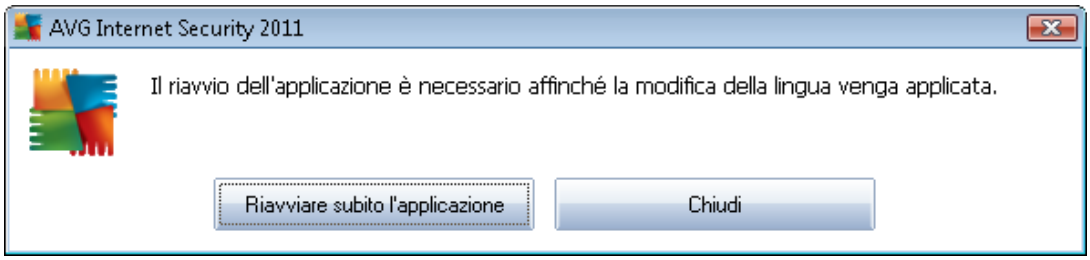


Selezione lingua

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 relativo all'opzione personalizzata*) e l'inglese (*installato per impostazione predefinita*). 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 viene descritto come disattivare la visualizzazione delle notifiche tramite fumetto presenti sulla barra delle applicazioni che informano circa lo stato dell'applicazione. Per impostazione predefinita, è consentita la visualizzazione delle notifiche tramite fumetto e si consiglia di mantenere questa configurazione. In genere le notifiche tramite fumetto forniscono informazioni sul cambiamento di stato dei componenti di AVG, pertanto devono essere 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 fumetto. Quando è attivata, è possibile selezionare inoltre 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 (azione automatica)***: 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 Firewall***: consente di decidere se visualizzare le informazioni relative ai processi e allo stato del firewall, quali avvisi di attivazione/disattivazione del componente, possibile blocco del traffico e così via.

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

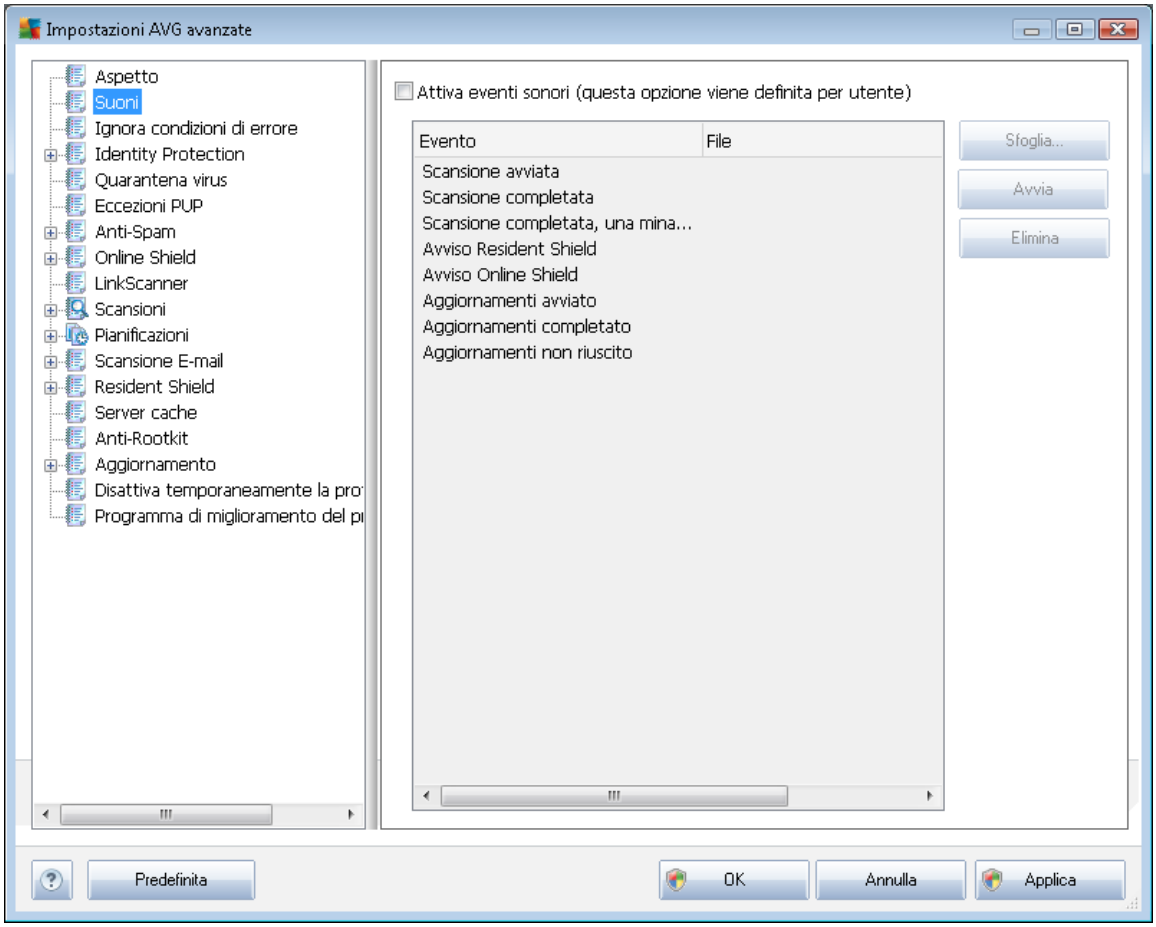
- ***Visualizza notifiche statistiche***: mantenere l'opzione selezionata per consentire la visualizzazione di regolari notifiche delle revisioni statistiche nella barra delle applicazioni.

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*).

9.2. 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:

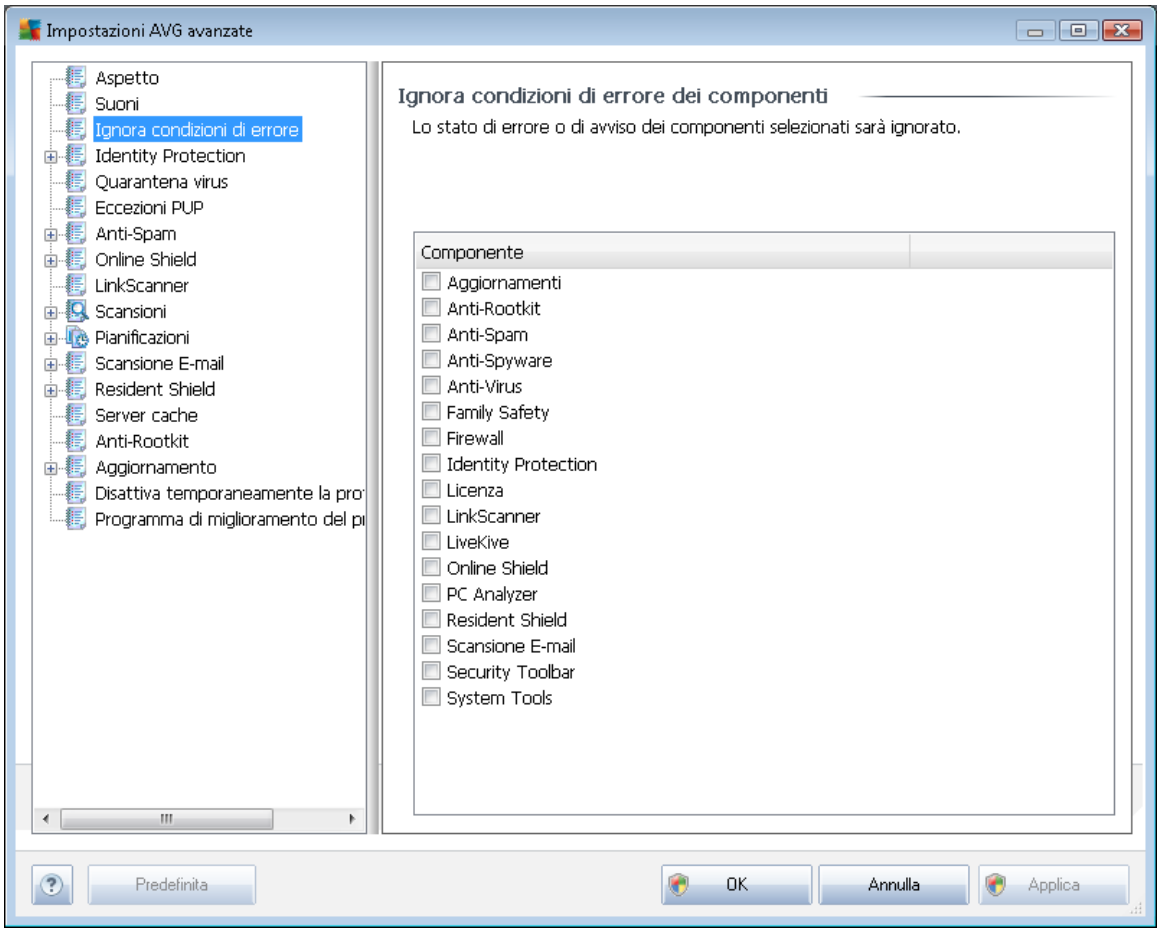


Quindi, selezionare l'evento pertinente dall'elenco e ricercare nel disco rigido (tramite ***Sfoglia***) un suono appropriato da assegnare all'evento. Per ascoltare il suono selezionato, evidenziare l'evento nell'elenco e fare clic sul pulsante ***Avvia***. Utilizzare il pulsante ***Elimina*** per rimuovere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

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

9.3. 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

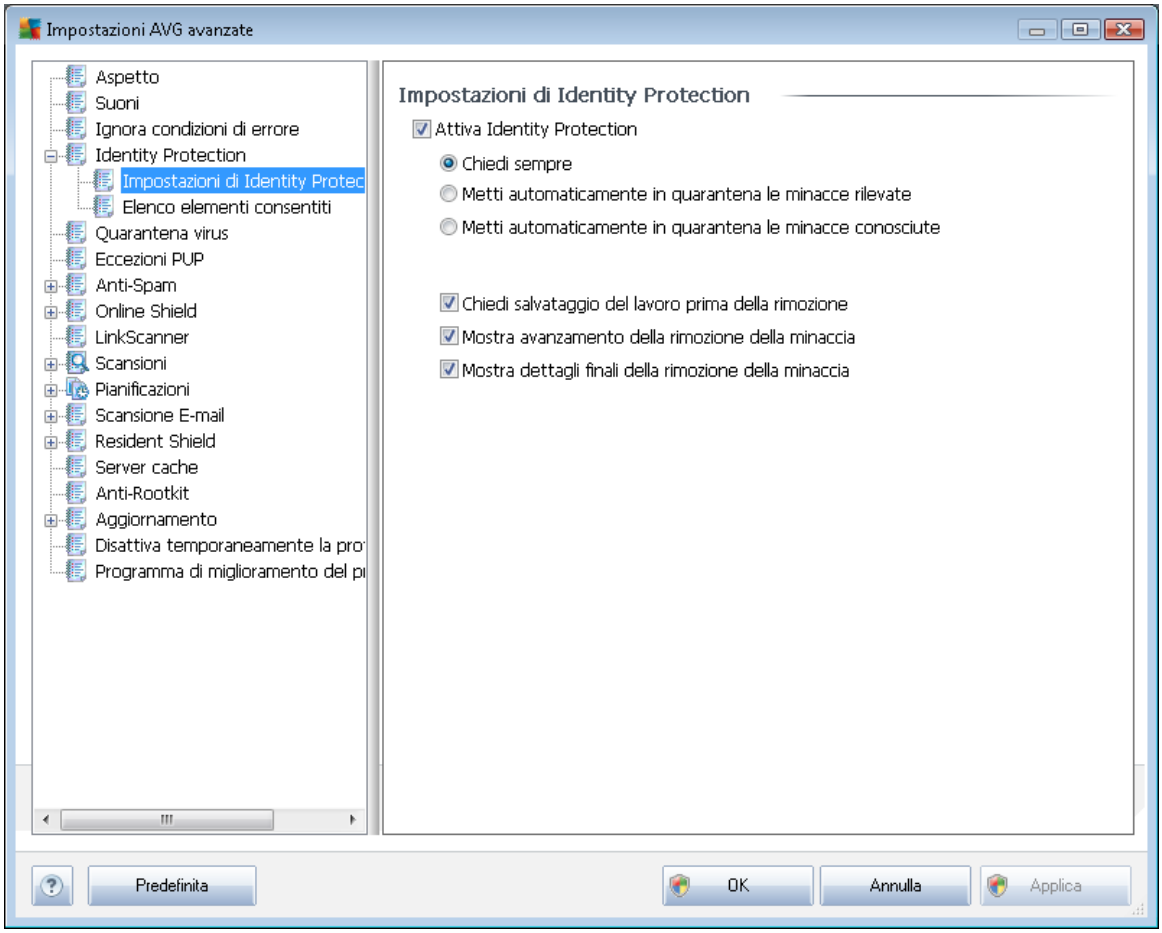
condizione è stata indotta deliberatamente dall'utente e si è consapevoli del potenziale rischio. Nel contempo, una volta che viene visualizzata in grigio, l'icona non può più segnalare eventuali errori ulteriori che potrebbero verificarsi.

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.

9.4. Identity Protection

9.4.1. Impostazioni di Identity Protection

La finestra di dialogo ***Impostazioni di Identity Protection***consente di attivare/disattivare le funzioni di base del componente ***Identity Protection***:



Attiva Identity Protection (*attivata per impostazione predefinita*): deselezionare la casella per disattivare il componente ***Identity Protection***.

Si consiglia di non disattivare questo componente a meno che non sia assolutamente

necessario.

Quando ***Identity Protection*** è attivato, è possibile specificare l'azione da intraprendere quando viene rilevata una minaccia:

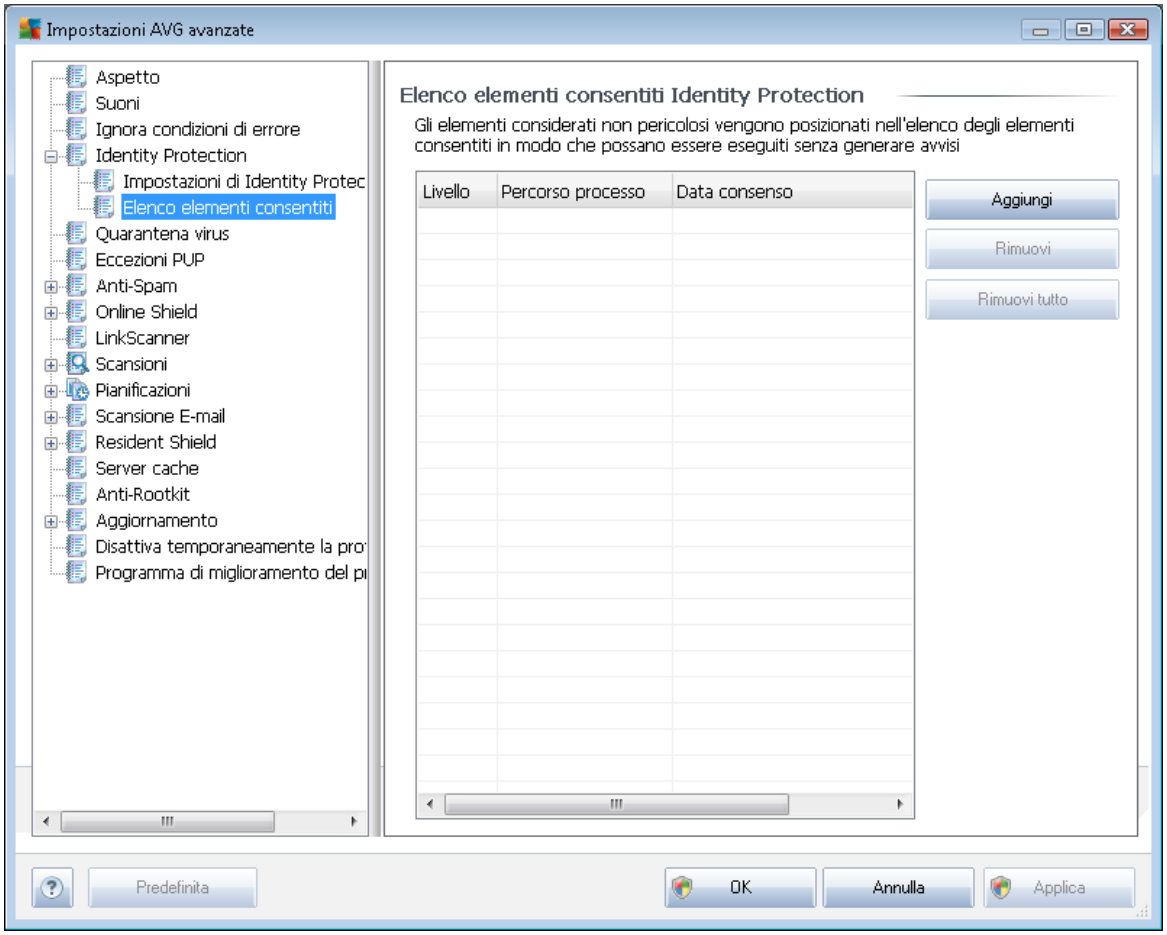
- ***Chiedi sempre***: (*attivata per impostazione predefinita*) quando viene rilevata una minaccia, verrà richiesto se spostarla in quarantena per assicurare che nessuna applicazione da eseguire venga rimossa.
- ***Metti automaticamente in quarantena le minacce rilevate***: selezionare questa casella di controllo per spostare immediatamente tutte le potenziali minacce rilevate nell'area sicura di ***Quarantena virus di AVG***. Se si mantengono le impostazioni predefinite, quando una minaccia viene rilevata verrà richiesto se spostarla in quarantena per assicurare che nessuna applicazione da eseguire venga rimossa.
- ***Metti automaticamente in quarantena le minacce conosciute***: mantenere selezionata questa voce se si desidera che tutte le applicazioni rilevate come possibili malware vengano messe subito in ***Quarantena virus di AVG*** automaticamente.

È inoltre possibile utilizzare voci specifiche per attivare facoltativamente ulteriori funzionalità di ***Identity Protection***:

- ***Chiedi salvataggio del lavoro prima della rimozione*** (*attivata per impostazione predefinita*): mantenere selezionata questa voce se si desidera essere avvertiti prima che l'applicazione rilevata come possibile malware venga messa in quarantena. Se l'applicazione è in uso, il progetto potrebbe venire perso, pertanto è necessario salvarlo. Questa voce è attivata per impostazione predefinita e si consiglia di non modificare questa impostazione.
- ***Mostra avanzamento della rimozione del malware*** (*attivata per impostazione predefinita*) : con questa voce attivata, quando viene rilevato un potenziale malware si apre una nuova finestra di dialogo per visualizzare l'avanzamento dello spostamento del malware in quarantena.
- ***Mostra i dettagli finali della rimozione del malware*** (*attivata per impostazione predefinita*): con questa voce attivata, ***Identity Protection*** visualizza informazioni dettagliate su ciascun oggetto spostato in quarantena (*livello di gravità, posizione e così via.*).

9.4.2. Elenco elementi consentiti

Se nella finestra di dialogo delle ***impostazioni di Identity Protection*** non è stata selezionata la voce ***Metti automaticamente in quarantena le minacce rilevate***, ogni qualvolta verrà rilevato un malware potenzialmente pericoloso verrà richiesto se tale malware dovrà essere rimosso. Se si contrassegna l'applicazione sospetta (*rilevata in base al comportamento*) come sicura e si conferma che è possibile mantenerla nel computer, l'applicazione verrà aggiunta all'***elenco degli elementi consentiti di Identity Protection*** e non verrà più segnalata come potenzialmente pericolosa:



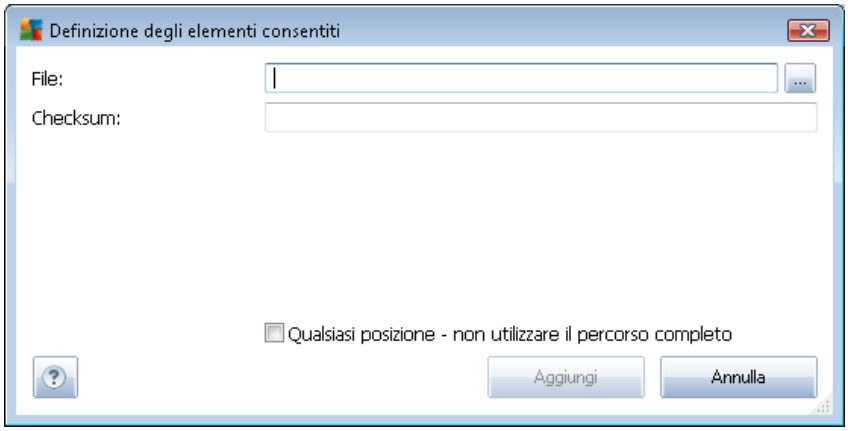
L'***elenco degli elementi consentiti di Identity Protection*** fornisce le seguenti informazioni su ciascuna applicazione:

- ***Livello***: identificazione grafica della gravità di un determinato processo valutata su una scala di quattro livelli dal meno grave (■□□□) al più grave (■■■■)
- ***Percorso processo***: posizione del file eseguibile (*processo*) dell'applicazione
- ***Data consenso***: data in cui l'applicazione è stata contrassegnata manualmente come sicura

Pulsanti di controllo

I pulsanti di controllo disponibili nella finestra di dialogo dell'***elenco degli elementi consentiti di Identity Protection*** sono i seguenti:

- ***Aggiungi***: fare clic su questo pulsante per aggiungere una nuova applicazione all'elenco degli elementi consentiti. Viene visualizzata la seguente finestra di dialogo:



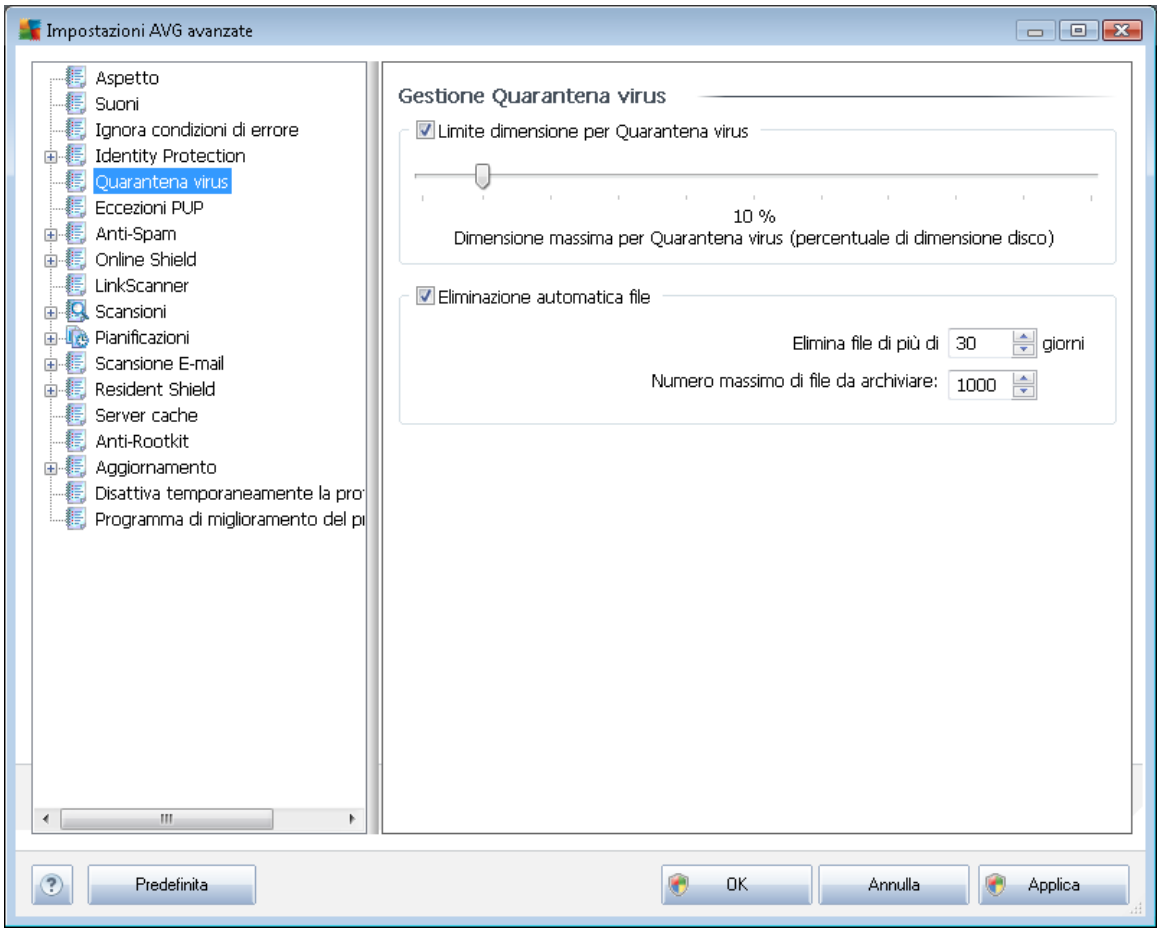
- o ***File***: digitare il percorso completo del file (*applicazione*) da contrassegnare come eccezione.

- o ***Checksum***: visualizza 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.

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

- ***Rimuovi***: selezionare questa opzione per rimuovere l'applicazione selezionata dall'elenco.
- ***Rimuovi tutto***: selezionare questa opzione per rimuovere tutte le applicazioni elencate.

9.5. Quarantena virus



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

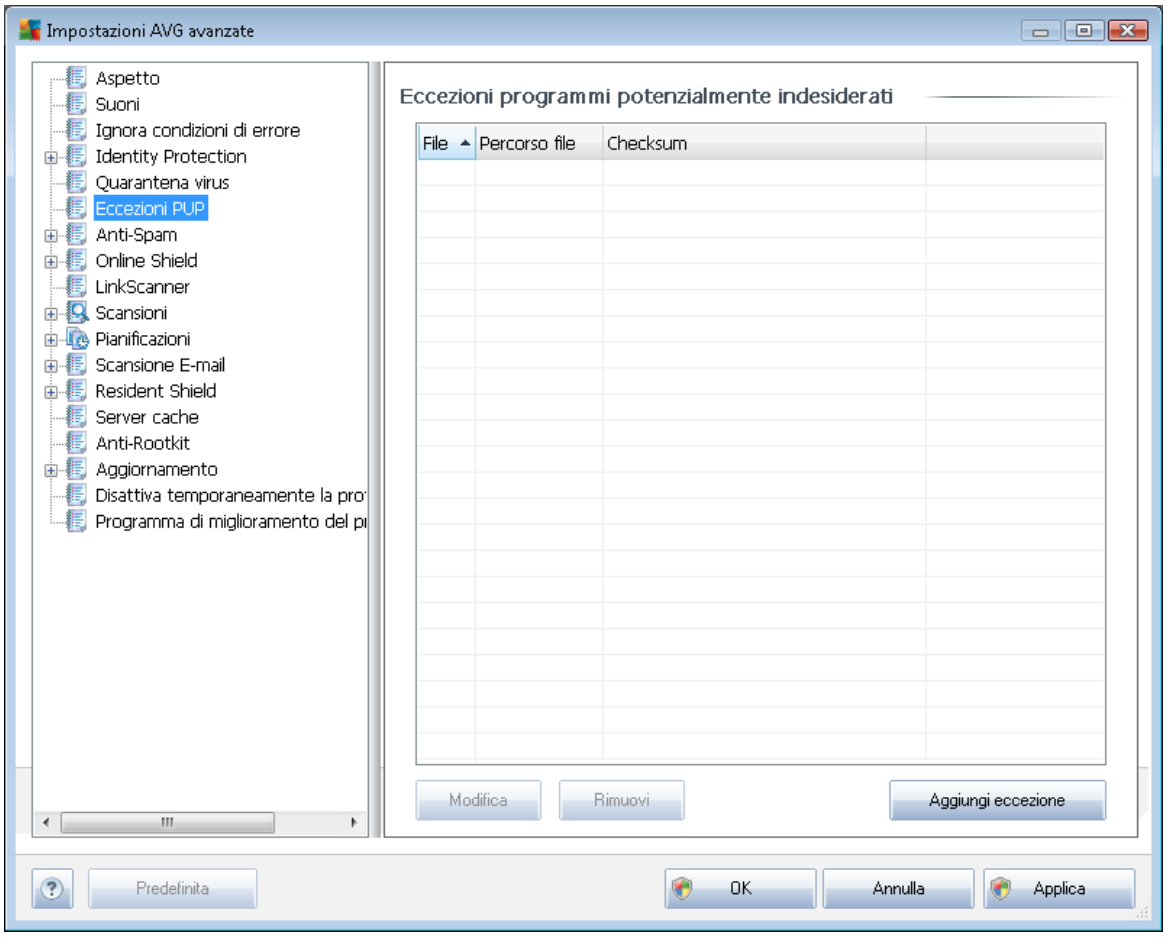
- ***Limite dimensione per Quarantena virus***: utilizzare il dispositivo di scorrimento per impostare la dimensione massima di ***Quarantena virus***. La dimensione è specificata in maniera proporzionale rispetto alla dimensione del disco locale.

- ***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***)

9.6. Eccezioni PUP

AVG Internet Security 2011 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 ai programmi potenzialmente indesiderati. È possibile modificare l'elenco, eliminare voci esistenti o aggiungere nuove eccezioni. L'elenco fornisce le seguenti informazioni per ciascuna eccezione:

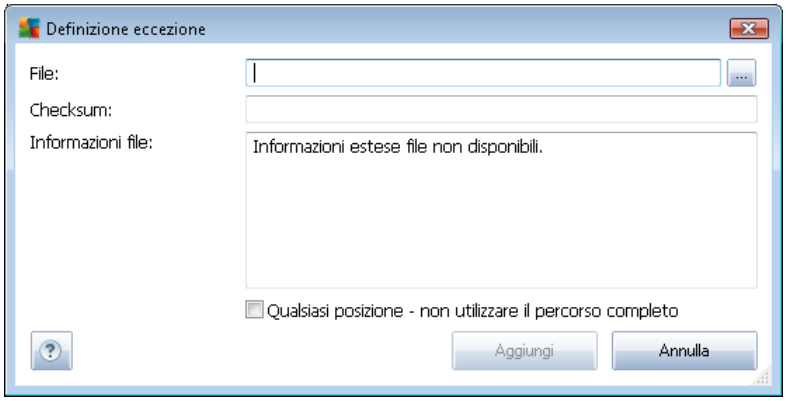
- ***File***: fornisce il nome della rispettiva applicazione
- ***Percorso file***: mostra la posizione dell'applicazione
- ***Checksum***: visualizza la "firma" univoca del file prescelto. Questo checksum è una stringa di caratteri generata automaticamente che consente a AVG di distinguere in modo inequivocabile il file prescelto 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

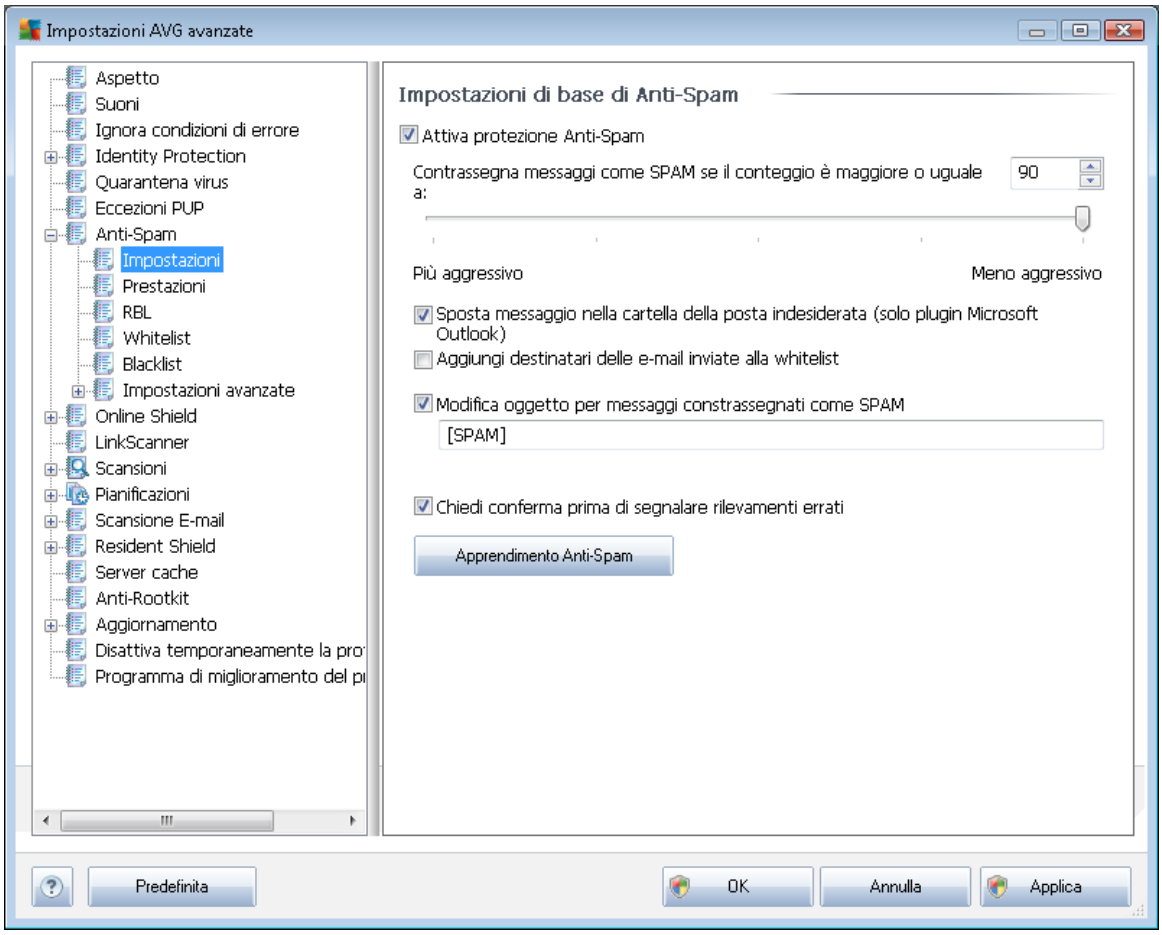
- ***Rimuovi***: consente di eliminare la voce selezionata dall'elenco di eccezioni.
- ***Aggiungi eccezione***: consente di aprire una finestra di dialogo per la modifica in cui è possibile definire i parametri della nuova eccezione da creare:



  - ***File***: digitare il percorso completo del file da contrassegnare come eccezione.
  - ***Checksum***: visualizza 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 prescelto 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 (*licenza, 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. Se la casella di controllo è selezionata, il file specificato viene definito come eccezione indipendentemente dalla relativa posizione (*tuttavia, è comunque necessario immettere il percorso completo dello specifico file; il file verrà quindi utilizzato come esemplare univoco nel caso in cui due file con lo stesso nome compaiano nel sistema*).

9.7. Anti-Spam

9.7.1. Impostazioni



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

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

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

- ***Valore compreso tra 80 e 90***: verranno filtrati i messaggi e-mail il cui contenuto potrebbe essere spam, ma potrebbero essere filtrati anche alcuni messaggi che non ne contengono.
- ***Valore compreso tra 60 e 79***: è considerata una configurazione piuttosto aggressiva.

Verranno filtrati i messaggi e-mail il cui contenuto può essere spam, ma potrebbero essere filtrati anche messaggi che non ne contengono.

- ***Valore compreso tra 50 e 59***: configurazione particolarmente aggressiva. È probabile che insieme ai messaggi e-mail contenenti spam vengano filtrati anche i messaggi normali. Questo intervallo di valori non è consigliato per l'uso normale.

Nella finestra di dialogo delle ***impostazioni di base Anti-Spam*** è possibile definire inoltre la modalità di gestione dei messaggi e-mail di spam:

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

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

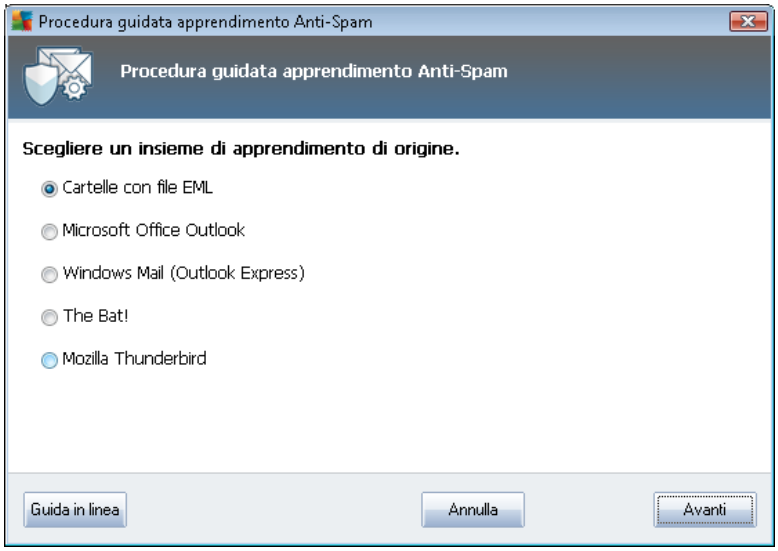
- ***Modifica oggetto per messaggi contrassegnati come spam***: selezionare questa casella di controllo se si desidera che tutti i messaggi rilevati come spam vengano contrassegnati con una parola o un carattere specifico nel campo dell'oggetto del messaggio e-mail; il testo desiderato può essere digitato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

- ***Chiedi conferma prima di segnalare rilevamenti errati***: se durante il processo di installazione si è scelto di partecipare al ***Programma di miglioramento del prodotto***, si è acconsentito a segnalare le minacce rilevate a AVG. La segnalazione viene effettuata automaticamente. Tuttavia, è possibile selezionare questa casella di controllo per specificare che si desidera venga richiesta una conferma prima che eventuale spam rilevato venga segnalato a AVG, in modo da assicurarsi che il messaggio possa effettivamente essere classificato come spam.

Pulsanti di controllo

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

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



Sono disponibili le seguenti opzioni:

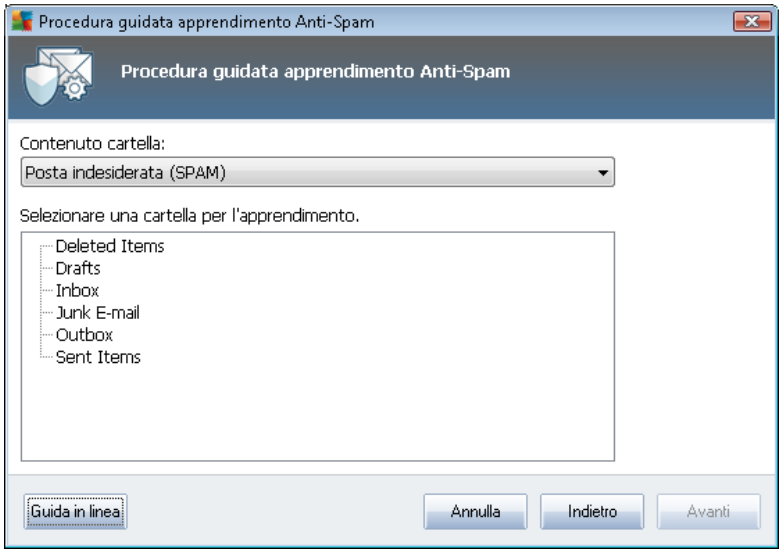
- ***Un client e-mail specifico***: se si utilizza uno dei client e-mail elencati (*MS Outlook, Outlook Express, The Bat!*), selezionare la relativa opzione
- ***Cartella con file EML***: se si utilizza qualsiasi altro programma e-mail, è necessario salvare i messaggi in una cartella specifica (*in formato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

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

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

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

Cartelle con file EML



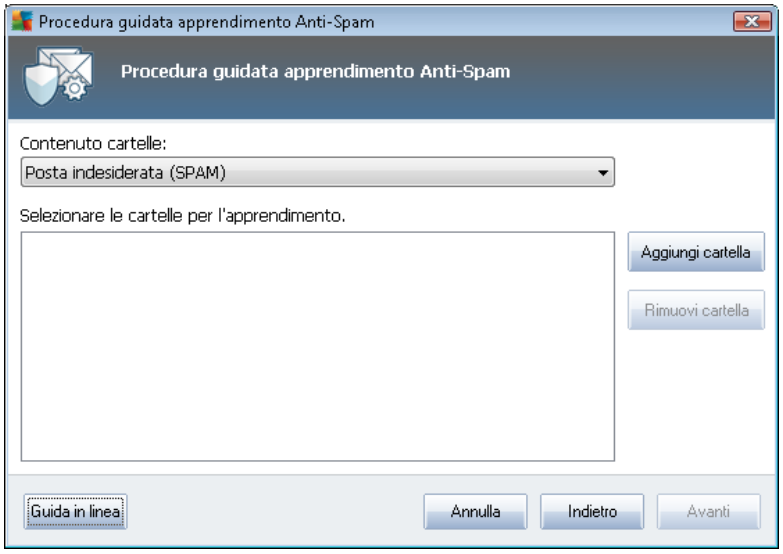
In questa finestra di dialogo selezionare la cartella contenente i messaggi che si desidera utilizzare per l'apprendimento. Fare clic sul pulsante ***Aggiungi cartella*** per individuare la cartella con i file .eml (*messaggi e-mail salvati*). La cartella selezionata verrà visualizzata nella finestra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

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

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

Client e-mail specifico

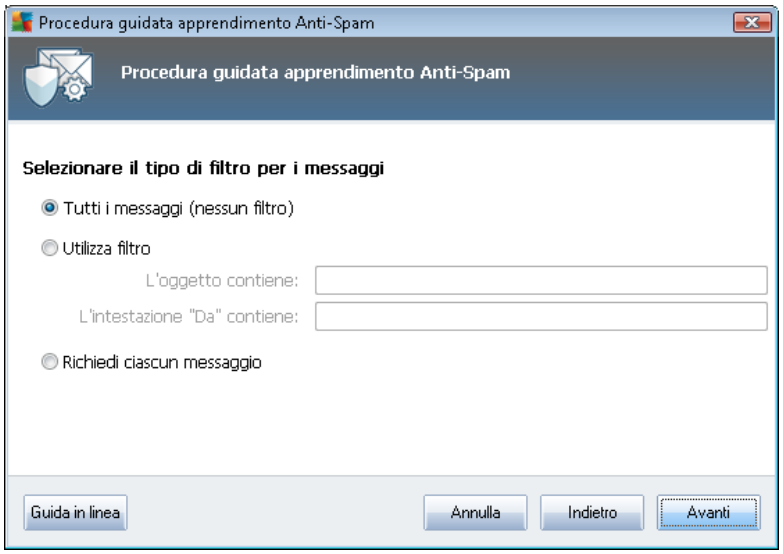
Dopo aver confermato un'opzione, viene visualizzata una nuova finestra di dialogo.



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

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

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



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

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

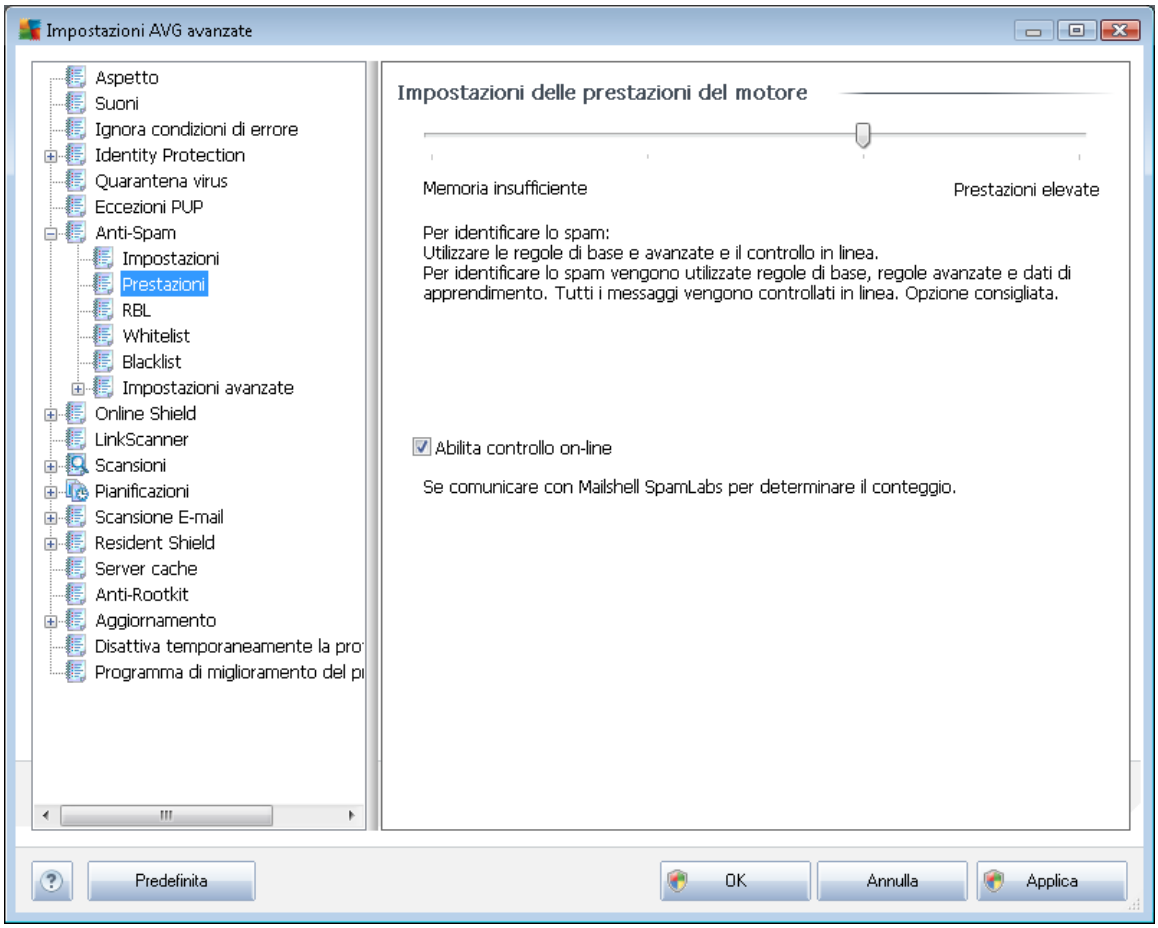
Se non si è certi dei messaggi contenuti nella cartella e si desidera che durante la procedura guidata venga richiesta una conferma per ogni singolo messaggio (al fine di determinare se utilizzarlo o meno per l'apprendimento), selezionare l'opzione ***Chiedi per ogni messaggio***.

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

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

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

9.7.2. Prestazioni



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

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

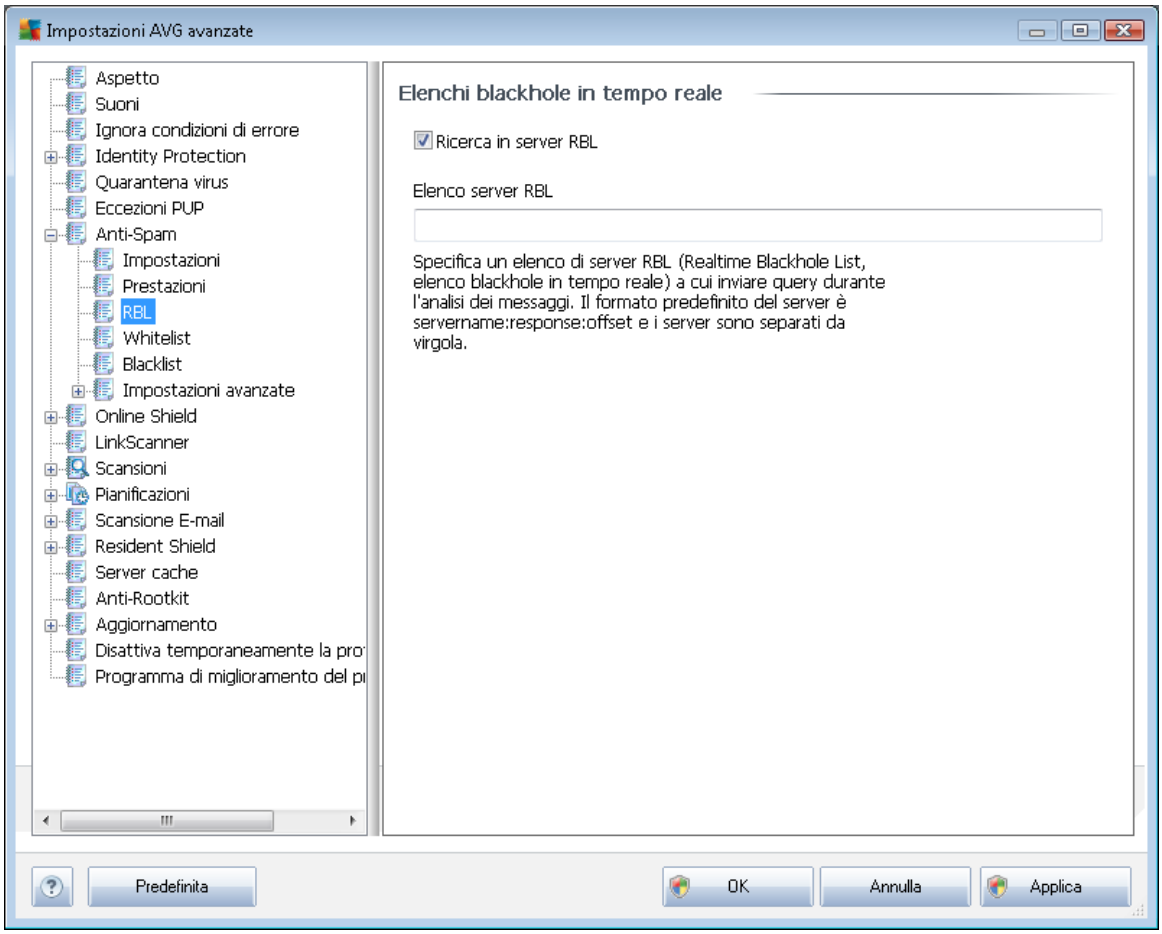
- ***Prestazioni elevate***: questa modalità richiederà una notevole quantità di memoria. Durante il processo di scansione per l'identificazione dello spam verranno utilizzate le seguenti funzionalità: regole e cache del database di spam, regole di base e avanzate, indirizzi IP e database di spammer.

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

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

9.7.3. RBL

L'elemento ***RBL*** consente di aprire una finestra di dialogo di modifica denominata ***Elenchi blackhole in tempo reale***:



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

Il server RBL (*Realtime Blackhole List, Elenchi blackhole in tempo reale*) è un server DNS con un vasto database di mittenti di spam noti. Se questa funzione è attivata, tutti i messaggi di posta elettronica verranno verificati in base al database del server RBL e verranno contrassegnati come spam se risultano identici a una delle voci nel database. I database dei server RBL contengono le impronte digitali di spam più aggiornate, per fornire il rilevamento di spam migliore e più accurato. La funzione è particolarmente utile per gli utenti che ricevono grandi quantità di messaggi di spam normalmente non rilevati dal motore Anti-Spam.

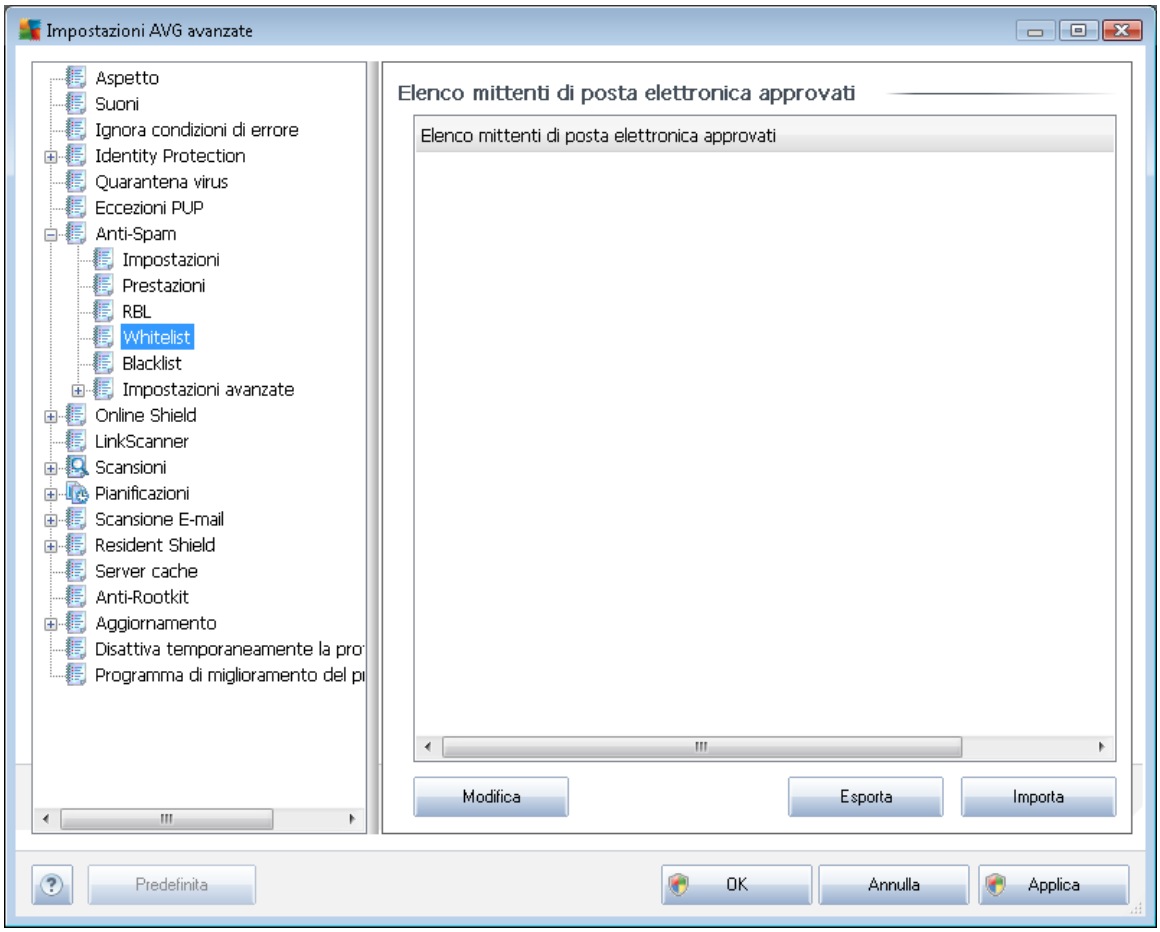
La funzione ***Elenco server RBL*** consente di definire le posizioni dei server RBL specifici.

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

Non vengono inviati dati personali al server.

9.7.4. Whitelist

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



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

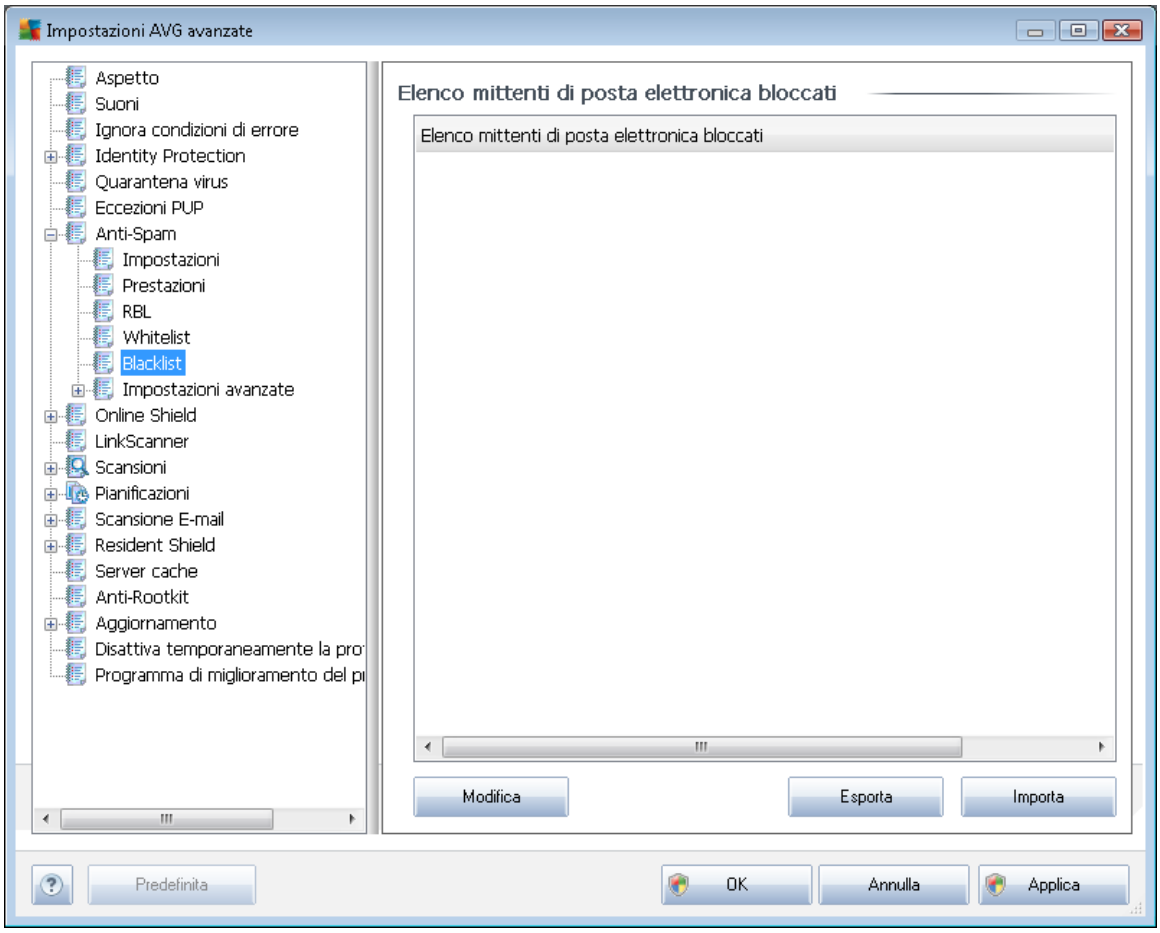
Dopo che è stato preparato l'elenco di mittenti e/o nomi di dominio, è possibile inserirli in due modi diversi: immettendo direttamente ciascun indirizzo e-mail o importando tutto l'elenco di indirizzi. Sono disponibili i seguenti pulsanti di controllo:

- ***Modifica***: selezionare questo pulsante per aprire una finestra di dialogo in cui è possibile immettere manualmente un elenco di indirizzi (*è inoltre possibile utilizzare il metodo copia e incolla*). Immettere una voce (*mittente o nome di dominio*) per riga.
- ***Esporta***: se per qualsiasi motivo si decide di esportare i record, è possibile fare clic su questo pulsante per eseguire l'operazione. Tutti i record verranno salvati in un file di testo normale.

- ***Importa***: se si possiede già un file di testo di indirizzi di posta elettronica o nomi di dominio, è possibile importare tale file selezionando questo pulsante. Il file deve includere una sola voce (*indirizzo, nome di dominio*) per riga.

9.7.5. Blacklist

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



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

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

- ***Modifica***: selezionare questo pulsante per aprire una finestra di dialogo in cui è possibile immettere manualmente un elenco di indirizzi (*è inoltre possibile utilizzare il metodo copia*

e incolla). Immettere una voce (*mittente o nome di dominio*) per riga.

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

- ***Importa***: se si possiede già un file di testo di indirizzi di posta elettronica o nomi di dominio, è possibile importare tale file selezionando questo pulsante.

9.7.6. Impostazioni avanzate

Il ramo Impostazioni avanzate contiene opzioni complete di impostazione per il componente Anti-Spam. Queste impostazioni sono destinate agli utenti esperti, in particolare agli amministratori di rete che devono eseguire una configurazione dettagliata della protezione anti-spam per garantire la massima protezione dei server e-mail. Per questo motivo non è disponibile una guida aggiuntiva nelle singole finestre di dialogo. Tuttavia, è disponibile direttamente nell'interfaccia utente una breve descrizione di ciascuna opzione.

Si consiglia di non modificare alcuna impostazione a meno che non si disponga di una conoscenza approfondita delle impostazioni avanzate di Spamcatcher (MailShell Inc.). Eventuali modifiche inappropriate possono dare luogo a una riduzione delle prestazioni o a un funzionamento errato del componente.

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

- ***Cache***: impronte digitali, reputazione dominio, LegitRepute

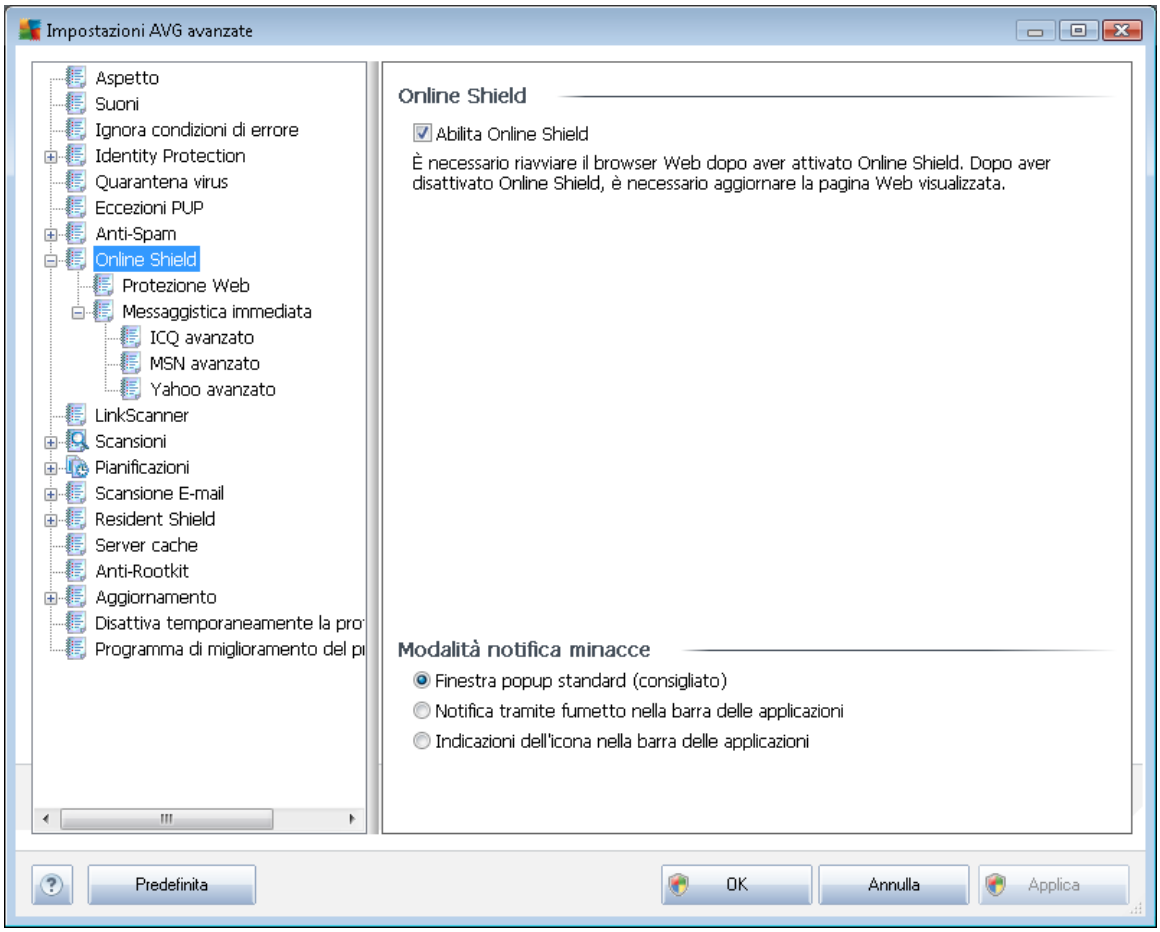
- ***Apprendimento***: numero massimo di parole, soglia di apprendimento automatico, peso

- ***Filtraggio***: elenco lingue, elenco paesi, IP approvati, IP bloccati, paesi bloccati, set di caratteri bloccati, mittenti contraffatti

- ***RBL***: server RBL, multihit, soglia, timeout, IP massimi

- ***Connessione Internet***: timeout, server proxy, autenticazione proxy

9.8. Online Shield



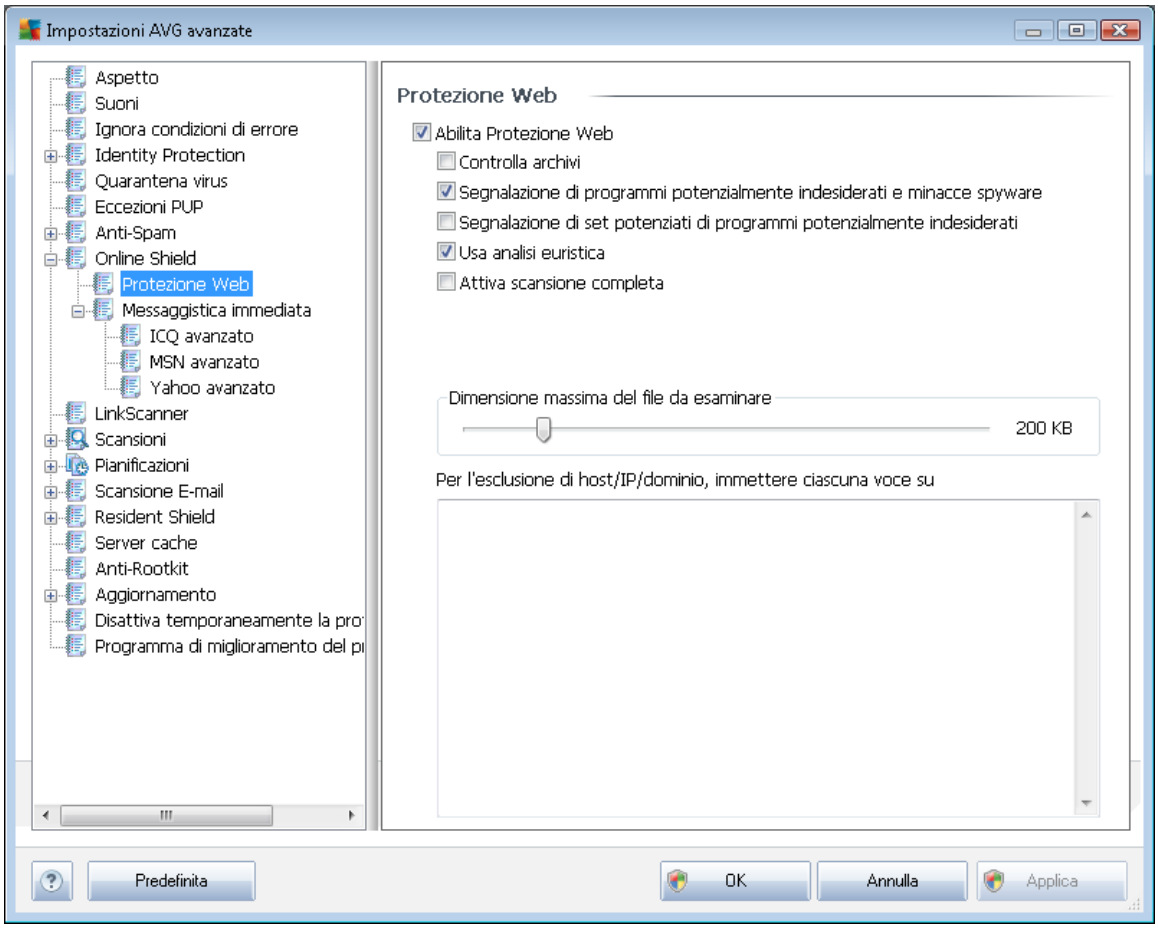
La finestra di dialogo ***Online Shield*** consente di attivare/disattivare completamente il componente ***Online Shield*** tramite l'opzione ***Abilita Online Shield*** (*attivata per impostazione predefinita*). Per altre impostazioni avanzate del componente passare alle finestre di dialogo successive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

9.8.1. Protezione Web



La finestra di dialogo ***Protezione Web*** consente di modificare la configurazione del componente relativamente 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*** (*disattivata per impostazione predefinita*): consente di eseguire la scansione del contenuto di eventuali 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*** (

disattivata per impostazione predefinita): selezionare questa casella di controllo 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.

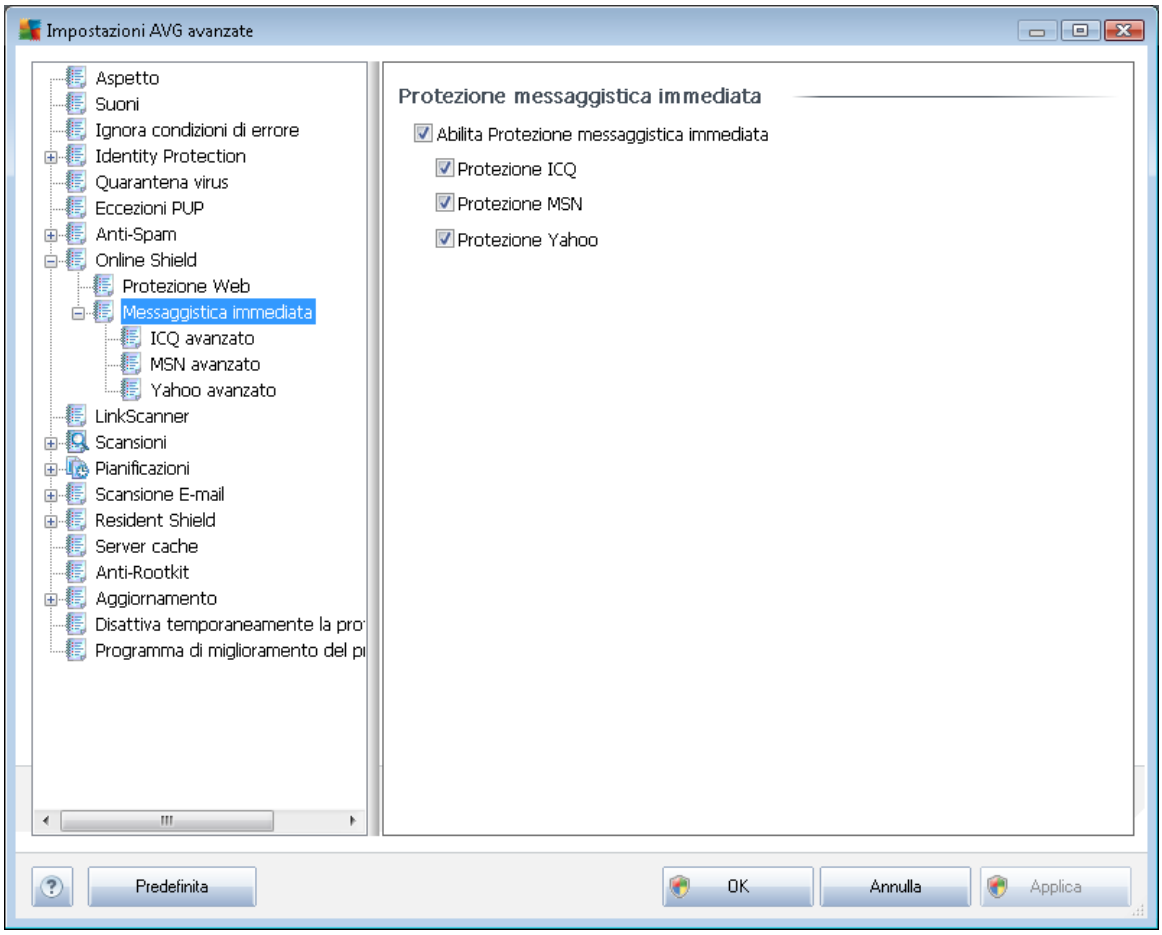
- ***Usa analisi euristica*** (*attivata per impostazione predefinita*): consente di eseguire la scansione del contenuto della pagina da visualizzare utilizzando il metodo dell'analisi euristica (*emulazione dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale*).

- ***Attiva scansione completa*** (*disattivata per impostazione predefinita*): in situazioni specifiche (*ad esempio se si sospetta che il computer sia stato infettato*) per maggiore sicurezza è possibile selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno anche le aree del computer che difficilmente vengono infettate. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.

- ***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.

9.8.2. Messaggistica immediata

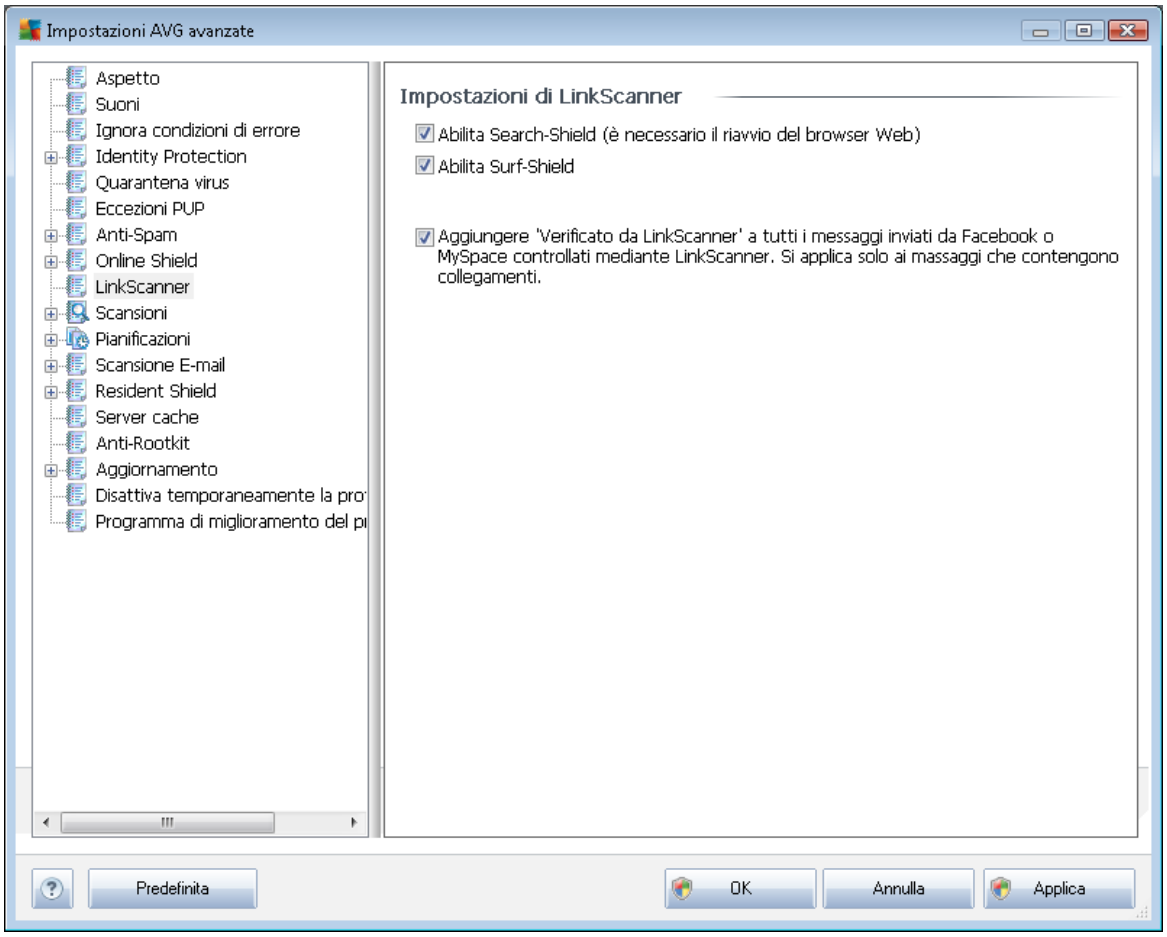


Nella finestra di dialogo ***Protezione messaggistica immediata*** è possibile modificare le impostazioni dei componenti di ***Online Shield*** che si riferiscono alla scansione della messaggistica immediata. Attualmente sono supportati tre programmi di messaggistica immediata: ***ICQ***, ***MSN*** e ***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*).

9.9. Link Scanner

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



- ***Abilita Search-Shield*** (*attivata per impostazione predefinita*): icone informative relative ai siti restituiti dalle ricerche eseguite in Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg o SlashDot il cui contenuto è stato precedentemente controllato.

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

- ***Aggiungere "Verificato da AVG LinkScanner"...***: selezionare questa voce per confermare che si desidera inserire un avviso di certificazione relativo al controllo ***Link Scanner*** in tutti i messaggi contenenti collegamenti ipertestuali attivi inviati dai social network Facebook e MySpace.

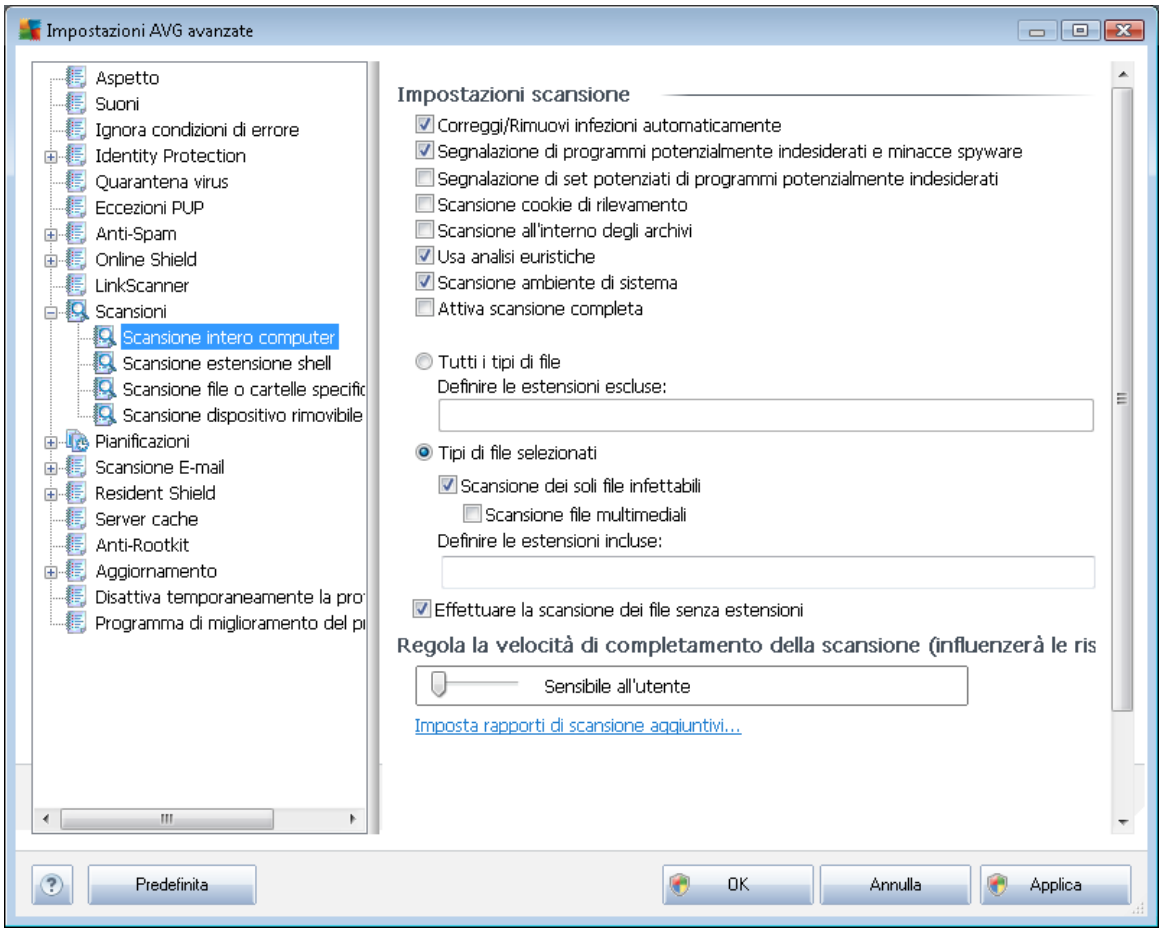
9.10. Scansioni

La sezione delle impostazioni di scansione avanzate è suddivisa in quattro categorie che fanno riferimento a specifici tipi di scansione definiti dal fornitore 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

9.10.1. Scansione intero computer

L'opzione ***Scansione intero computer*** consente di modificare i parametri di una delle scansioni predefinite dal fornitore del 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*** (*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, 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*** (*disattivata per impostazione predefinita*): selezionare questa casella di controllo 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*** (*disattivata per impostazione predefinita*): 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*** (*disattivata per impostazione predefinita*): 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*** (*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.

- ***Attiva scansione completa*** (*disattivata per impostazione predefinita*): in situazioni specifiche (*ad esempio se si sospetta che il computer sia stato infettato*) per maggiore sicurezza è possibile selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno anche le aree del computer che difficilmente vengono infettate. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.

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.

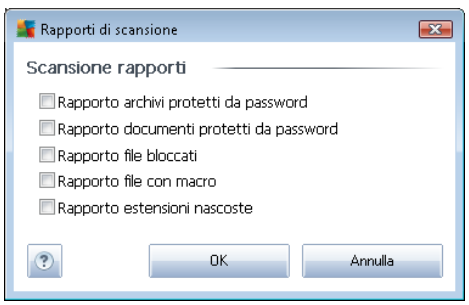
- Facoltativamente, è possibile sottoporre a scansione i file senza estensione tramite ***Effettuare la scansione dei file senza estensioni***: questa opzione è attivata per impostazione predefinita e si consiglia di non modificare questa impostazione a meno che non siano presenti motivi validi per farlo.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

Regola la velocità di completamento della scansione

All'interno della sezione ***Regola la velocità di completamento della 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 *sensibile all'utente* per l'utilizzo automatico delle risorse. Se si desidera aumentare la velocità della scansione, il tempo impiegato sarà inferiore ma l'utilizzo delle risorse di sistema aumenterà notevolmente durante l'esecuzione e rallenterà le altre attività svolte 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.

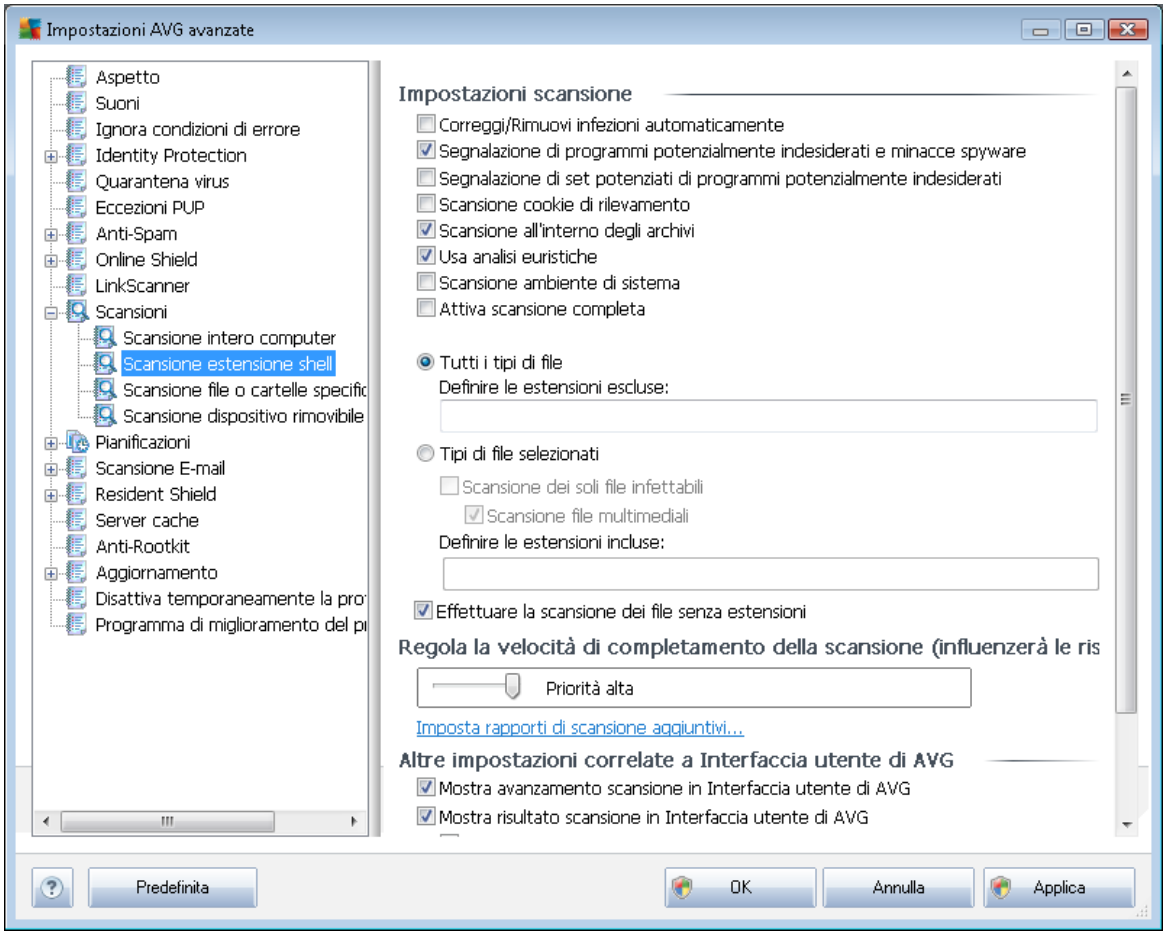
Imposta rapporti di scansione aggiuntivi...

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:



9.10.2. 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 del 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***:



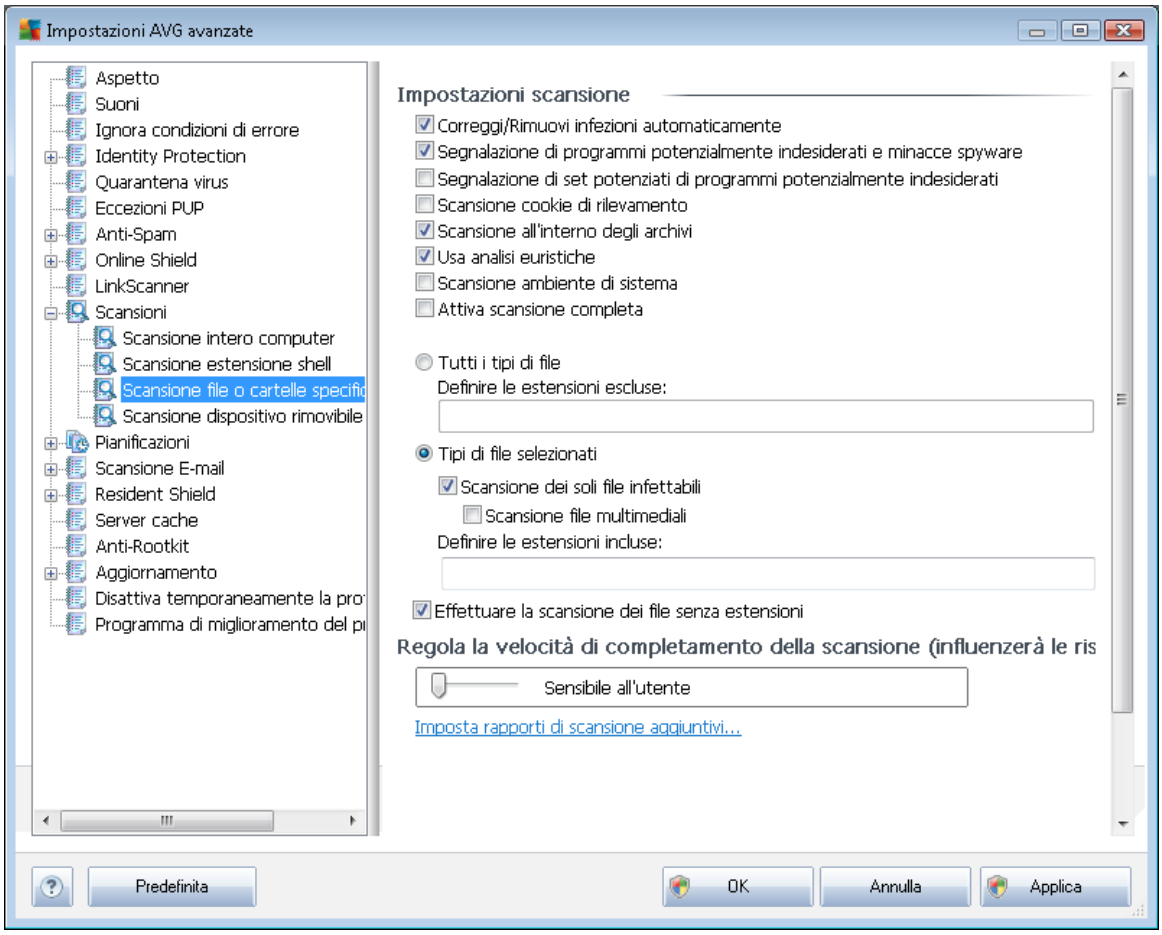
L'elenco dei parametri è identico a quello disponibile per ***Scansione intero computer***. Tuttavia, le impostazioni predefinite sono diverse (*ad esempio, per impostazione predefinita Scansione intero computer non controlla gli archivi ma esamina l'ambiente di sistema, viceversa per Scansione estensione shell*).

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

Rispetto alla finestra di dialogo ***Scansione intero computer***, la finestra di dialogo ***Scansione estensione shell*** include inoltre la sezione denominata ***Altre impostazioni correlate all'Interfaccia utente di AVG***, in cui è possibile specificare se si desidera accedere all'avanzamento della scansione e ai risultati della scansione dall'Interfaccia utente di AVG. Inoltre, è possibile definire se il risultato della scansione deve essere visualizzato solo nel caso in cui venga rilevata un'infezione durante la scansione.

9.10.3. 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***:

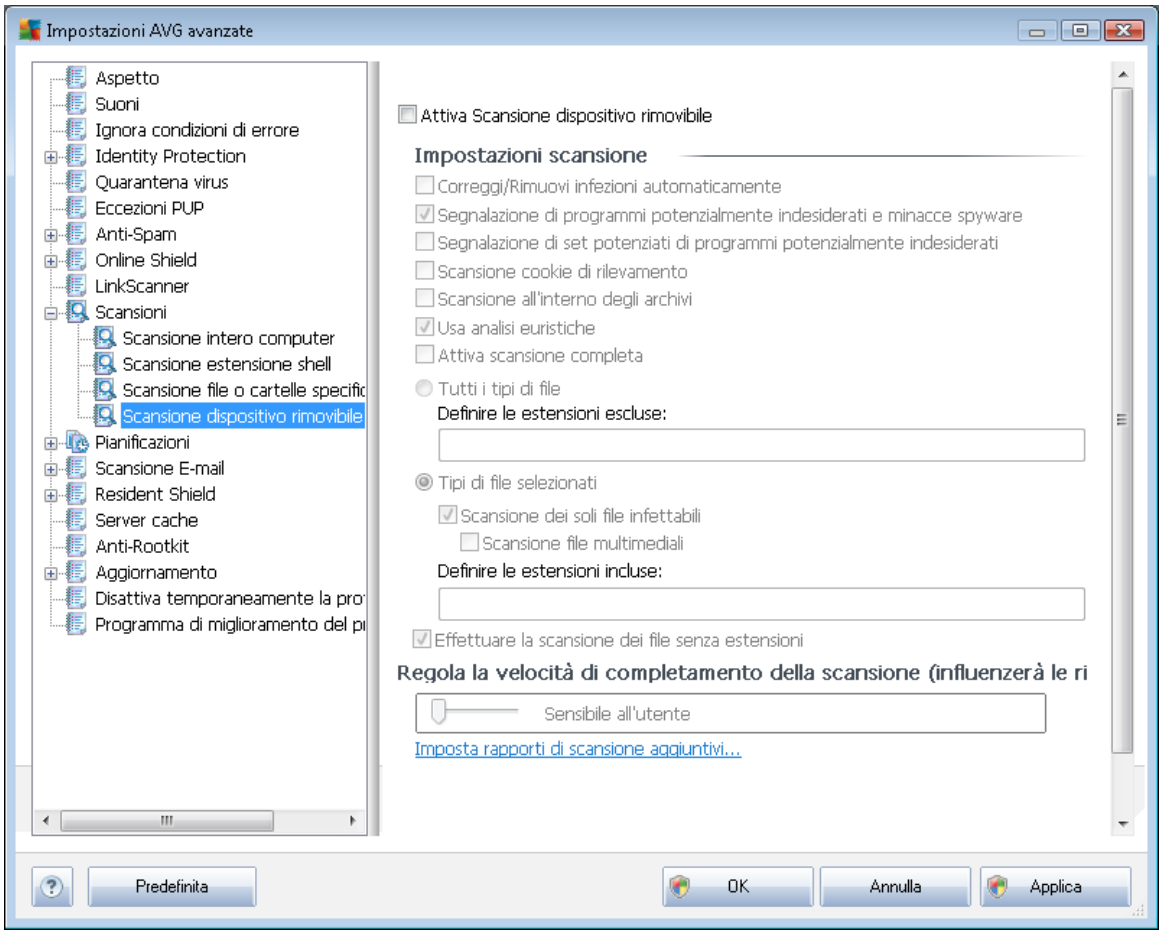


Tutti i parametri impostati in questa finestra di dialogo di configurazione si applicano solo alle aree selezionate per la scansione con il comando ***Scansione file o cartelle specifiche***!

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

9.10.4. 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****.*

9.11. Pianificazioni

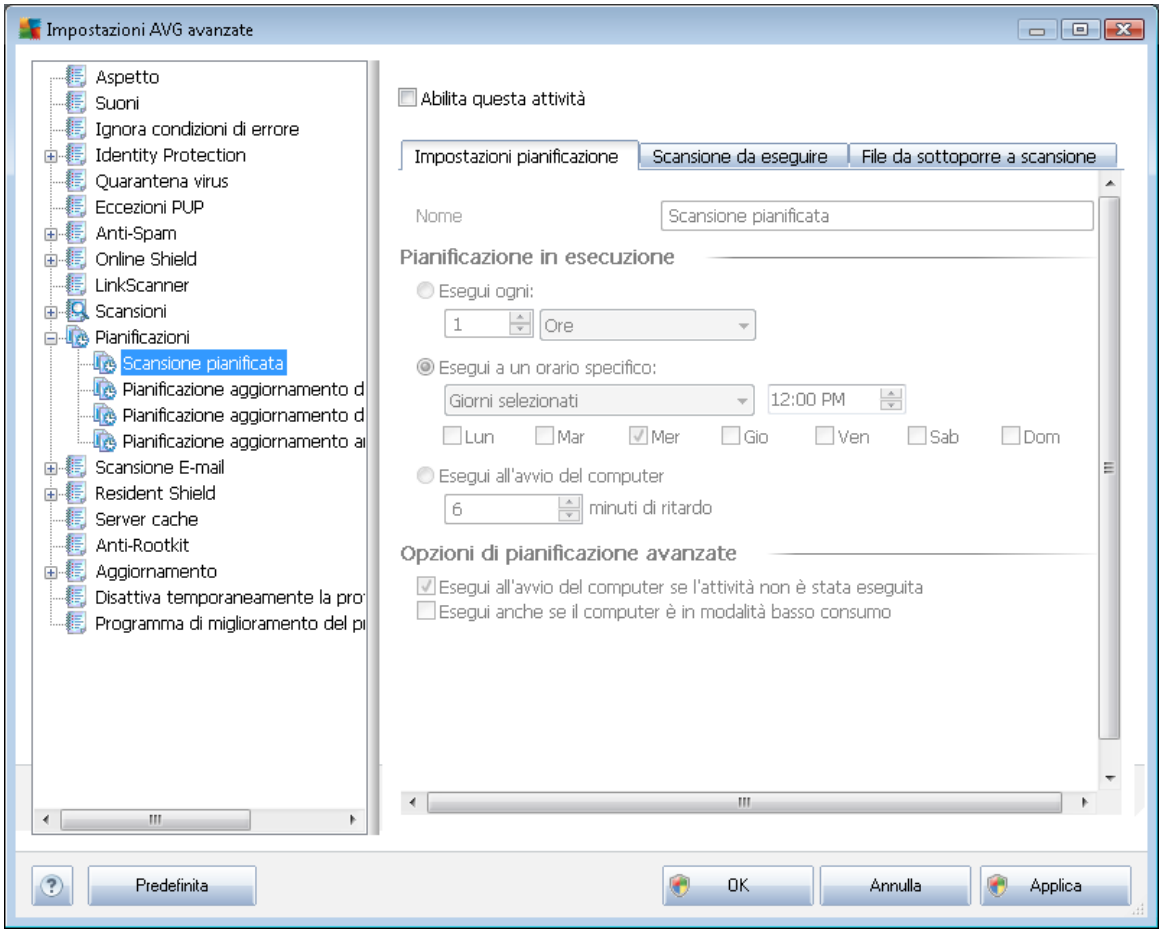
Nella sezione ***Pianificazioni*** è possibile modificare le impostazioni predefinite di:

- Scansione pianificata

- Pianificazione aggiornamento del database di virus
- Pianificazione aggiornamento del programma
- Pianificazione aggiornamenti Anti-Spam

9.11.1. Scansione pianificata

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

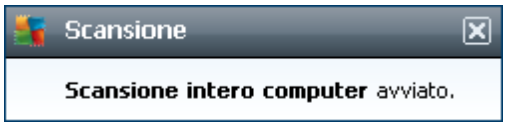
Pianificazione in esecuzione

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***).

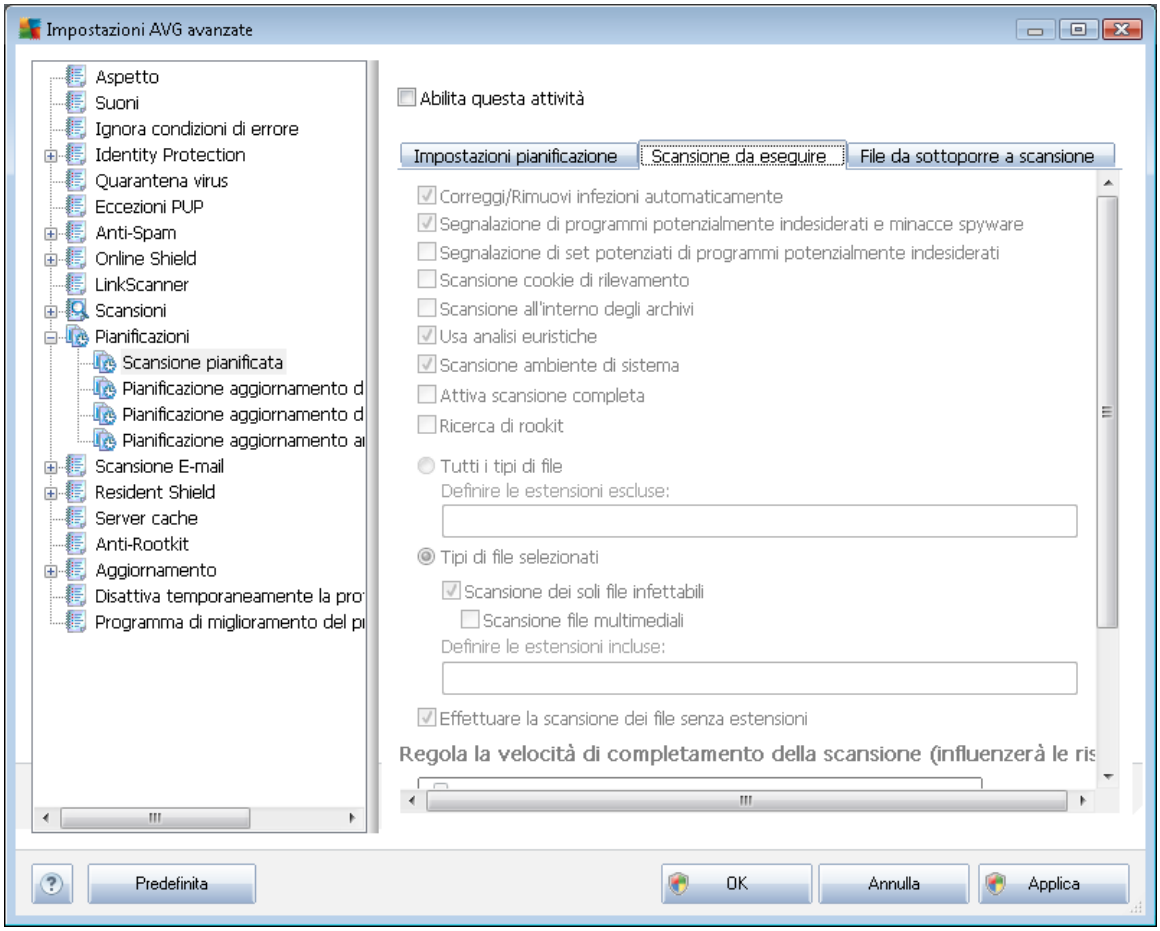
Opzioni di pianificazione avanzate

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 luce lampeggiante*) per comunicare che è in corso una scansione pianificata. Fare clic con il pulsante destro del mouse sull'icona AVG della scansione in esecuzione per aprire un menu di scelta rapida in cui è possibile decidere se sospendere o arrestare la scansione in esecuzione, nonché modificarne la priorità:



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 non esista un motivo valido 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, 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*** (*disattivata per impostazione predefinita*): selezionare questa casella di controllo 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*** (*disattivata 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*** (*disattivata 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.

- ***Attiva scansione completa*** (*disattivata per impostazione predefinita*): in situazioni specifiche (*ad esempio se si sospetta che il computer sia stato infettato*) per maggiore sicurezza è possibile selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno anche le aree del computer che difficilmente vengono infettate. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.

- ***Ricerca di rootkit*** (*disattivata per impostazione predefinita*): 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.

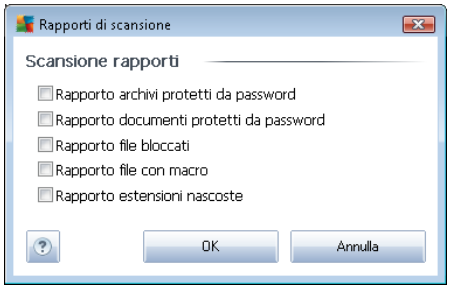
- Facoltativamente, è possibile sottoporre a scansione i file senza estensione tramite ***Effettuare la scansione dei file senza estensioni***: questa opzione è attivata per impostazione predefinita e si consiglia di non modificare questa impostazione a meno che non siano presenti motivi validi per farlo.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

Regola la velocità di completamento della scansione

All'interno della sezione ***Regola la velocità di completamento della 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 *sensibile all'utente* per l'utilizzo automatico delle risorse. Se si desidera aumentare la velocità della scansione, il tempo impiegato sarà inferiore ma l'utilizzo delle risorse di sistema aumenterà notevolmente durante l'esecuzione e rallenterà le altre attività svolte 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

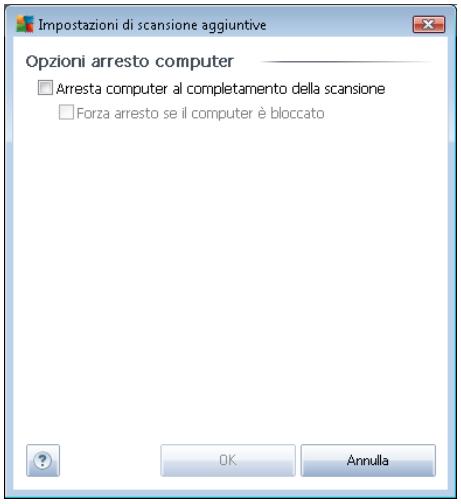
Fare clic sul collegamento ***Imposta rapporti di scansione aggiuntivi...*** per aprire una finestra di dialogo autonoma denominata ***Rapporti di scansione*** in cui è possibile selezionare diversi elementi per definire i tipi di rilevamenti da segnalare:

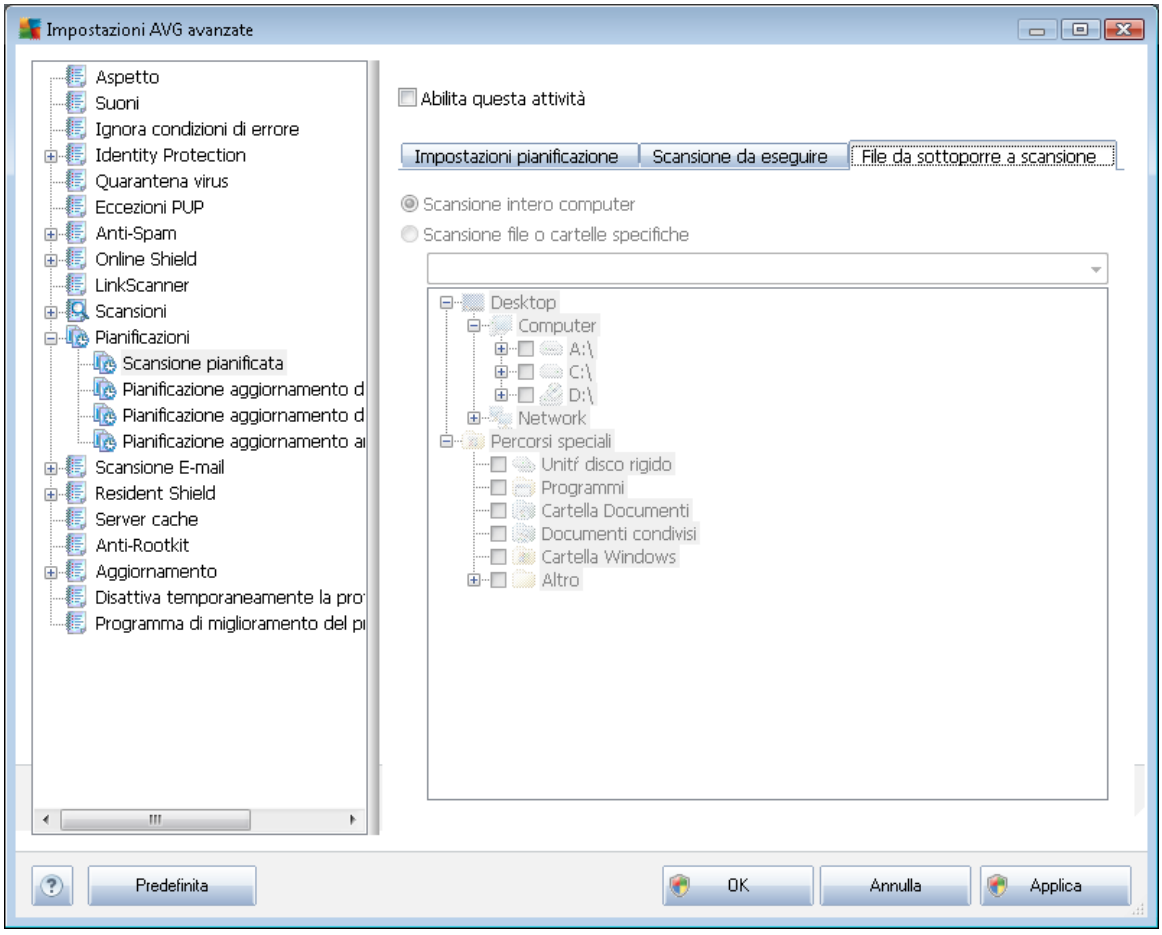


Impostazioni di scansione aggiuntive

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***).

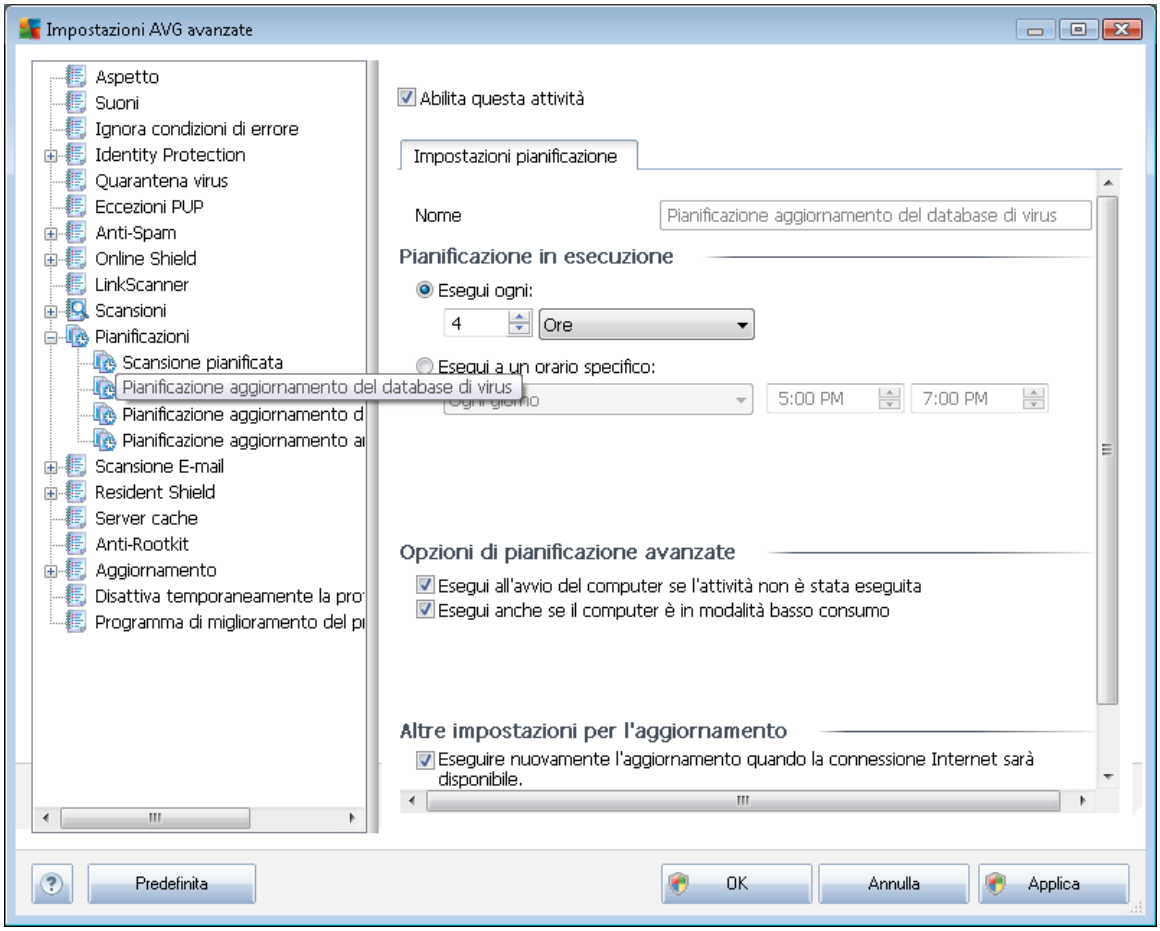




Nella scheda ***File da sottoporre a scansione*** è possibile definire se si desidera pianificare la scansione dell'intero computer o la scansione di file o cartelle specifiche. Se si seleziona la scansione di file o cartelle specifiche, nella parte inferiore di questa finestra di dialogo viene attivata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

9.11.2. Pianificazione dell'aggiornamento del database dei virus

Se ***realmente necessario***, è possibile deselezionare la voce ***Abilita questa attività*** per disattivare temporaneamente l'aggiornamento del database dei virus pianificato e attivarlo nuovamente in seguito:



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.

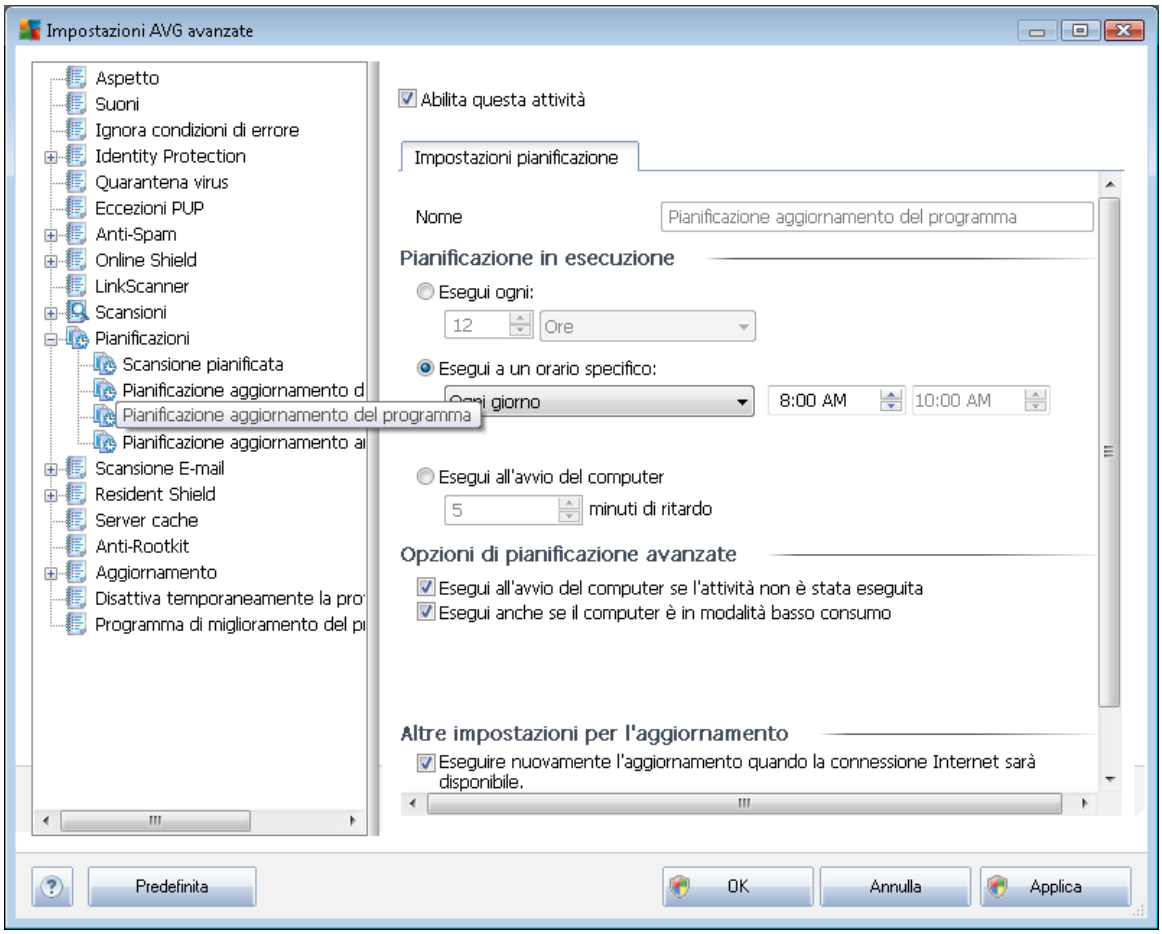
Altre impostazioni per l'aggiornamento

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***).

9.11.3. Pianificazione dell'aggiornamento del programma

Se ***realmente necessario***, è possibile deselezionare la voce ***Abilita questa attività*** per disattivare temporaneamente l'aggiornamento del programma pianificato e attivarlo nuovamente in seguito:



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

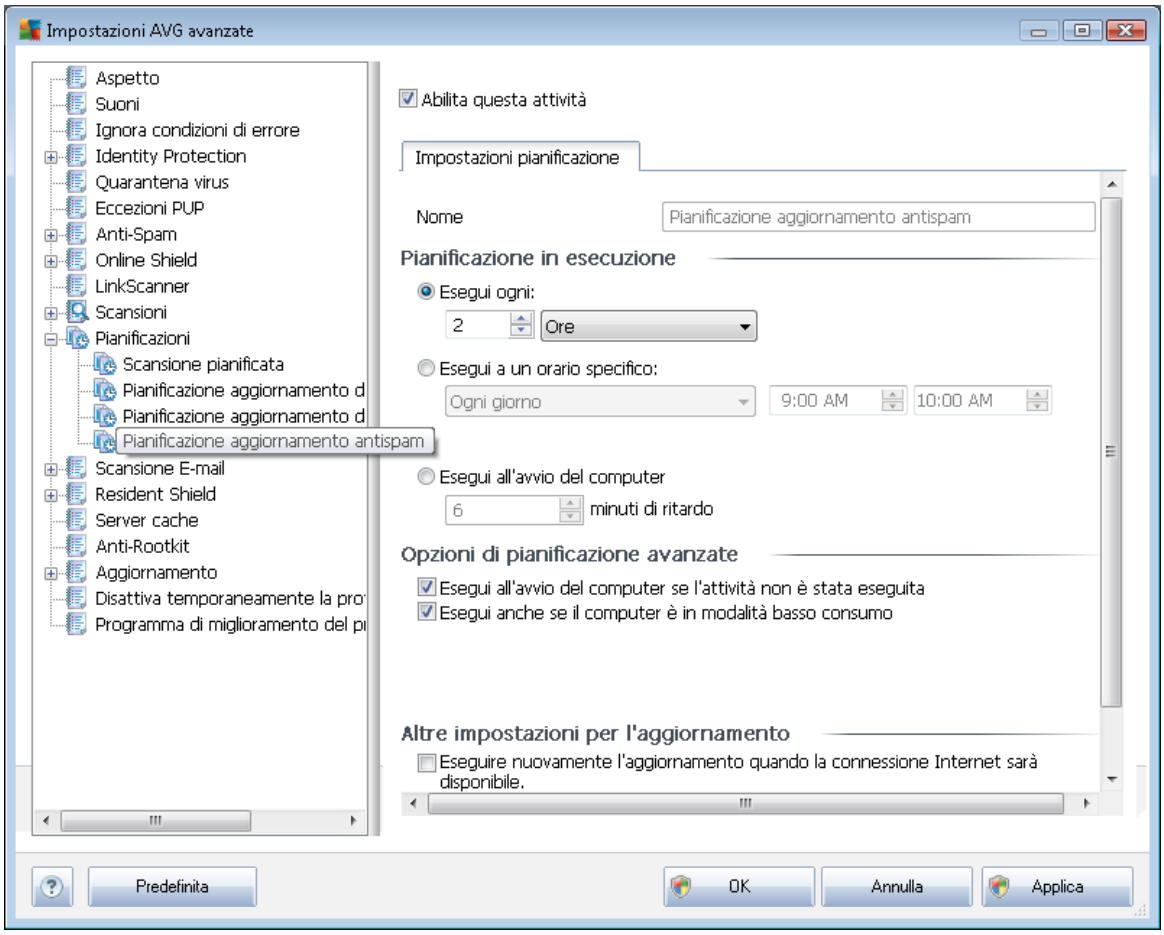
Selezionare l'opzione ***Eseguire nuovamente l'aggiornamento quando la connessione Internet sarà disponibile*** per assicurarsi che, se la connessione Internet si interrompesse e il processo di aggiornamento non riuscisse, tale processo venga avviato di nuovo subito dopo il ripristino della connessione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

9.11.4. Pianificazione aggiornamenti Anti-Spam

Se ***realmente necessario***, è possibile deselezionare la voce ***Abilita questa attività*** per disattivare temporaneamente l'***aggiornamento*** Anti-Spam pianificato e attivarlo nuovamente in seguito:



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

Questa sezione consente di specificare gli intervalli di tempo per l'avvio dell'aggiornamento ***Anti-Spam*** che è stato pianificato. È possibile definire l'ora in base all'avvio ripetuto dell'aggiornamento ***Anti-Spam***dopo un certo periodo di tempo (***Esegui ogni...***) oppure specificando data e ora esatte (***Esegui a un orario specifico...***) oppure specificando 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 essere avviato o non avviato l'aggiornamento ***Anti-Spam***se il computer si trova in modalità basso consumo oppure se è completamente spento.

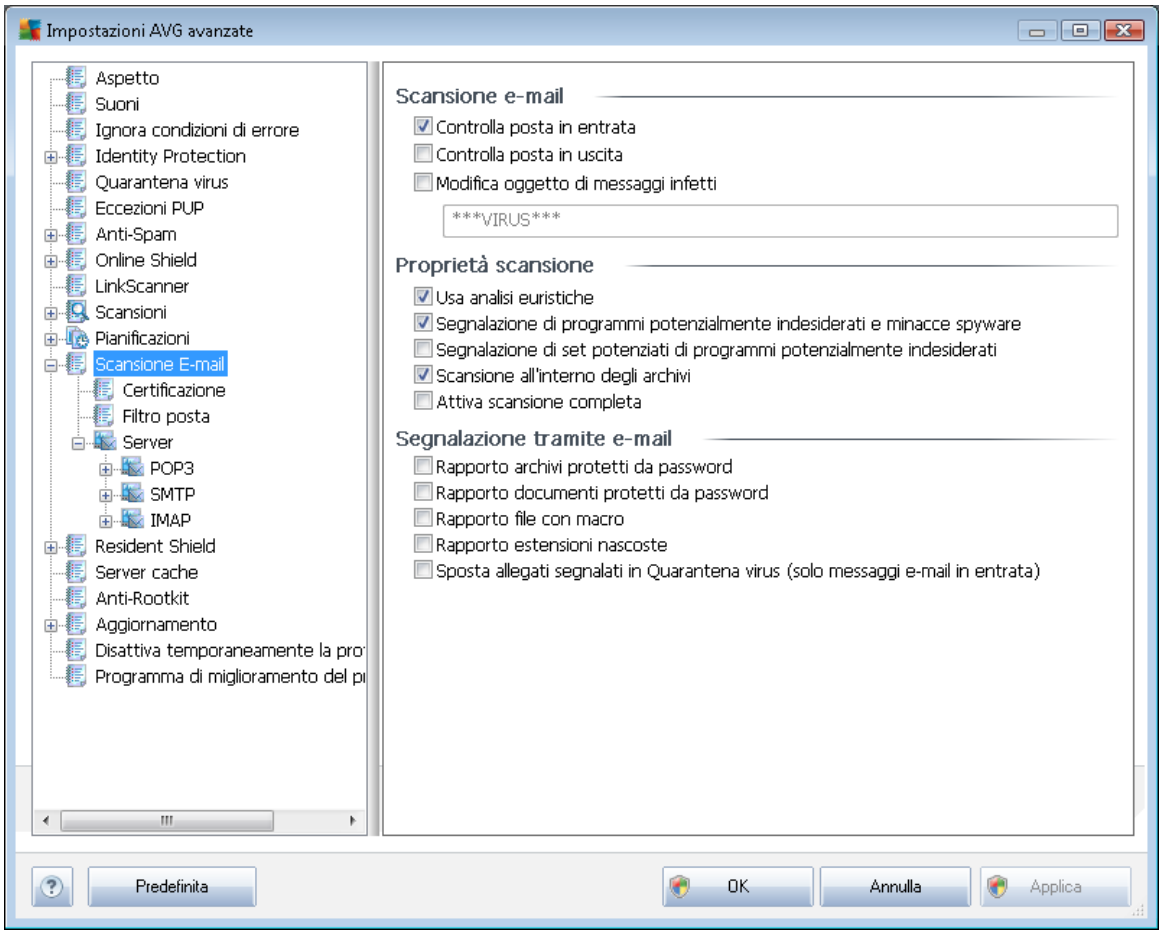
Altre impostazioni per l'aggiornamento

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 ***Anti-Spam***non riuscisse, tale processo venga avviato di nuovo subito dopo il ripristino della connessione Internet.

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

9.12. 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:

- ***Controlla posta in entrata*** (*attivata per impostazione predefinita*): selezionare per attivare/disattivare l'opzione di scansione di tutti i messaggi e-mail consegnati al client e-mail
- ***Controlla posta in uscita*** (*disattivata per impostazione predefinita*): selezionare per attivare/disattivare l'opzione di scansione di tutti i messaggi e-mail inviati dall'account e-mail
- ***Modifica oggetto di messaggi infetti*** (*disattivata per impostazione predefinita*): per essere informati del fatto che il messaggio e-mail esaminato si è rivelato infetto, selezionare questa voce e immettere il testo desiderato nel campo di testo. Il testo verrà aggiunto al campo "Oggetto" di ogni messaggio rilevato come infetto per facilitarne l'identificazione e il filtro. Il valore predefinito è ***VIRUS***. Si consiglia di mantenere questa impostazione.

Proprietà scansione

In questa sezione è possibile specificare la modalità di scansione dei messaggi e-mail:

- ***Usa analisi euristiche*** (*attivata per impostazione predefinita*): selezionare questa casella di controllo per utilizzare il metodo di rilevamento tramite 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*** (*disattivata per impostazione predefinita*): selezionare questa casella di controllo 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*** (*attivata per impostazione predefinita*): selezionare questa casella di controllo per eseguire la scansione del contenuto degli archivi allegati ai messaggi e-mail.
- ***Attiva scansione completa*** (*disattivata per impostazione predefinita*): in situazioni specifiche (*ad esempio se si sospetta che il computer sia stato infettato da un virus o un exploit*) per maggiore sicurezza è possibile selezionare questa opzione per attivare gli

algoritmi di scansione più completi che esamineranno anche le aree del computer che difficilmente vengono infettate. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.

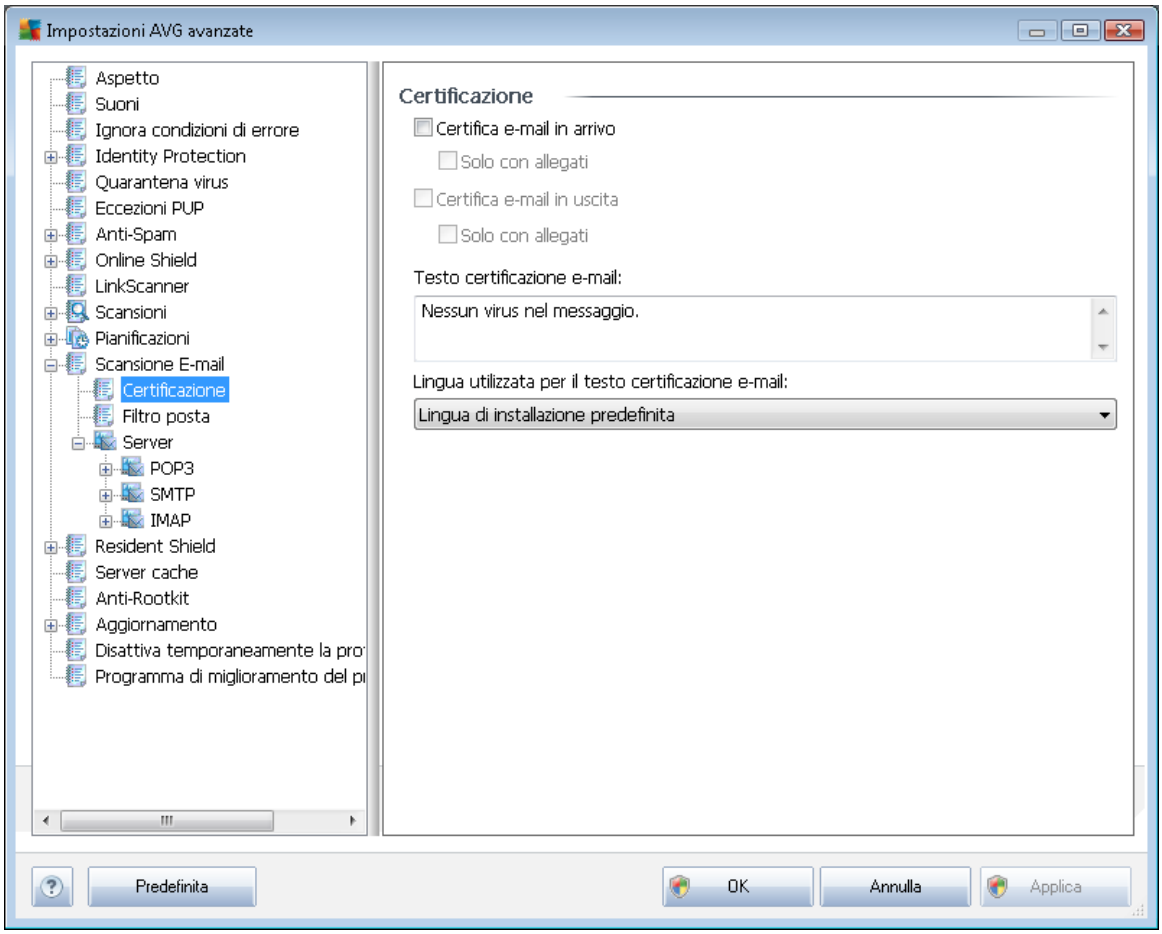
Segnalazione allegati e-mail

In questa sezione, è possibile impostare rapporti 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 archivi protetti da password***: gli archivi (*ZIP, RAR e così via*) protetti da password non possono essere sottoposti alla scansione antivirus. 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 alla scansione antivirus. 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 eseguibile sospetto, ad esempio "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***.

9.12.1. Certificazione

Nella finestra di dialogo ***Certificazione*** è possibile specificare il testo e la lingua della certificazione per i messaggi e-mail in ingresso e in uscita:



Il testo della certificazione include due parti: la parte dell'utente e la parte del sistema. Vedere il seguente esempio: la prima riga rappresenta la parte dell'utente, il resto viene generato automaticamente:

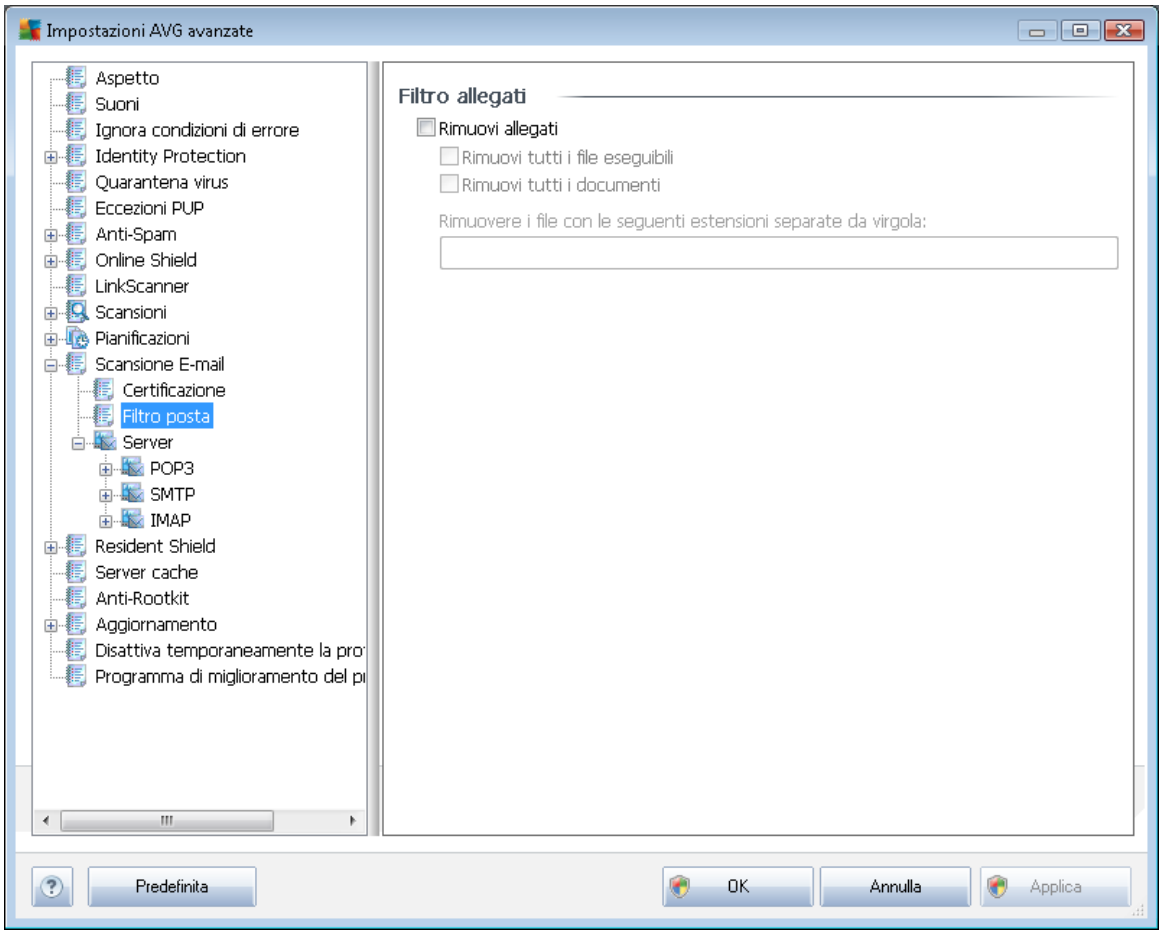
Nessun virus nel messaggio.

Controllato da AVG.

Versione: x.y.zz / Database dei virus: xx.y.z - Data di rilascio: 12/9/2010

Se si decide di utilizzare la certificazione dei messaggi e-mail in ingresso e in uscita, in questa finestra di dialogo è possibile specificare il contenuto della parte del testo di certificazione dell'utente (***Testo certificazione e-mail***) e scegliere la lingua da utilizzare per la parte di certificazione generata automaticamente dal sistema (***Lingua utilizzata per il testo certificazione e-mail***).

9.12.2. Filtro posta

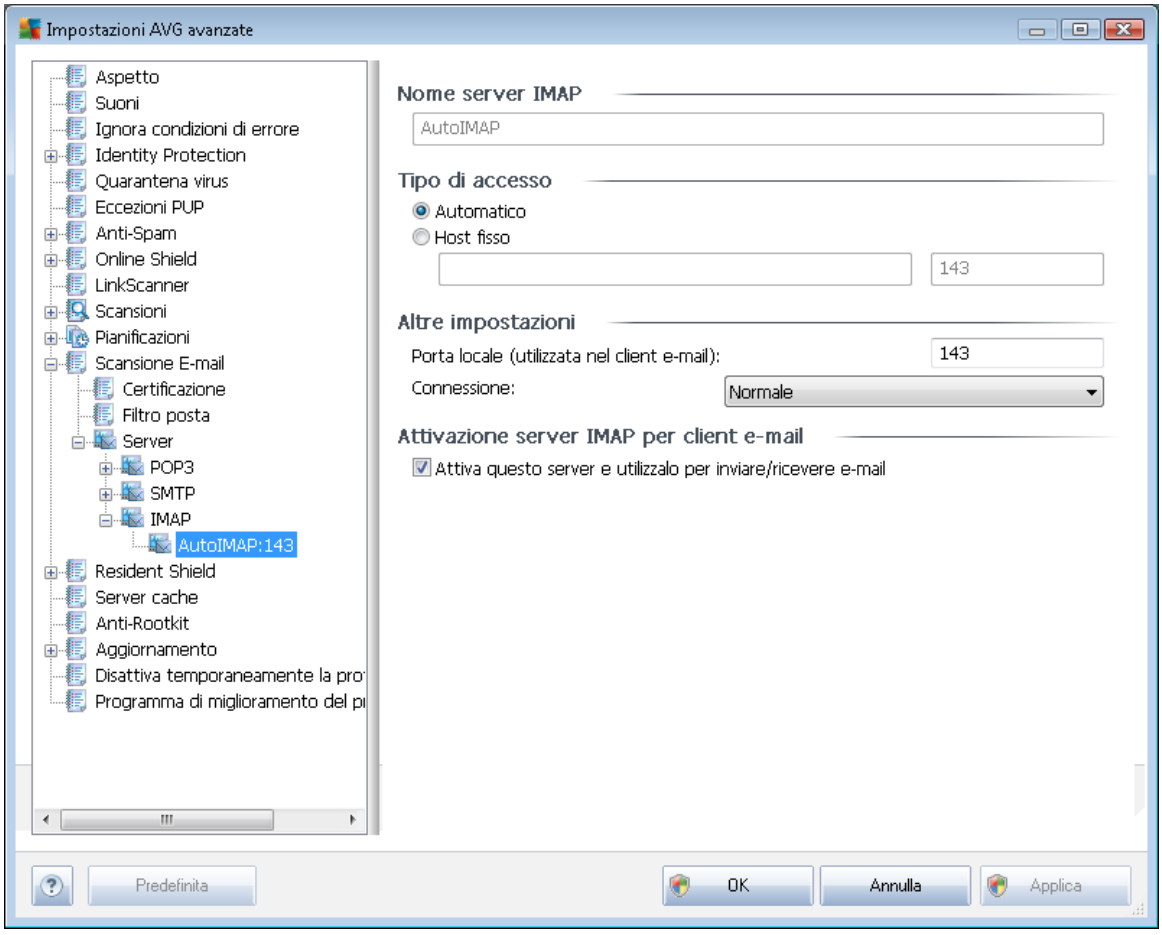


La finestra di dialogo ***Filtro allegati*** consente di impostare i parametri per la scansione degli allegati dei messaggi e-mail. Per impostazione predefinita, l'opzione ***Rimuovi allegati*** è disattivata. Se si decide di attivarla, tutti gli allegati dei messaggi e-mail rilevati come infetti o potenzialmente 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

9.12.3. 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***: in questo campo è possibile specificare il nome dei nuovi server aggiunti (*per aggiungere un server POP3, fare clic con il pulsante destro del mouse sulla voce POP3 nel menu di esplorazione a sinistra*). Per i server "AutoPOP3" creati automaticamente questo campo è disattivato.

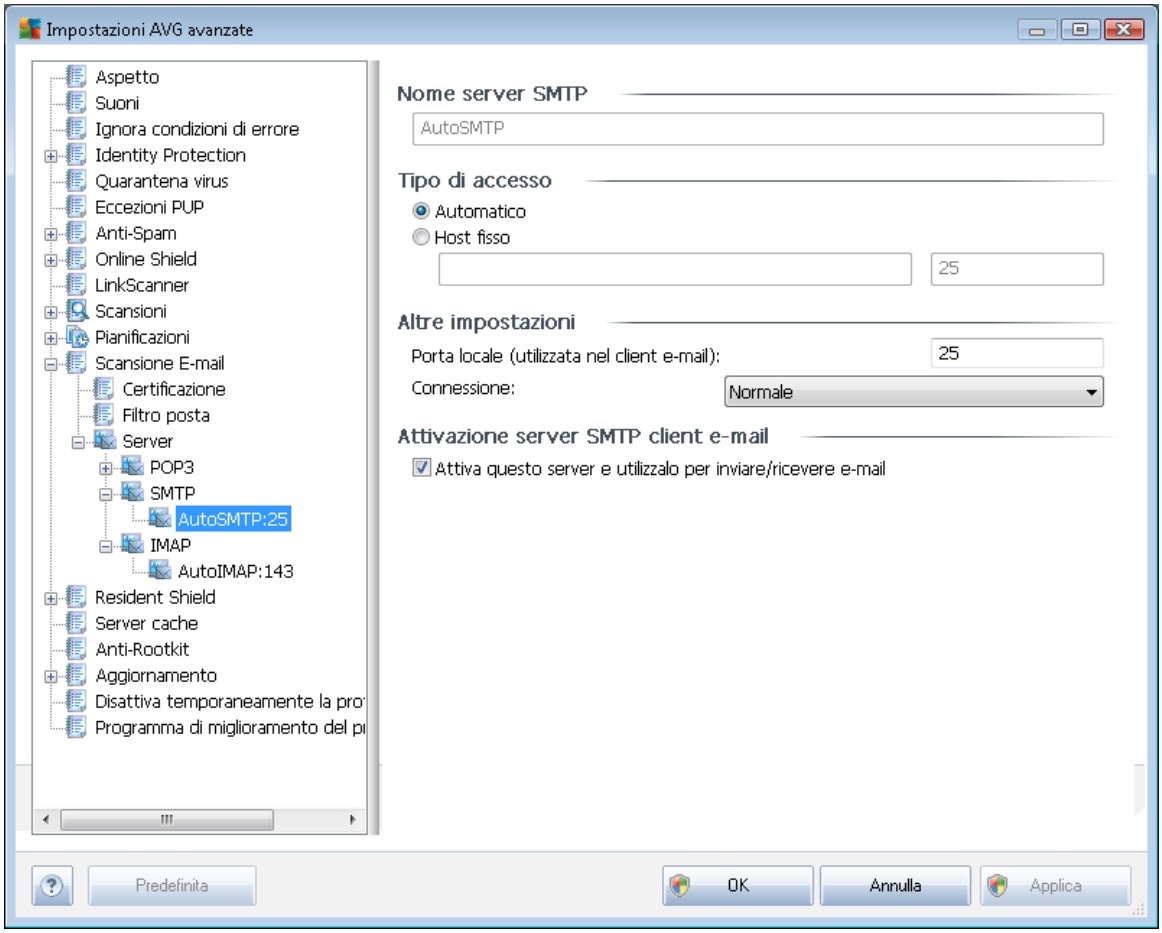
- ***Tipo di accesso***: definisce il metodo per determinare il server e-mail utilizzato per la posta in entrata:

    - o ***Automatico***: l'accesso verrà effettuato automaticamente, in base alle impostazioni del client e-mail.

    - o ***Host fisso***: in questo caso verrà sempre utilizzato il server specificato in questo campo. Specificare l'indirizzo o il nome del server e-mail. 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 e-mail 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 e-mail sarà quindi necessario specificare tale porta come porta per la comunicazione POP3.
  - ***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 terzi. Questa funzionalità inoltre è disponibile solo se supportata dal server e-mail di destinazione.
- ***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 di ***Scansione E-mail*** che utilizza il protocollo SMTP per la posta in uscita:

- ***Nome server SMTP***: in questo campo è possibile specificare il nome dei nuovi server aggiunti (*per aggiungere un server SMTP, fare clic con il pulsante destro del mouse sulla voce SMTP nel menu di esplorazione a sinistra*). Per i server "AutoSMTP" creati automaticamente questo campo è disattivato.

- ***Tipo di accesso***: definisce il metodo per determinare il server e-mail utilizzato per la posta in uscita:

    - ***Automatico***: l'accesso verrà effettuato automaticamente, in base alle impostazioni del client e-mail

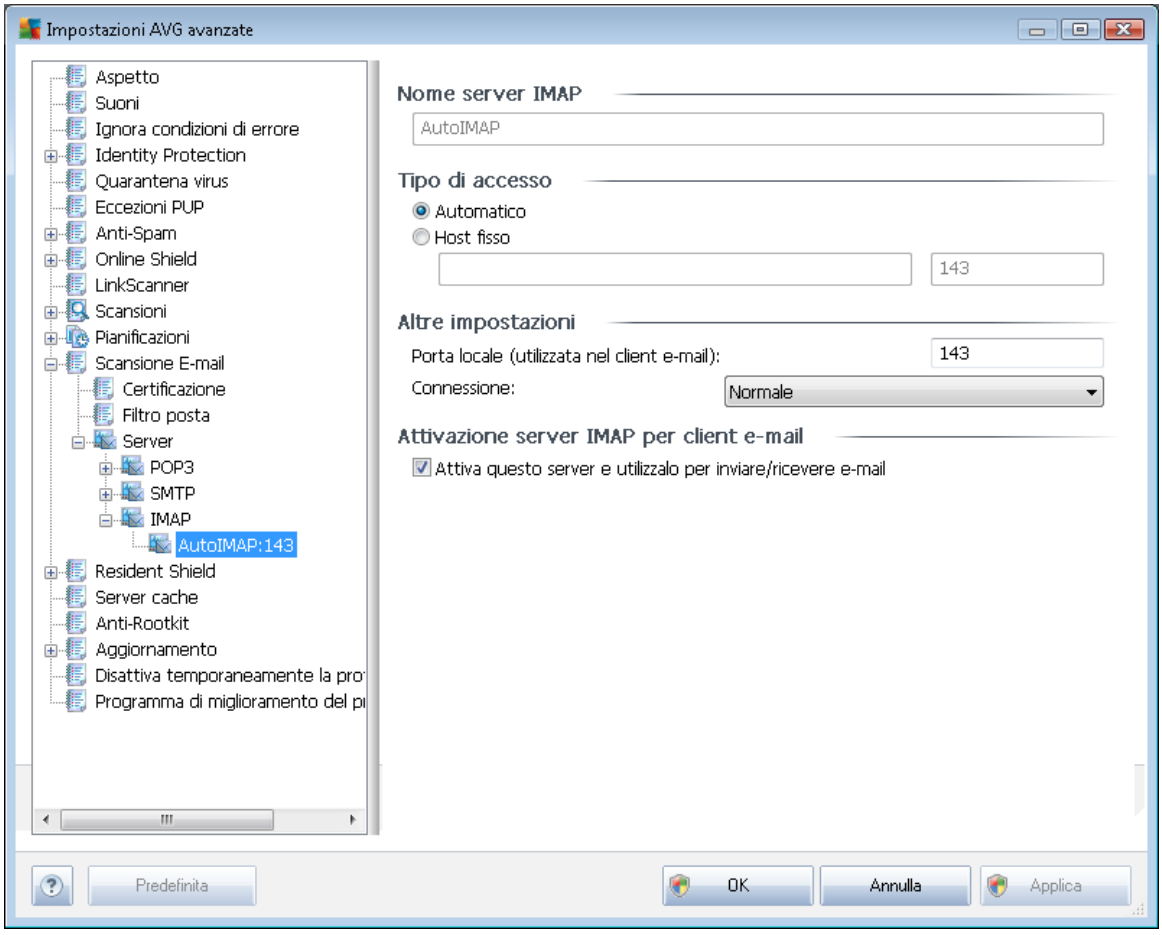
    - ***Host fisso***: in questo caso verrà sempre utilizzato il server specificato in questo campo. Specificare l'indirizzo o il nome del server e-mail. Per il nome, è possibile utilizzare un nome di dominio (*ad esempio imap.acme.com*) o un indirizzo IP (*ad esempio 123.45.67.89*). Se il server e-mail 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 e-mail sarà quindi necessario specificare tale porta come porta per la comunicazione SMTP.

    - ***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 terzi. Questa funzionalità è disponibile solo se supportata dal server e-mail di destinazione.

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



Questa finestra di dialogo (accessibile tramite ***Server / IMAP***) consente di impostare un nuovo server ***Scansione E-mail*** che utilizza il protocollo IMAP per la posta in uscita:

- ***Nome server IMAP***: in questo campo è possibile specificare il nome dei nuovi server aggiunti (*per aggiungere un server IMAP, fare clic con il pulsante destro del mouse sulla voce IMAP nel menu di esplorazione a sinistra*). Per i server "AutoIMAP" creati automaticamente questo campo è disattivato.

- ***Tipo di accesso***: definisce il metodo per determinare il server e-mail utilizzato per la posta in uscita:

    - ***Automatico***: l'accesso verrà effettuato automaticamente, in base alle impostazioni del client e-mail

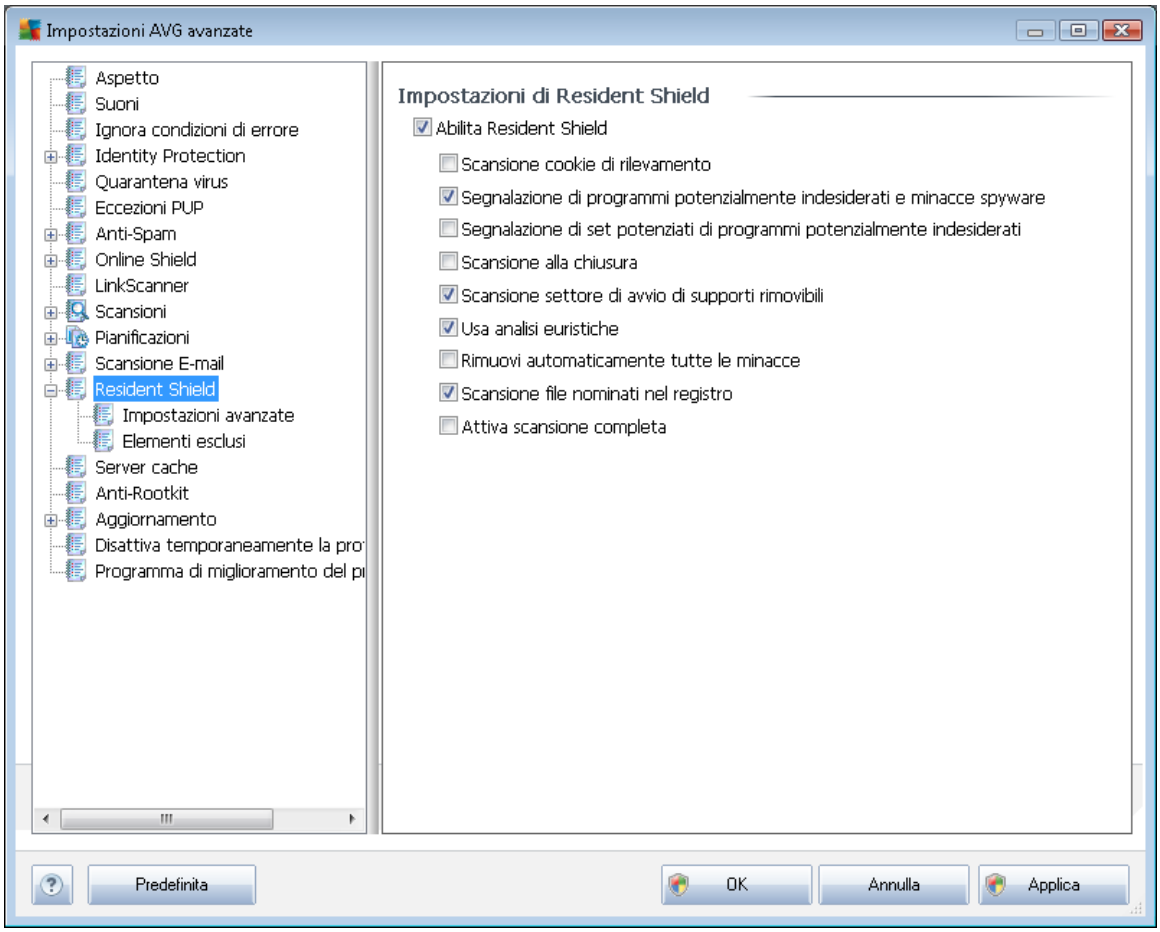
    - ***Host fisso***: in questo caso verrà sempre utilizzato il server specificato in questo campo. Specificare l'indirizzo o il nome del server e-mail. Per il nome, è possibile utilizzare un nome di dominio (*ad esempio imap.acme.com*) o un indirizzo IP (*ad esempio 123.45.67.89*). Se il server e-mail 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 imap.acme.com:8200*. La porta

standard per la comunicazione IMAP è la numero 143.

- ***Altre impostazioni***: specifica parametri più dettagliati:
  - ***Porta locale***: specifica la porta su cui è prevista la comunicazione dall'applicazione e-mail. Nell'applicazione e-mail sarà quindi necessario specificare tale porta come porta per la comunicazione IMAP.
  - ***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 terzi. Questa funzionalità è disponibile solo se supportata dal server e-mail di destinazione.
- ***Attivazione server IMAP client e-mail***: selezionare/deselezionare questa casella per attivare/disattivare il server IMAP specificato

9.13. Resident Shield

Il componente***Resident Shield*** fornisce una protezione attiva di file e cartelle da virus, spyware e altri 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*** (*disattivata per impostazione predefinita*): 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*** (*disattivata per impostazione predefinita*): selezionare questa casella di controllo 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*** (*disattivata per impostazione predefinita*): 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 scansione in un ambiente informatico virtuale*)

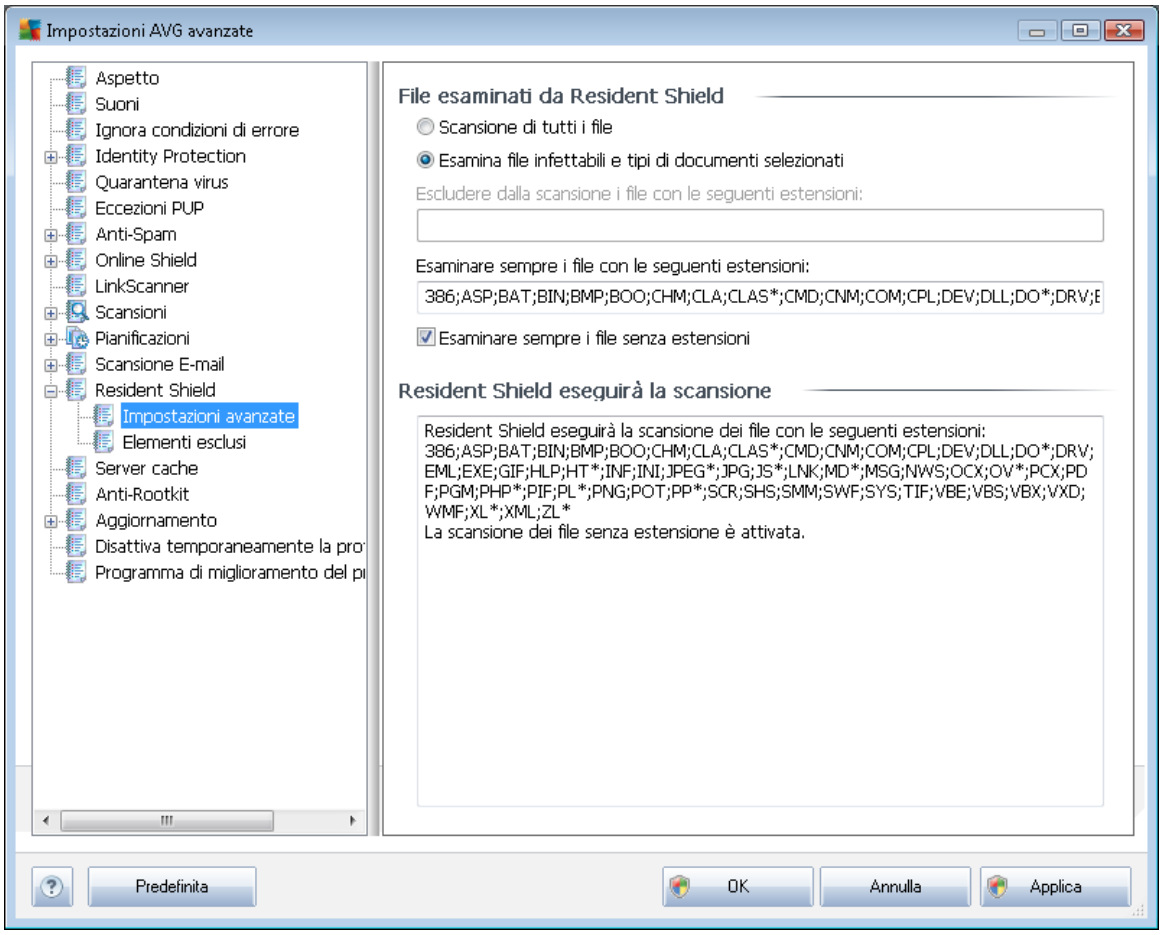
- ***Rimuovi automaticamente tutte le minacce*** (*disattivata per impostazione predefinita*): tutte le infezioni rilevate verranno corrette automaticamente se è disponibile una soluzione e tutte le infezioni che non possono essere corrette verranno rimosse.

- ***Scansione file nominati nel registro*** (*attivata per impostazione predefinita*): questo parametro specifica che AVG sottoporrà a scansione tutti i file eseguibili aggiunti al registro di avvio per evitare che un'infezione nota venga eseguita al successivo avvio del computer.

- ***Attiva scansione completa*** (*disattivata per impostazione predefinita*): in situazioni specifiche (*stati di estrema emergenza*) è possibile selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno accuratamente tutti gli oggetti potenzialmente minacciosi. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.

9.13.1. Impostazioni avanzate

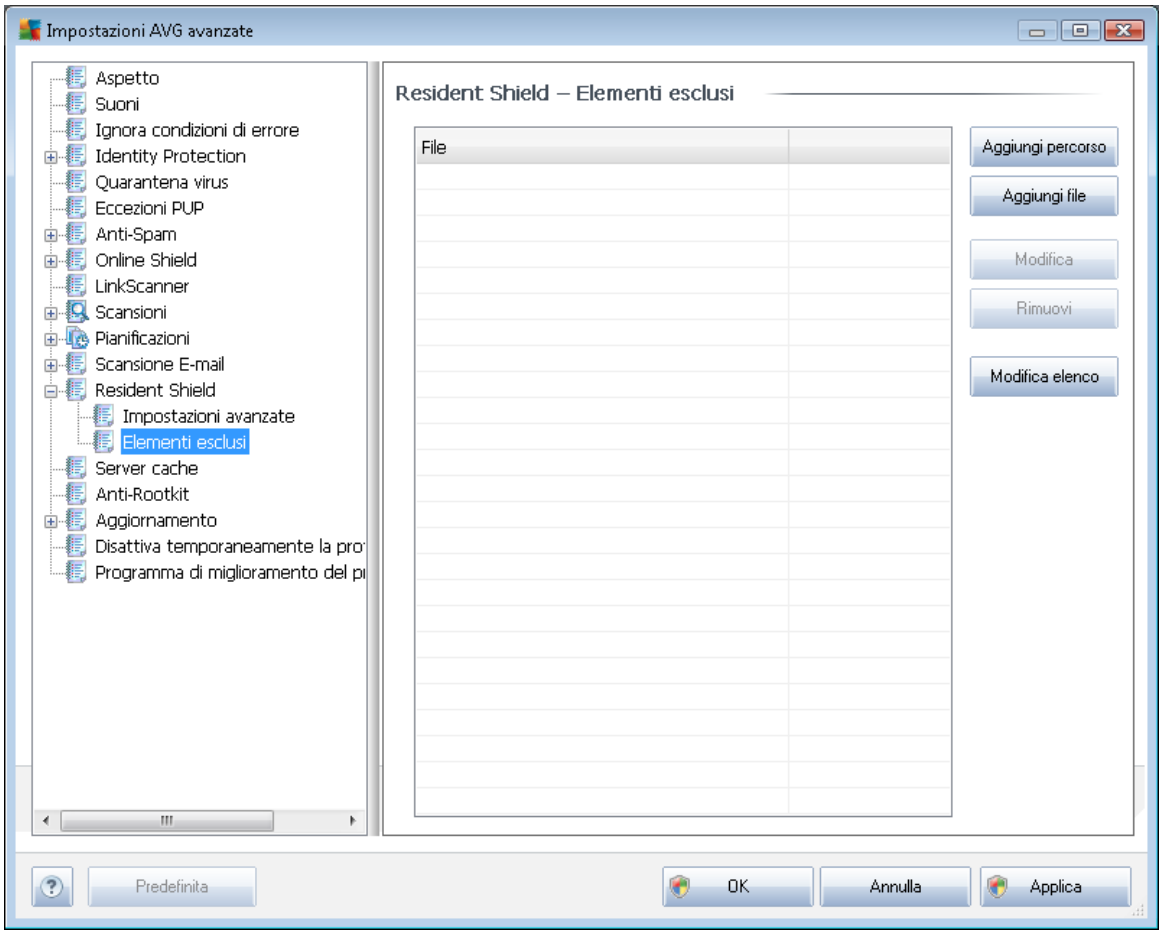
Nella finestra di dialogo ***File esaminati da Resident Shield*** è possibile configurare i file che verranno sottoposti a scansione (*in base a estensioni specifiche*):



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 relative ai file da escludere dalla scansione e un elenco di estensioni relative ai file che devono essere sottoposti a scansione in qualsiasi circostanza.

La seguente sezione ***Oggetto dell'esame di Resident Shield*** fornisce un'ulteriore panoramica dettagliata degli elementi che verranno effettivamente sottoposti a scansione da ***Resident Shield***.

9.13.2. Elementi esclusi



La finestra di dialogo ***Resident Shield - Elementi esclusi*** offre la possibilità di definire i file e/o le cartelle che devono essere esclusi dalla scansione ***Resident Shield***.

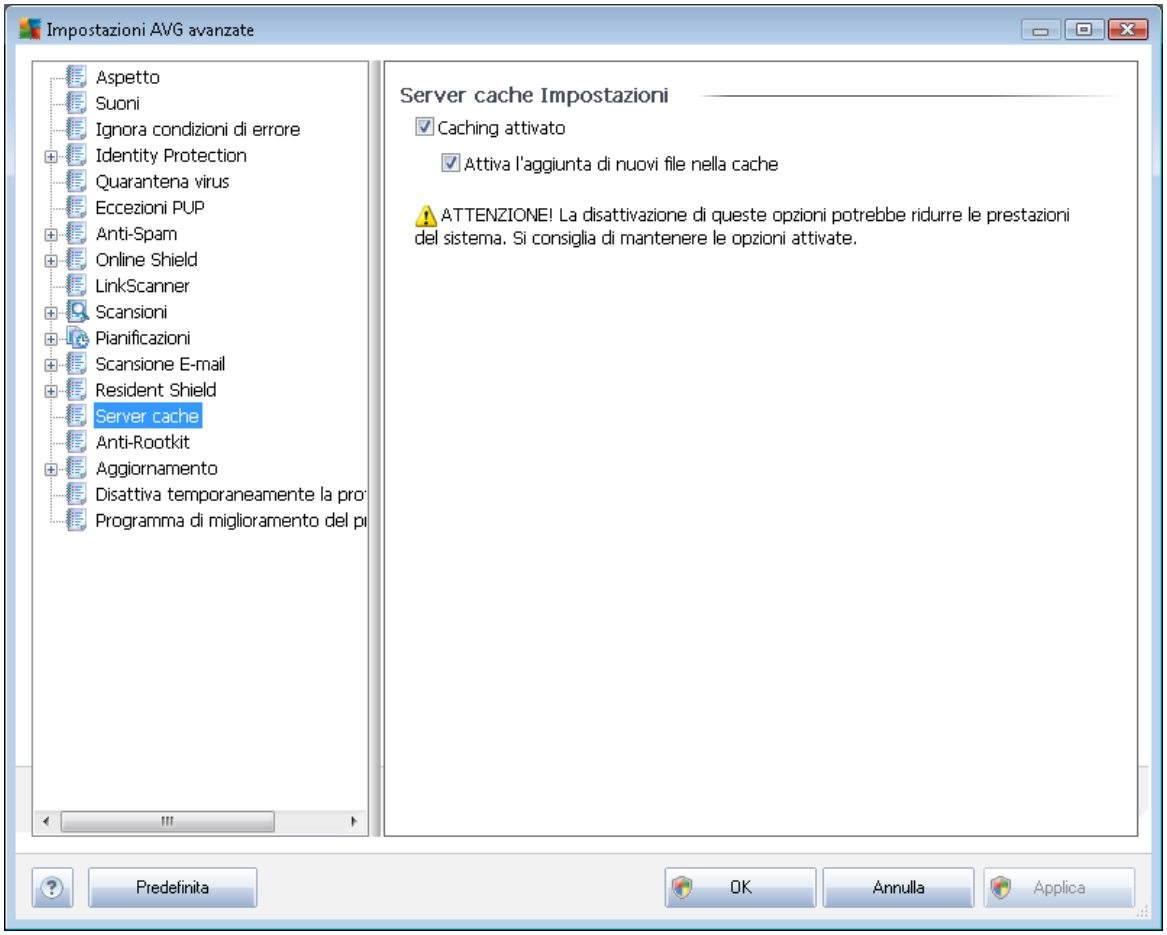
Se non è essenziale, si consiglia di non escludere alcun elemento.

La finestra di dialogo fornisce i seguenti pulsanti di controllo:

- ***Aggiungi percorso***: consente di specificare le directory da escludere dalla scansione selezionandole una alla volta dalla struttura di esplorazione del disco locale
- ***Aggiungi file***: consente di specificare i file da escludere dalla scansione selezionandoli uno alla volta dalla struttura di esplorazione del disco locale
- ***Modifica elemento***: consente di modificare il percorso specificato di un file o una cartella selezionati
- ***Rimuovi elemento***: consente di eliminare dall'elenco il percorso dell'elemento selezionato

9.14. 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.



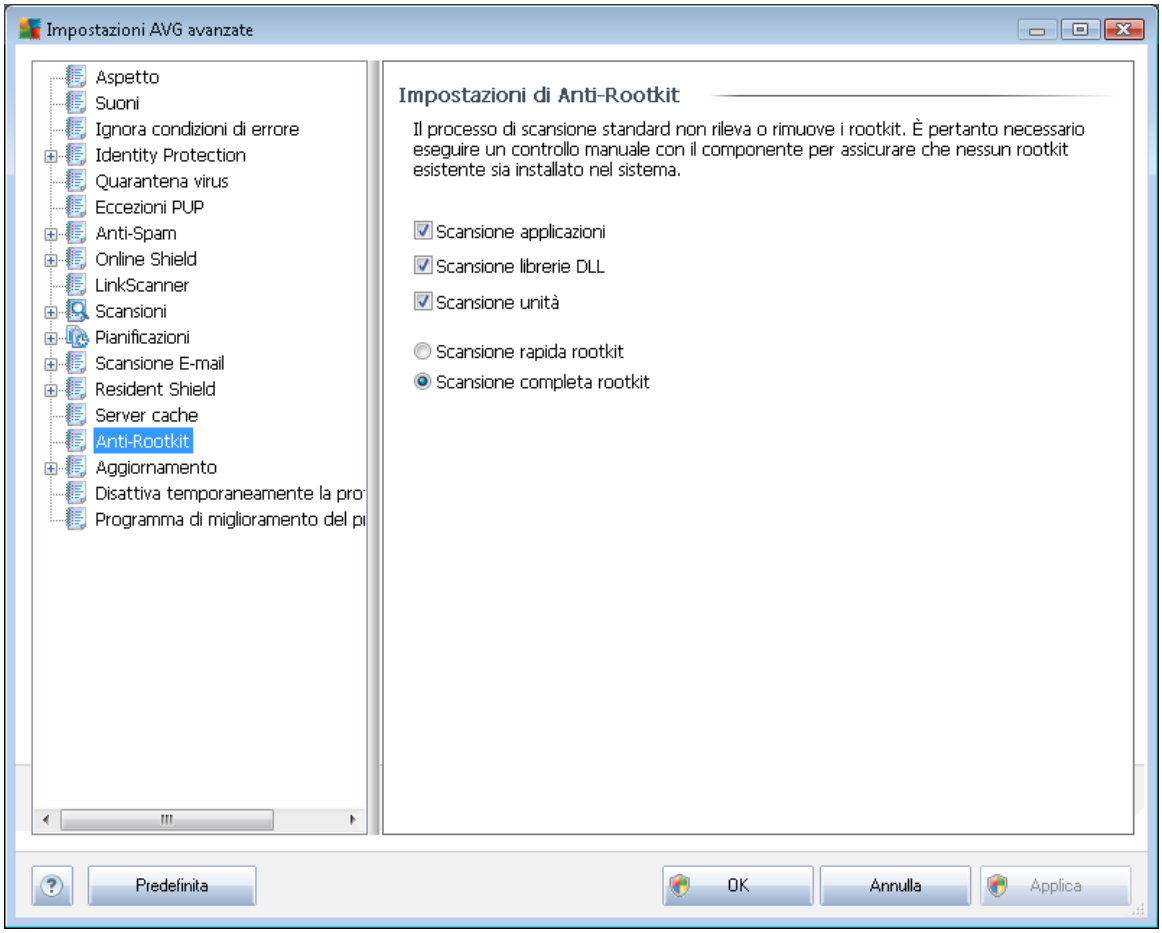
La finestra di dialogo di impostazione offre due opzioni:

- ***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.

9.15. 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:

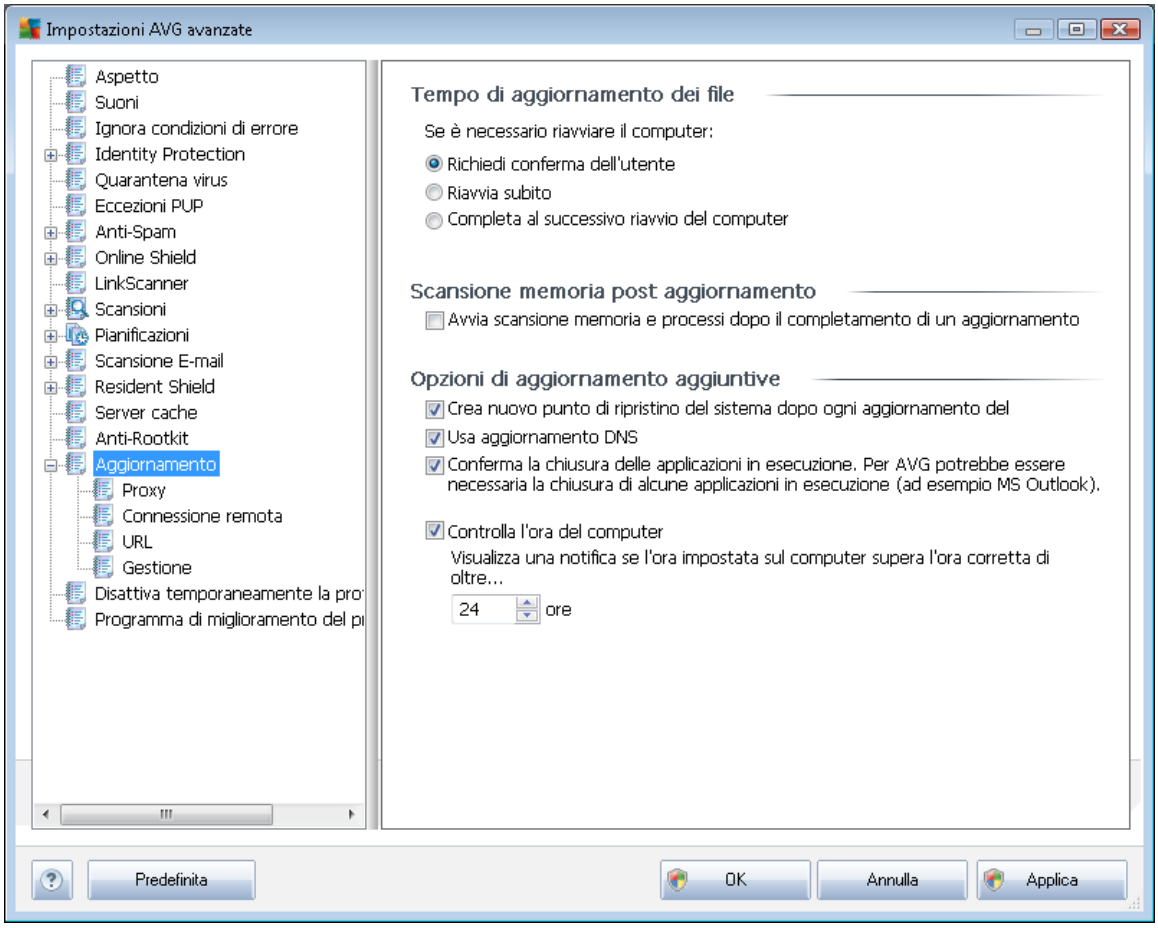
- ***Scansione applicazioni***
- ***Scansione librerie DLL***
- ***Scansione unità***

Quindi, è possibile selezionare la modalità di scansione anti-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*)

9.16. Aggiornamento



La voce ***Aggiorna*** consente di aprire una finestra di dialogo in cui è possibile specificare i parametri generali relativi all'aggiornamento di AVG:

Quando eseguire l'aggiornamento dei file

In questa sezione è possibile effettuare la selezione tra tre diverse opzioni da utilizzare nel caso in cui il processo di aggiornamento richieda il riavvio del PC. È possibile pianificare la finalizzazione dell'aggiornamento per il successivo riavvio del PC oppure è possibile procedere subito al riavvio:

- ***Richiedi conferma dell'utente*** *(impostazione predefinita)*: verrà richiesto di approvare un riavvio del PC necessario per finalizzare il processo di aggiornamento
- ***Riavvia subito***: il computer verrà riavviato immediatamente in maniera automatica dopo la finalizzazione del processo di aggiornamento senza richiesta di conferma da parte dell'utente

- ***Completa al successivo riavvio del computer***: la finalizzazione del processo di aggiornamento verrà posticipata al successivo riavvio del computer. Tenere presente che questa opzione è consigliata solo se si è certi che il computer venga 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

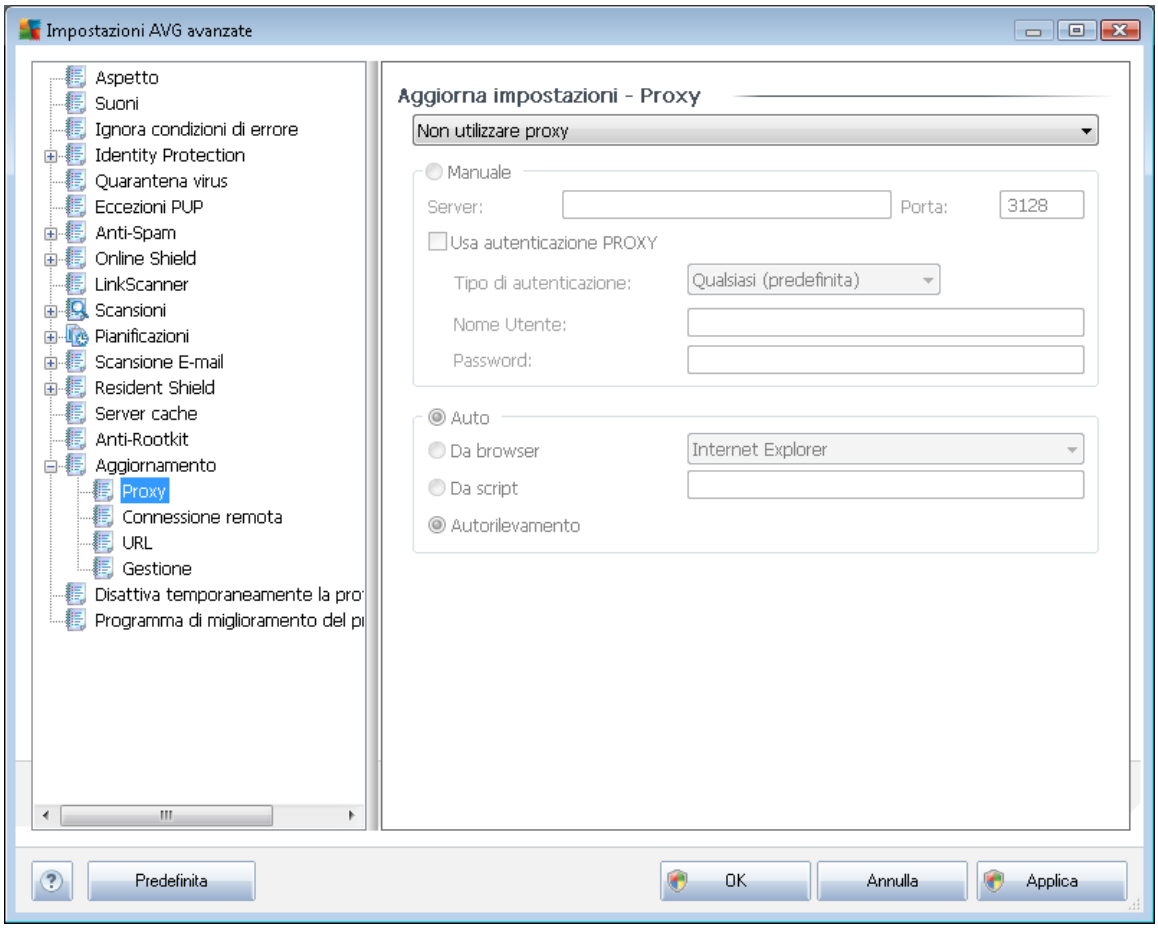
- ***Crea nuovo punto di ripristino del sistema durante ogni aggiornamento del programma***: prima dell'avvio di ciascun aggiornamento del programma AVG viene creato un punto di ripristino del sistema. Se il processo di aggiornamento non ha esito positivo e il sistema operativo si blocca, è possibile 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*** (*attiva per impostazione predefinita*): con questa voce selezionata, una volta avviato l'aggiornamento, **AVG Internet Security 2011** ricerca informazioni sulla versione del database dei virus più recente e sulla versione del programma più recente sul server DNS. Quindi, solo i file di aggiornamento più piccoli e indispensabili vengono scaricati e applicati. In questo modo la quantità totale di dati scaricati viene ridotta al minimo e il processo di aggiornamento viene accelerato.

  - ***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.

9.16.1. 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*)

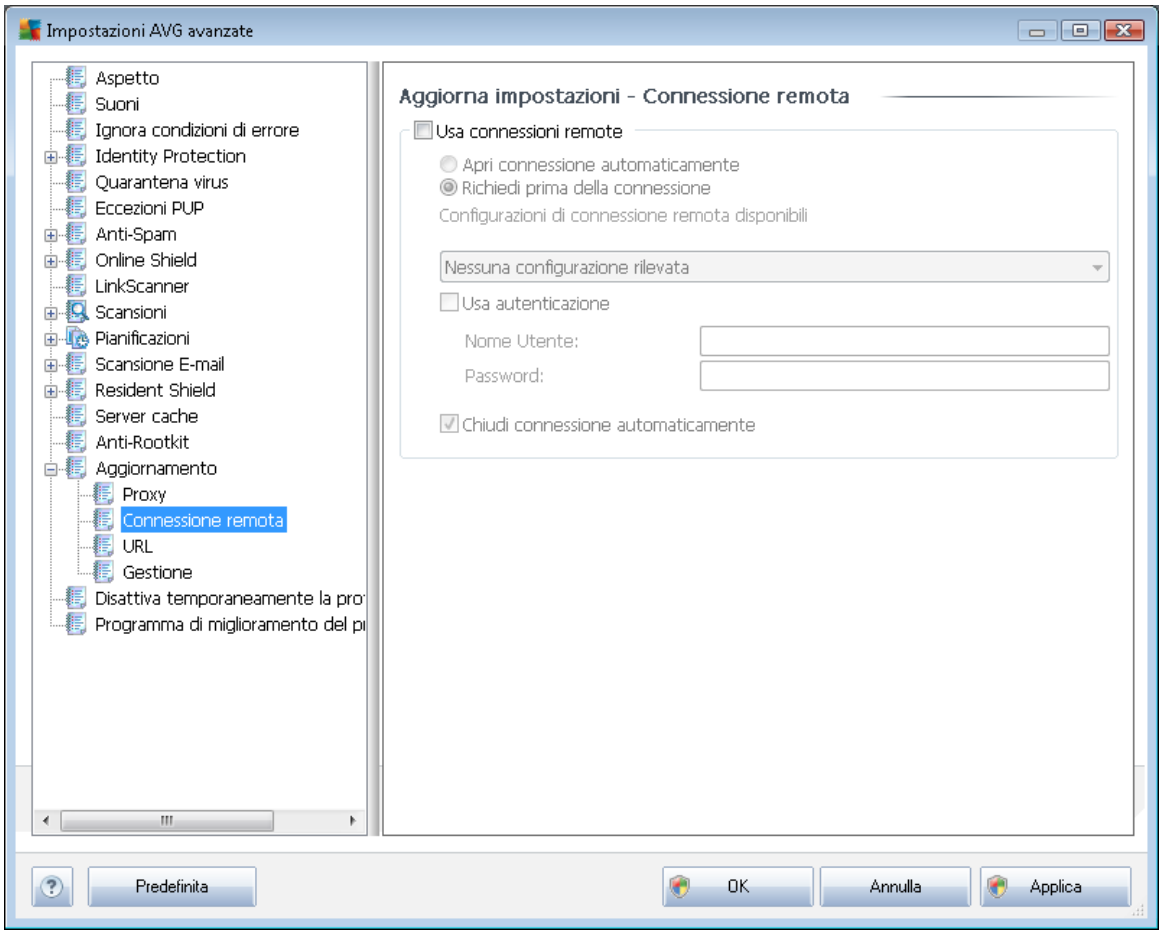
È anche possibile che sul server proxy siano state configurate regole specifiche per ciascun utente. Se il server proxy è impostato in questo modo, selezionare l'opzione ***Usa autenticazione PROXY*** per verificare che nome utente e password siano validi per la connessione a Internet tramite il server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

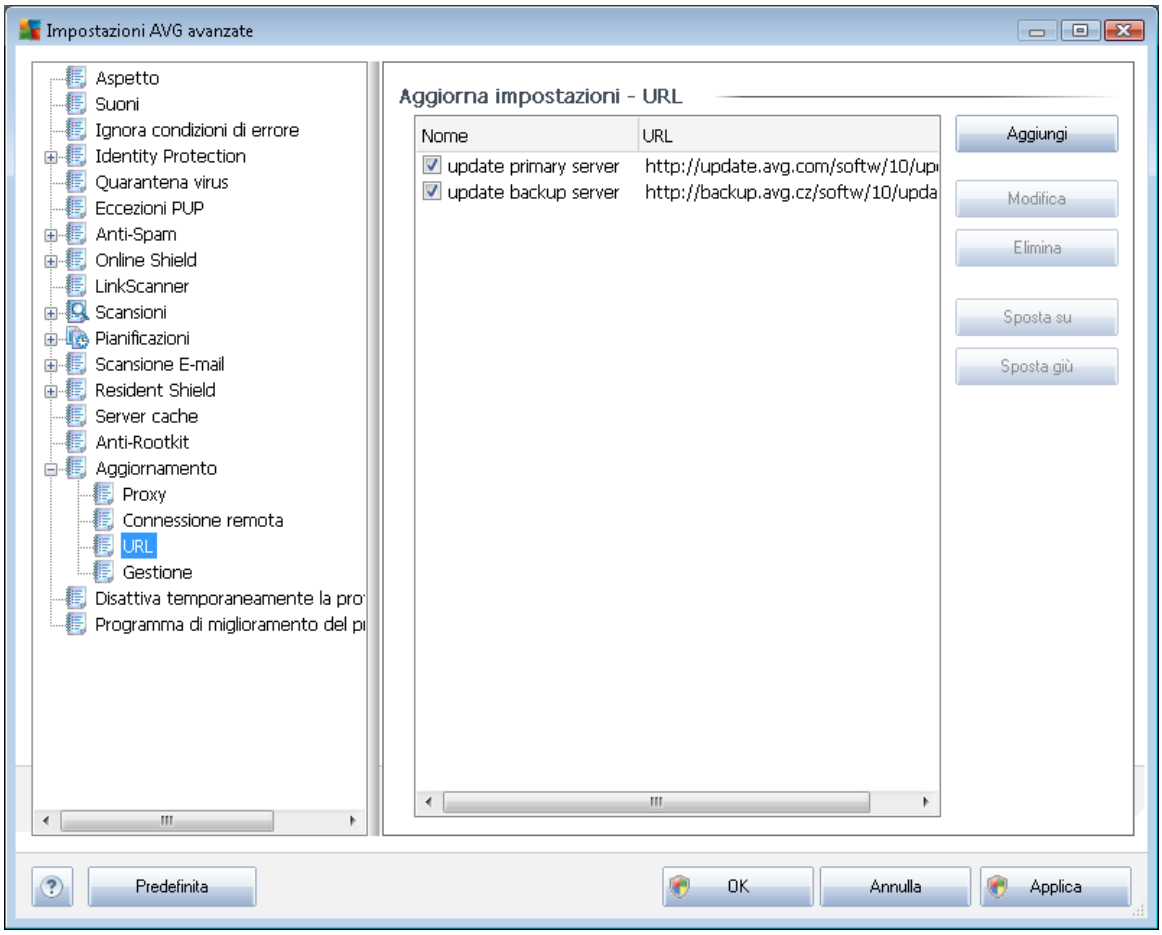
9.16.2. Connessione remota



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***).

9.16.3. URL

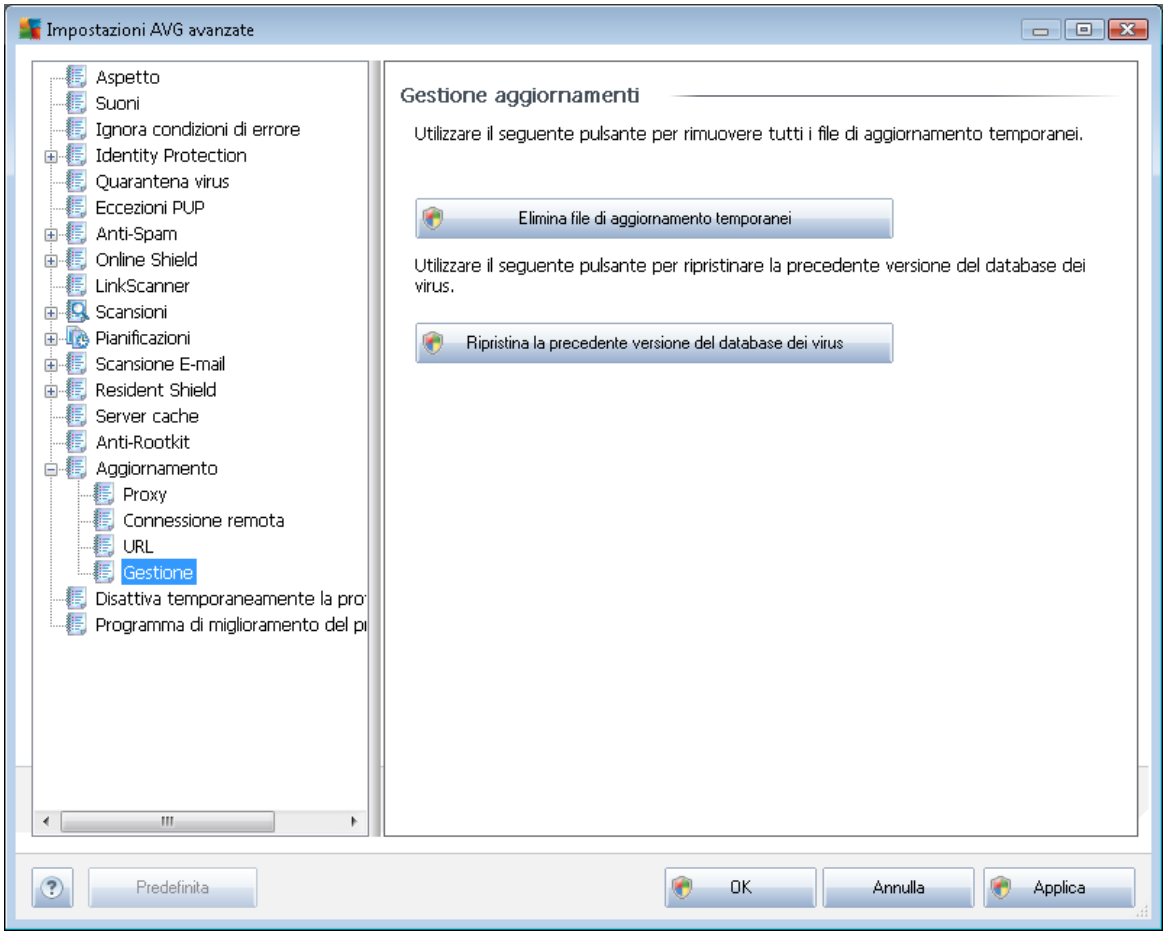


Nella finestra di dialogo ***URL*** è contenuto un elenco di indirizzi Internet da cui è possibile scaricare i file di aggiornamento. È possibile modificare l'elenco e i suoi elementi utilizzando i seguenti pulsanti di controllo:

- ***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

9.16.4. Gestione

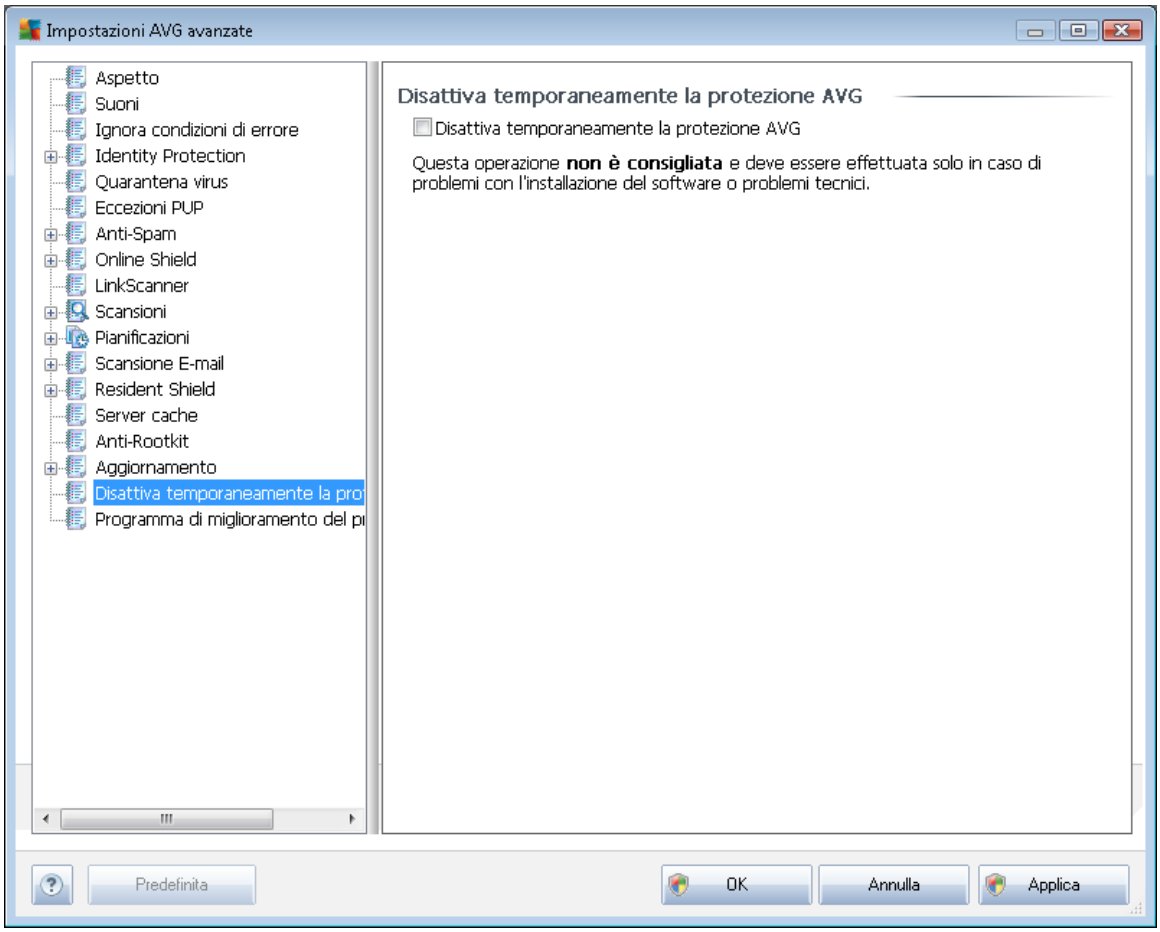
La finestra di dialogo ***Gestione*** offre due opzioni accessibili tramite due pulsanti:



- ***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*)

9.17. Disabilitare temporaneamente la protezione di AVG



Nella finestra di dialogo ***Disabilitare temporaneamente la protezione di AVG*** è possibile disattivare l'intera protezione fornita da **AVG Internet Security 2011**.

Non utilizzare questa opzione se non è assolutamente necessario.

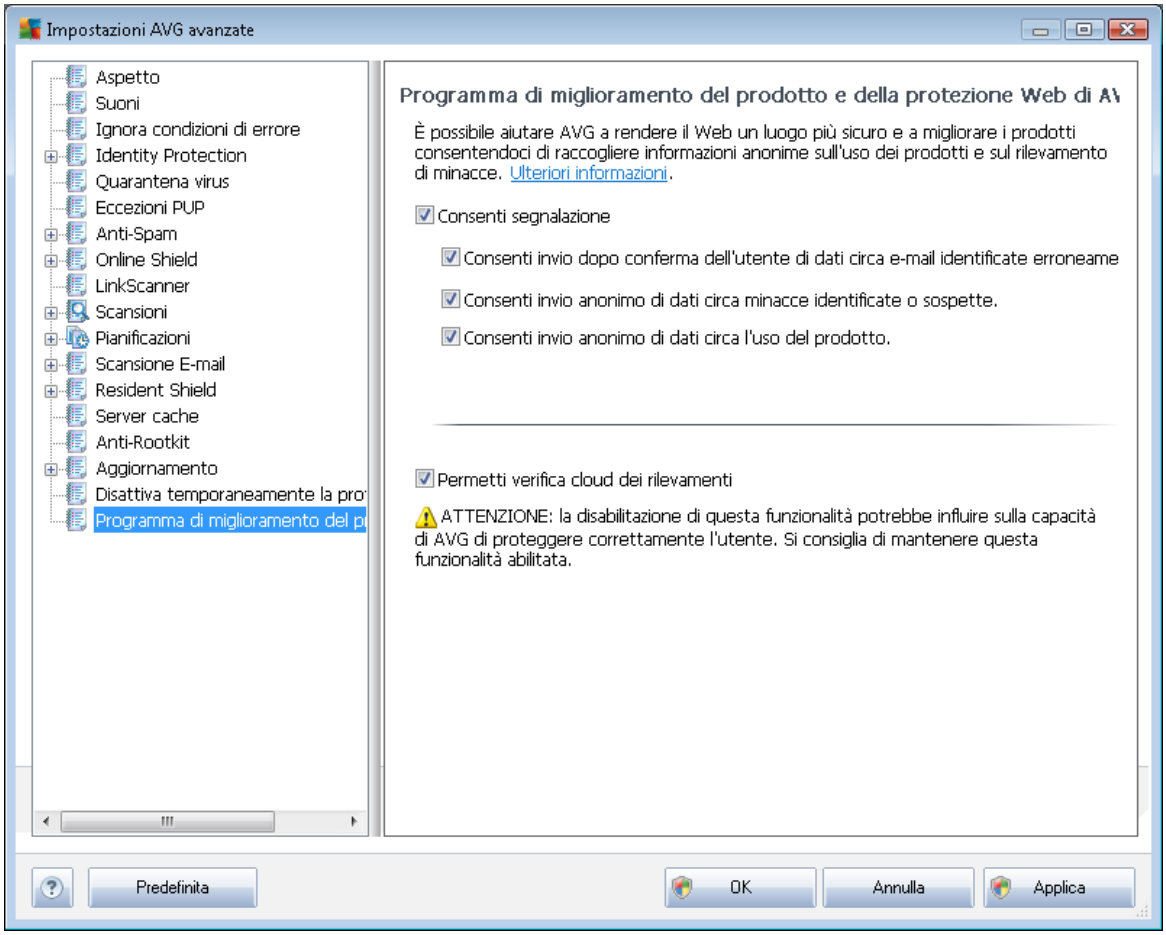
Nella gran parte dei casi, ***non è necessario*** disattivare AVG prima di installare nuovi software o driver, neppure se il programma di installazione o la procedura guidata suggeriscono di chiudere tutti i programmi e le applicazioni in esecuzione per accertarsi che non si verifichino interruzioni indesiderate durante il processo di installazione. In caso di problemi durante l'installazione, provare a disattivare innanzitutto il componente ***Resident Shield***. Se è necessario disattivare temporaneamente AVG, lo si dovrà riattivare non appena possibile. Se si è connessi a Internet o a una rete mentre il software antivirus è disattivato, il computer sarà esposto a potenziali attacchi.

9.18. Programma di miglioramento del prodotto

La finestra di dialogo ***Programma di miglioramento del prodotto e della protezione Web di AVG*** invita a collaborare al miglioramento del prodotto AVG per aiutarci ad aumentare il livello di protezione generale in Internet. Selezionare l'opzione ***Consenti segnalazione*** per attivare la segnalazione delle minacce rilevate a AVG. Questo ci consente di raccogliere informazioni

aggiornate sulle minacce più recenti da tutti gli utenti a livello mondiale e di migliorare la protezione per tutti.

La segnalazione viene elaborata automaticamente, pertanto non provoca alcun disturbo all'utente, e nei rapporti non vengono inclusi dati personali. La segnalazione delle minacce rilevate è facoltativa, tuttavia è consigliabile attivare anche questa funzionalità in quanto ci consente di migliorare la protezione per tutti gli utenti di AVG.



Attualmente le minacce esistenti non si limitano più ai semplici virus. Gli autori di codici dannosi e di siti Web pericolosi hanno molta inventiva, per cui emergono abbastanza di frequente nuovi tipi di minacce, la maggior parte delle quali in Internet. Di seguito vengono riportati alcuni dei tipi più comuni:

- ***Un virus*** è un codice dannoso che si copia e si diffonde in maniera automatica, spesso passando inosservato fino al compimento del danno. Alcuni virus rappresentano una minaccia seria, poiché eliminano o modificano direttamente i file, mentre altri agiscono in maniera apparentemente innocua, ad esempio durante la riproduzione di un brano musicale. Tuttavia, tutti i virus sono pericolosi a causa della capacità di base di moltiplicarsi. Anche un virus semplice è in grado di assorbire tutta la memoria di un computer in un istante causando danni.

- ***Il worm*** è una sottocategoria di virus che, a differenza dei virus normali, non necessita di un oggetto "trasportatore" a cui collegarsi; si invia automaticamente ad altri computer, solitamente tramite e-mail, provocando spesso sovraccarichi sui server e-mail e sui sistemi di rete.

- ***Spyware*** si definisce solitamente come una categoria di malware (*malware = qualsiasi software dannoso, virus compresi*) che comprende alcuni programmi, in genere trojan horse, il cui scopo è quello di appropriarsi di informazioni personali, password, numeri delle carte di credito o infiltrarsi in un computer consentendo all'autore dell'attacco di assumere il controllo in modalità remota, ovviamente senza che il proprietario del computer ne sia a conoscenza o abbia dato il proprio consenso.

- ***I programmi potenzialmente indesiderati*** sono un tipo di spyware che può essere o meno pericoloso per il computer. Un esempio specifico di PUP è l'adware, un software progettato per distribuire annunci, solitamente tramite la visualizzazione di popup. Può essere fastidioso ma non realmente dannoso.

- ***I cookie di rilevamento*** possono inoltre essere considerati come un tipo di spyware, in quanto si tratta di piccoli file archiviati nel browser Web e inviati automaticamente al sito Web principale quando lo si visita di nuovo, e possono contenere dati quali la cronologia di esplorazione e altre informazioni simili.

- ***Exploit*** è un codice dannoso che sfrutta un'imperfezione o una vulnerabilità di un sistema operativo, un browser Internet o un altro programma fondamentale.

- ***Il phishing*** è un tentativo di acquisire dati personali sensibili fingendosi un'organizzazione nota e affidabile. In genere, le vittime potenziali vengono contattate tramite messaggi e-mail inviati in blocco in cui vengono richiesti, ad esempio, i dati del conto bancario. A questo scopo, gli utenti vengono invitati a seguire il collegamento fornito che li indirizza a un sito Web della banca falso.

- ***Gli hoax*** sono messaggi e-mail inviati in blocco contenenti informazioni pericolose, allarmanti o semplicemente inutili e fastidiose. Molte delle minacce sopraelencate per diffondersi utilizzano i messaggi e-mail hoax.

- ***I siti Web dannosi*** sono quei siti che installano deliberatamente software dannoso nel computer, in modo simile ai siti manomessi, anche se questi ultimi sono siti Web legittimi che sono stati compromessi da visitatori che hanno introdotto infezioni.

Per proteggere il computer da tutte queste minacce, in AVG sono disponibili componenti specifici:

- ***Anti-Virus*** per proteggere il computer dai virus,

- ***Anti-Spyware*** per proteggere il computer dagli spyware,

- ***Online Shield*** per proteggere sia da virus che da spyware durante la navigazione in Internet,

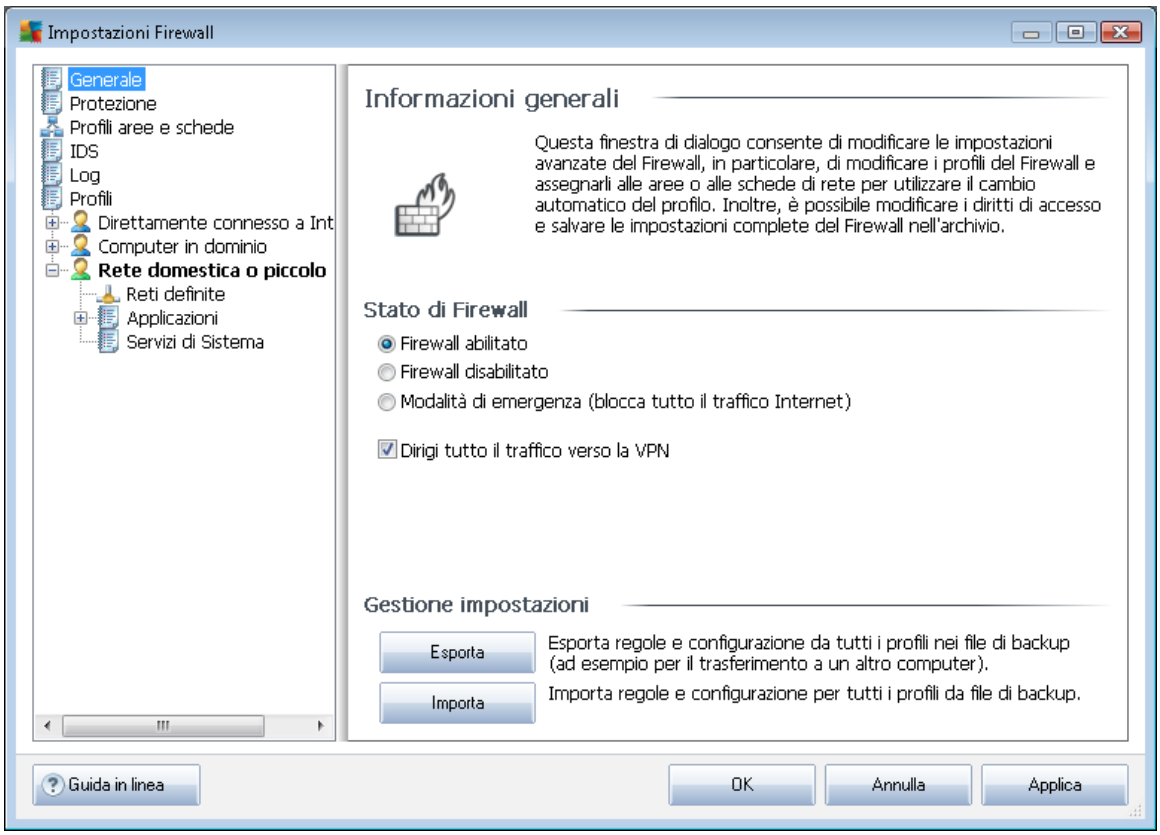
- ***Link Scanner*** per proteggere il computer da altre minacce presenti in rete citate in questo capitolo.

10. Impostazioni Firewall

La finestra di dialogo di configurazione di ***Firewall*** viene aperta in una nuova finestra dove in varie finestre di dialogo è possibile impostare parametri del componente molto avanzati. ***La modifica della configurazione avanzata, tuttavia, è destinata solo a utenti esperti.***

10.1. Generale

La finestra di dialogo ***Informazioni generali*** è divisa in due sezioni:



Stato del firewall:

Nella sezione ***Stato del firewall*** è possibile modificare lo stato del ***Firewall*** in base alle esigenze:

- ***Firewall abilitato***: selezionare questa opzione per consentire la comunicazione alle applicazioni contrassegnate come "consentite" nell'insieme di regole definito all'interno del ***profilo Firewall***
- ***Firewall disabilitato***: questa opzione consente di disattivare completamente il componente ***Firewall***. Tutto il traffico di rete viene consentito ma non controllato.
- ***Modalità di emergenza*** *(blocca tutto il traffico Internet)*: selezionare questa opzione per bloccare tutto il traffico su ogni singola porta di rete; il ***Firewall*** è ancora in esecuzione ma

tutto il traffico di rete viene interrotto

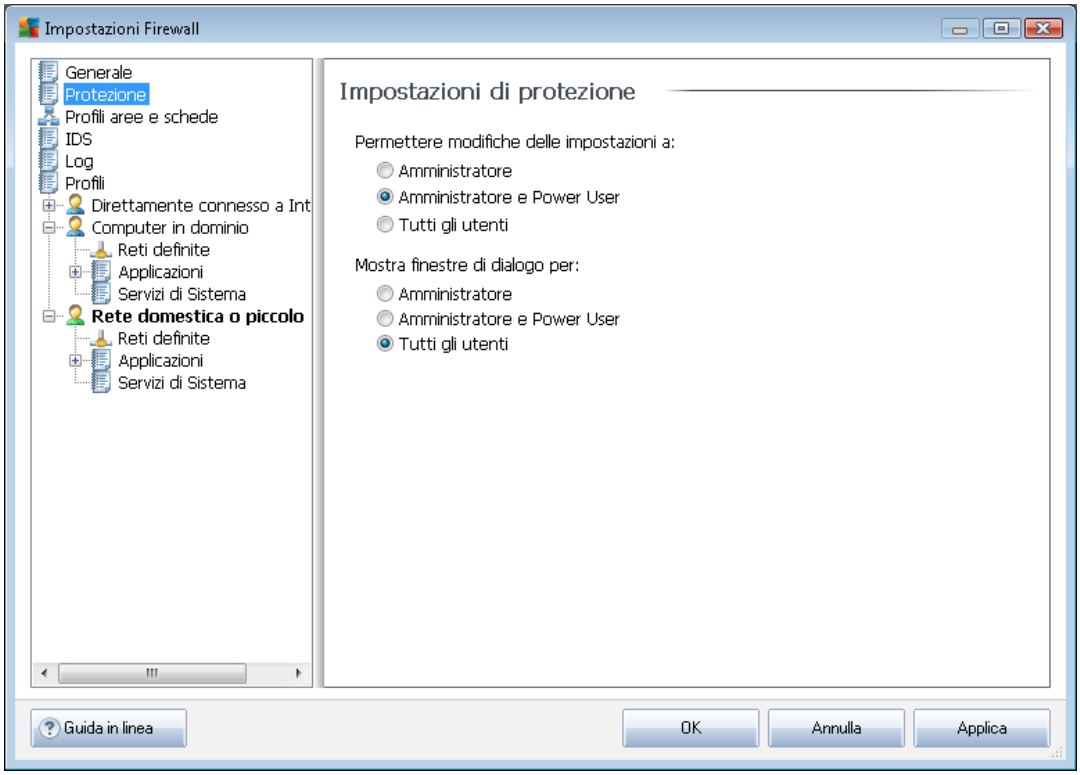
- ***Dirigi tutto il traffico verso la VPN***: se si utilizza una connessione VPN *(Virtual Private Network)*, ad esempio per connettersi all'ufficio da casa, si consiglia di selezionare questa casella. ***AVG Firewall*** cercherà automaticamente tra le schede di rete, troverà quelle utilizzate per la connessione VPN e consentirà a tutte le applicazioni di connettersi alla rete di destinazione *(valido solo per le applicazioni senza specifiche regole Firewall assegnate)*. Su un sistema standard con schede di rete comuni, questo semplice passaggio dovrebbe evitare di dover impostare una regola dettagliata per ciascuna applicazione da utilizzare sulla VPN.

Nota: *per attivare la connessione VPN completamente, è necessario consentire la comunicazione ai seguenti protocolli di sistema: GRE, ESP, L2TP, PPTP. Questa operazione può essere effettuata nella finestra di dialogo Servizi di sistema.*

Gestione impostazioni

Nella sezione ***Informazioni generali*** è possibile utilizzare le opzioni ***Esporta*** / ***Importa*** per la configurazione del componente ***Firewall***, ossia esportare le regole e le impostazioni ***Firewall*** definite nei file di backup oppure, dall'altra parte, importare il file dell'intero backup.

10.2. Protezione



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

- ***Permettere modifiche delle impostazioni a***: consente di specificare a chi è consentito modificare la configurazione di ***Firewall***.

- ***Mostra finestre di dialogo per***: consente di specificare gli utenti per i quali devono essere visualizzate le finestre di dialogo di conferma (*finestre di dialogo in cui si chiede una decisione in una situazione che non è coperta da una regola definita di* ***Firewall***).

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

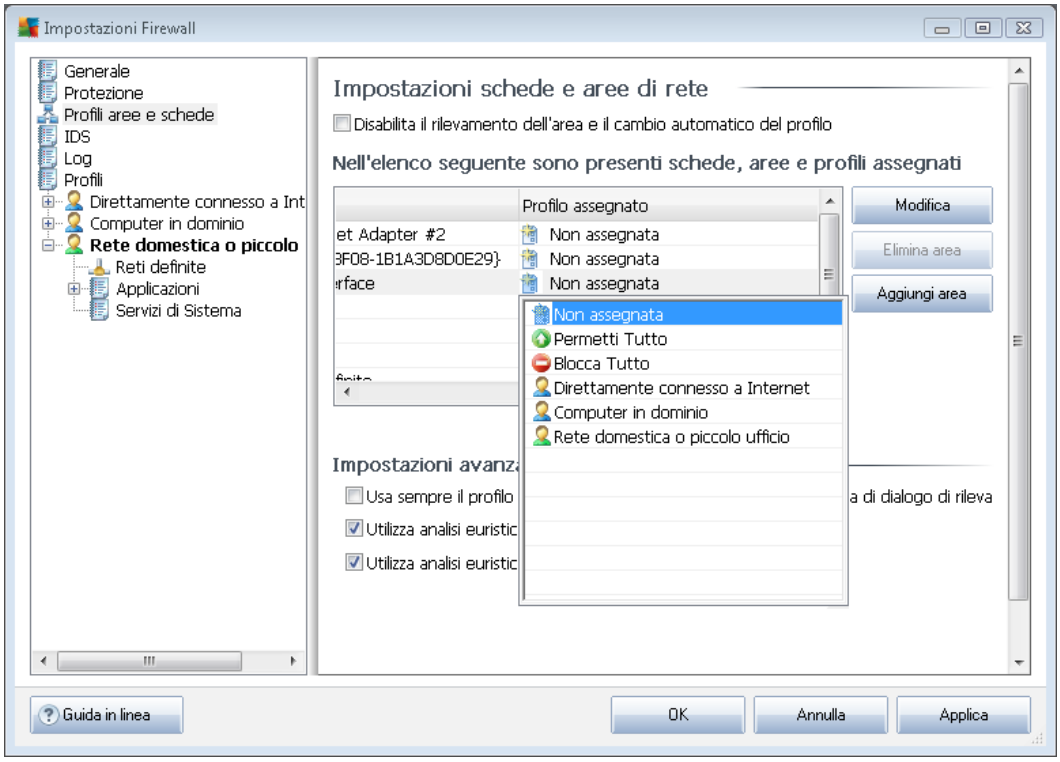
- ***Amministratore*** : consente di controllare completamente il PC e dispone dei diritti per assegnare ogni utente ai vari gruppi con autorità definite in modo specifico.

- ***Amministratore e Power User*** : l'amministratore può assegnare qualunque utente a un gruppo specifico (*Power User*) e definire le autorità dei membri del gruppo.

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

10.3. Profili di aree e schede

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



- ***Disabilita rilevamento delle aree e attivazione dei profili***: uno dei profili definiti può

essere assegnato a ciascun tipo di interfaccia di rete, relativamente a ciascuna area. Se non si desidera definire profili specifici, verrà utilizzato un profilo comune. Tuttavia, se si decide di distinguere i profili e assegnarli a schede e aree specifiche e in seguito, per qualsiasi motivo, si desidera cambiare temporaneamente questa impostazione, selezionare l'opzione ***Disabilita rilevamento delle aree e attivazione dei profili***.

- ***Elenco di schede, aree e profili assegnati***: in questo elenco è possibile trovare una panoramica delle schede e delle aree rilevate. A ciascuna di esse è possibile assegnare un profilo specifico dal menu dei profili definiti. Per aprire questo menu, fare clic sulla rispettiva voce nell'elenco delle schede e selezionare il profilo.

Impostazioni avanzate

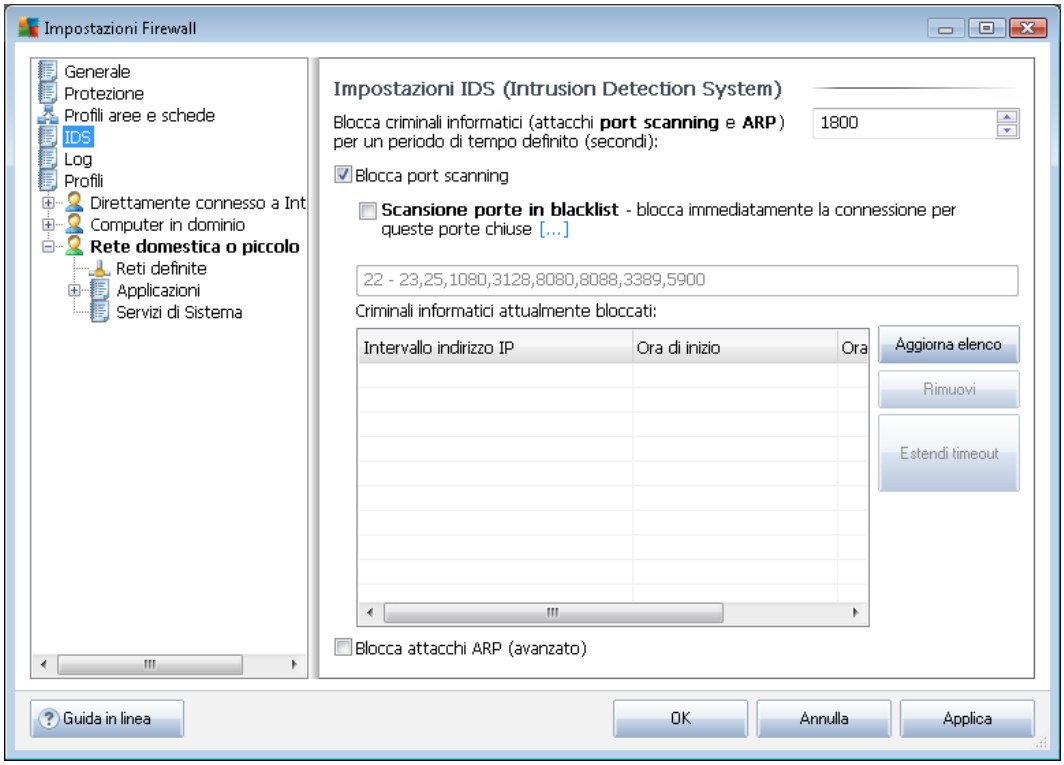
- ***Usa sempre il profilo predefinito e non visualizzare la nuova finestra di dialogo di rilevamento rete***: ogni volta che il computer stabilisce una connessione a una nuova rete, il ***Firewall*** visualizza una finestra di dialogo in cui viene richiesto di selezionare un tipo di connessione di rete e di assegnare alla connessione un ***profilo Firewall***. Se non si desidera che tale finestra venga visualizzata, deselezionare questa casella di controllo.

- ***Utilizza analisi euristica di AVG per rilevamento nuove reti***: consente di acquisire informazioni su una nuova rete rilevata con il metodo proprio di AVG (*questa opzione è disponibile solo su Windows Vista e versioni successive*).

- ***Utilizza analisi euristica di Microsoft per rilevamento nuove reti***: consente di acquisire informazioni su una nuova rete rilevata dal servizio Windows (*questa opzione è disponibile solo su Windows Vista e versioni successive*).

10.4. IDS

IDS (Intrusion Detection System) è una speciale funzionalità di analisi del comportamento progettata per identificare e bloccare tentativi di comunicazione sospetti su porte specifiche del computer. È possibile configurare i parametri IDS all'interno della seguente interfaccia:



La finestra di dialogo ***Impostazioni IDS (Intrusion Detection System)*** offre le seguenti opzioni di configurazione:

- ***Blocca attacchi per un periodo di tempo definito***: consente di specificare per quanti secondi una porta deve essere bloccata ogni volta che viene rilevato un tentativo di comunicazione sospetto su tale porta. Per impostazione predefinita, l'intervallo di tempo è impostato su 1800 secondi (*30 minuti*).

- ***Blocca scansione porta***: selezionare questa casella per bloccare i tentativi di comunicazione su tutte le porte TCP e UDP che raggiungono il computer dall'esterno. Per ogni connessione di questo tipo, sono consentiti cinque tentativi e il sesto viene bloccato.

    - ***Blocca scansione porta*** : selezionare questa casella per bloccare immediatamente qualsiasi tentativo di comunicazione sulle porte specificate nel campo di testo seguente. Le singole porte o gli intervalli di porte devono essere separati da virgole. Se si desidera utilizzare questa funzionalità, è disponibile un elenco predefinito di porte consigliate.

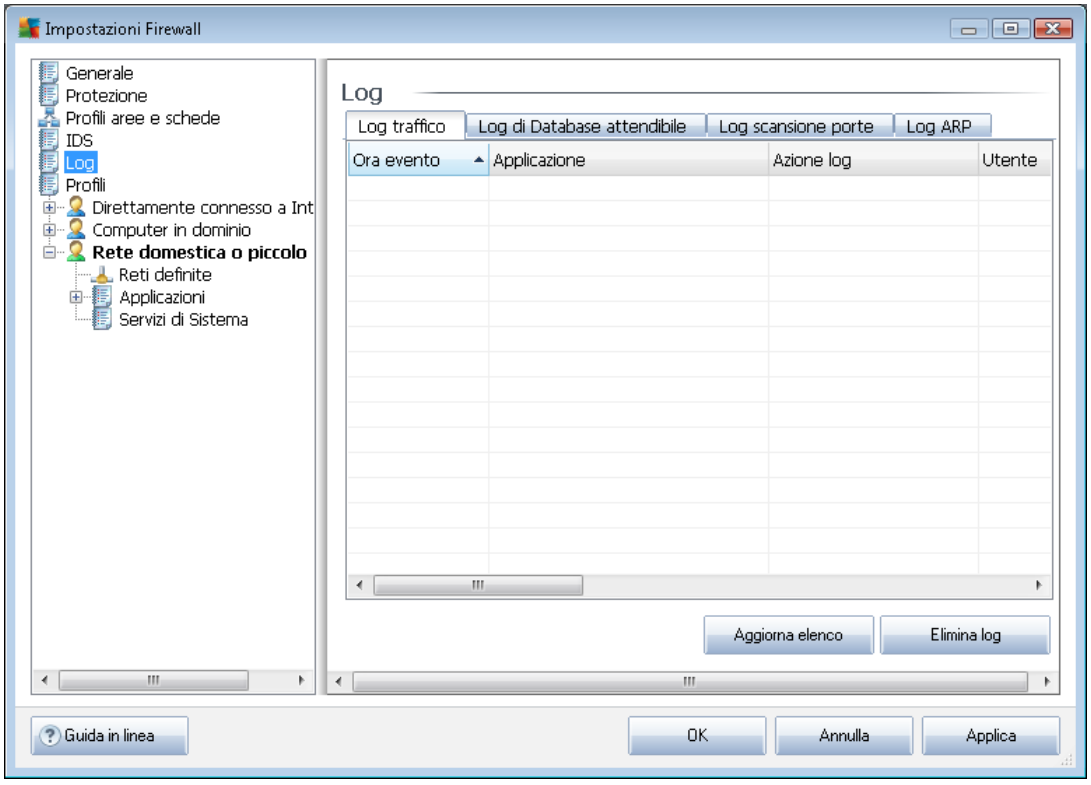
    - ***Attacchi bloccati***: questa sezione elenca tutti i tentativi di comunicazione bloccati dal ***Firewall***. La cronologia completa dei tentativi bloccati può essere visualizzata nella finestra di dialogo ***Log*** (scheda *Log scansione porte*).

- ***Blocca attacchi ARP*** attiva il blocco di speciali tipi di tentativi di comunicazione all'interno della rete locale rilevati da ***IDS*** come potenzialmente pericolosi. Viene applicata l'ora impostata in ***Blocca attacchi per un periodo di tempo definito***. È consigliabile che questa funzionalità venga utilizzata solo da utenti esperti, che conoscono il tipo e il livello di rischio della rete locale.

Pulsanti di controllo

- ***Aggiorna elenco***: selezionare il pulsante per aggiornare l'elenco (*in modo da includere gli eventuali tentativi bloccati più recenti*)
- ***Rimuovi***: selezionare per annullare un blocco selezionato
- ***Estendi timeout***: selezionare per prolungare il periodo di tempo per il quale un tentativo selezionato viene bloccato. Verrà visualizzata una nuova finestra di dialogo con opzioni estese che consentono di impostare data e ora specifiche o una durata illimitata.

10.5. Log



La finestra di dialogo ***Log*** consente di esaminare l'elenco di tutti gli eventi e le azioni ***Firewall*** registrati con una descrizione dettagliata dei relativi parametri (*ora dell'evento, nome dell'applicazione, rispettiva azione log, nome utente, PID, direzione del traffico, tipo di protocollo, numeri delle porte remote e locali e così via*) in quattro schede:

- ***Log traffico***: fornisce informazioni sull'attività di tutte le applicazioni che hanno tentato di connettersi alla rete.
- ***Log database attendibile***: il *database attendibile* è un database interno di AVG che raccoglie informazioni sulle applicazioni certificate e attendibili che saranno sempre autorizzate a comunicare in linea. La prima volta in cui una nuova applicazione tenta di

connettersi alla rete (*ossia quando non è ancora stata specificata alcuna regola firewall per tale applicazione*), è necessario stabilire se la comunicazione di rete deve essere consentita per tale applicazione. Innanzitutto, AVG effettua una ricerca nel *database attendibile*. Se l'applicazione è elencata, sarà automaticamente autorizzata ad accedere alla rete. Se nel database non sono presenti informazioni sull'applicazione, verrà richiesto in una nuova finestra di dialogo se si desidera autorizzare l'applicazione ad accedere alla rete.

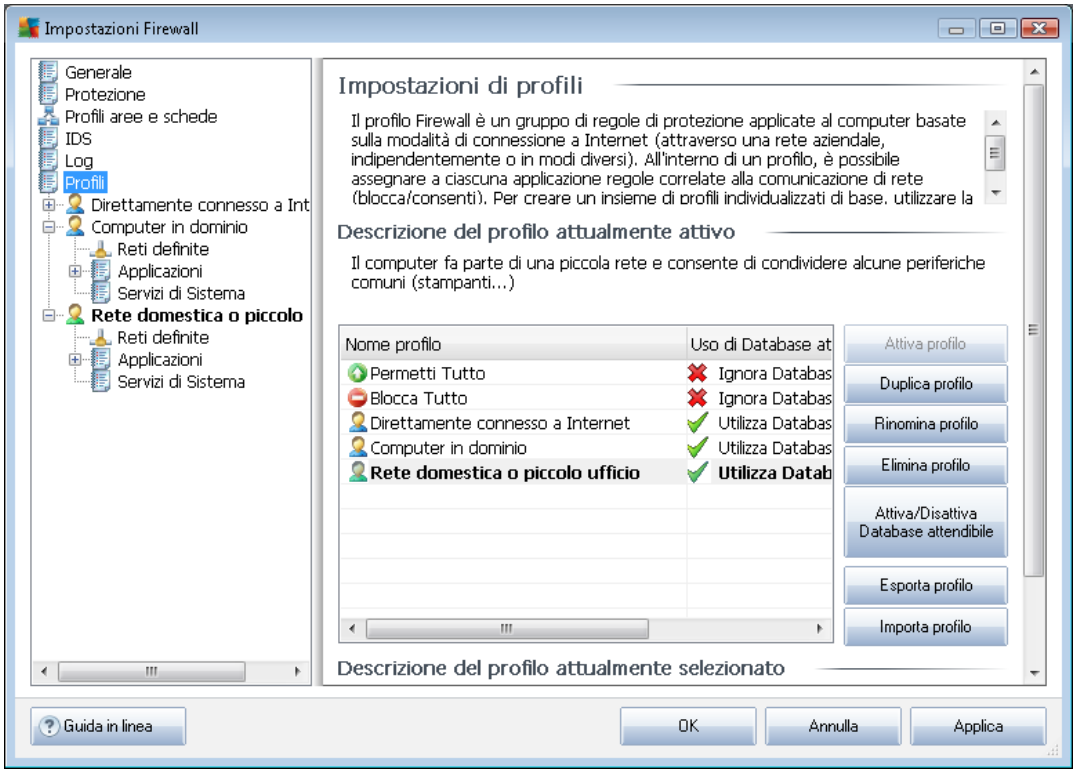
- ***Log scansione porte***: fornisce i log di tutte le attività di ***Intrusion Detection System***.
- ***Log ARP***: log relativi al blocco di tipi speciali di tentativi di comunicazione all'interno di una rete locale (opzione *Blocca attacchi ARP*) rilevati da ***Intrusion Detection System*** come potenzialmente pericolosi.

Pulsanti di controllo

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

10.6. Profili

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



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

- ***Attiva profilo***: questo pulsante consente di impostare il profilo selezionato come attivo. Significa che il profilo selezionato verrà utilizzato dal ***Firewall*** per controllare il traffico di rete.
- ***Duplica profilo***: consente di creare una copia identica del profilo selezionato. In seguito sarà possibile modificare e rinominare la copia per creare un nuovo profilo basato sull'originale duplicato.
- ***Rinomina profilo***: consente di definire un nuovo nome per il profilo selezionato.
- ***Elimina profilo***: consente di eliminare dall'elenco il profilo selezionato.
- ***Attiva/disattiva database attendibile***: per il profilo selezionato è possibile decidere di utilizzare le informazioni del *database attendibile* (*il database attendibile è un database interno di AVG che raccoglie dati sulle applicazioni certificate e attendibili che saranno sempre autorizzate a comunicare in linea*).
- ***Esporta profilo***: consente di registrare la configurazione del profilo selezionato in un file che verrà salvato per un possibile ulteriore utilizzo.

- ***Importa profilo***: consente di configurare le impostazioni del profilo selezionato in base ai dati esportati dal file di configurazione di backup.

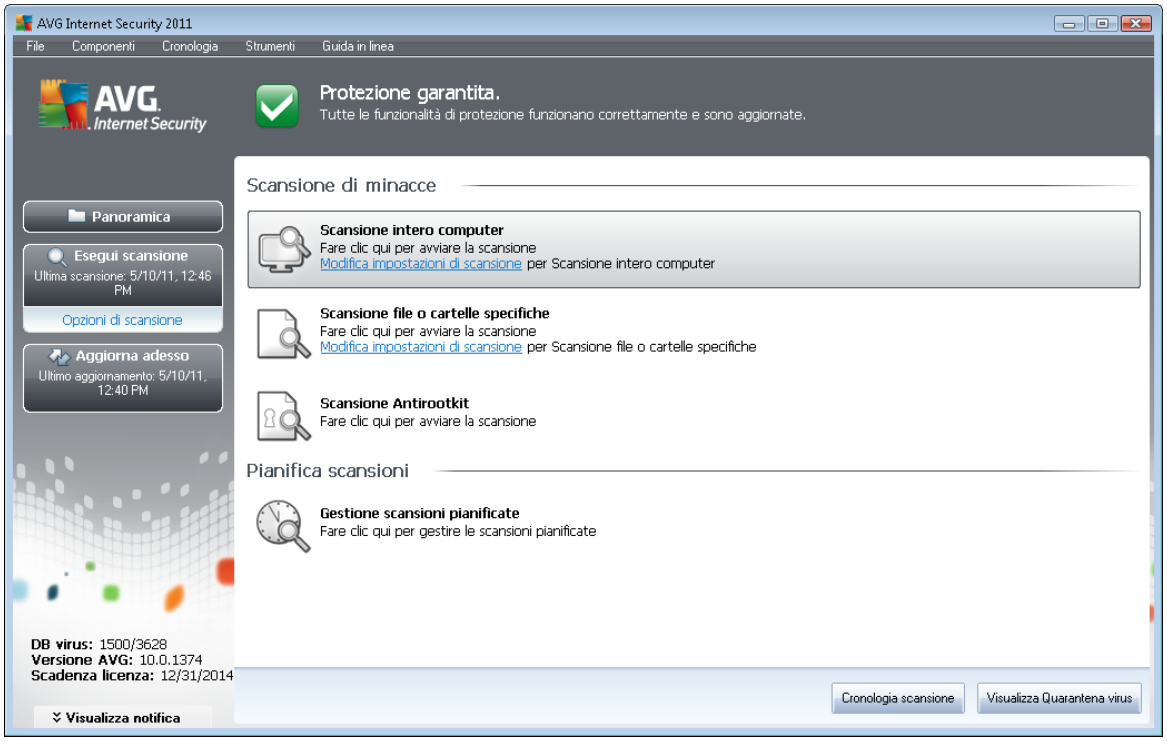
Nella sezione inferiore della finestra di dialogo si trova la descrizione del profilo attualmente selezionato nell'elenco.

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

11. Scansione AVG

La scansione è una parte fondamentale della funzionalità di **AVG Internet Security 2011**. 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***Opzioni di scansione***. 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 Anti-Rootkit***
- 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 Internet Security 2011** 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.

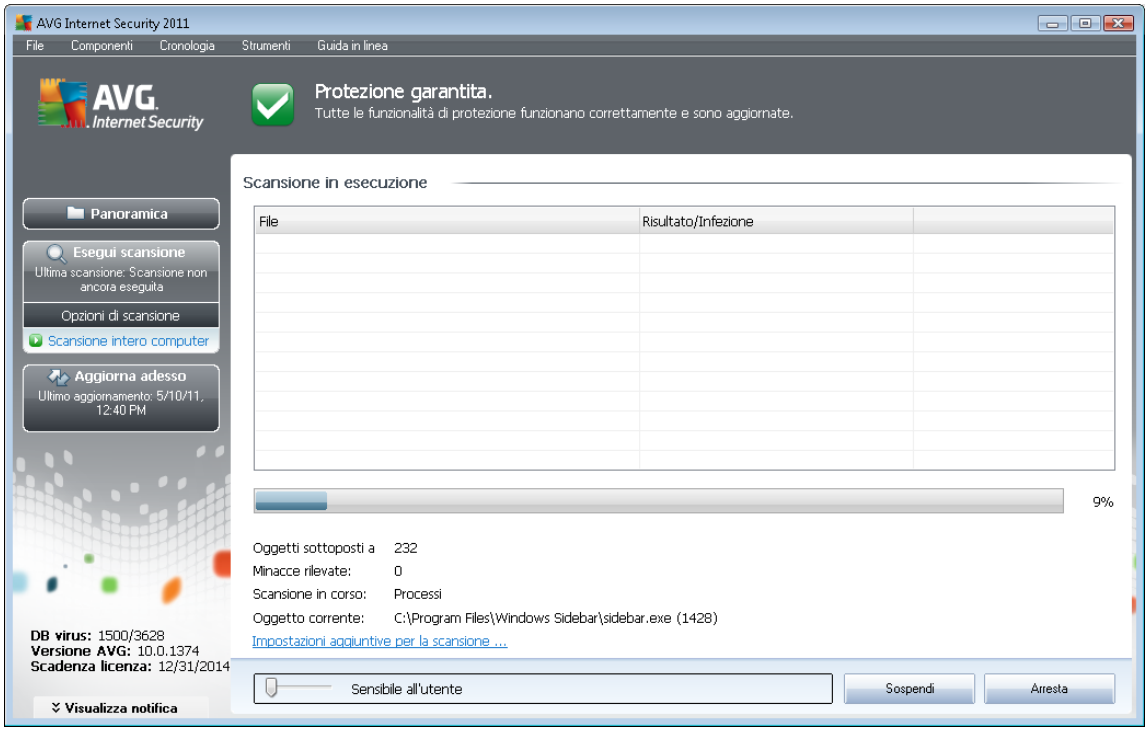
In **AVG Internet Security 2011** sono disponibili i seguenti tipi di scansione predefiniti dal fornitore del software:

11.2.1. Scansione intero computer

Scansione intero computer: consente di eseguire la scansione 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 sposterà l'infezione rilevata in ***Quarantena virus***. È necessario pianificare la scansione completa di una workstation almeno una volta la settimana.

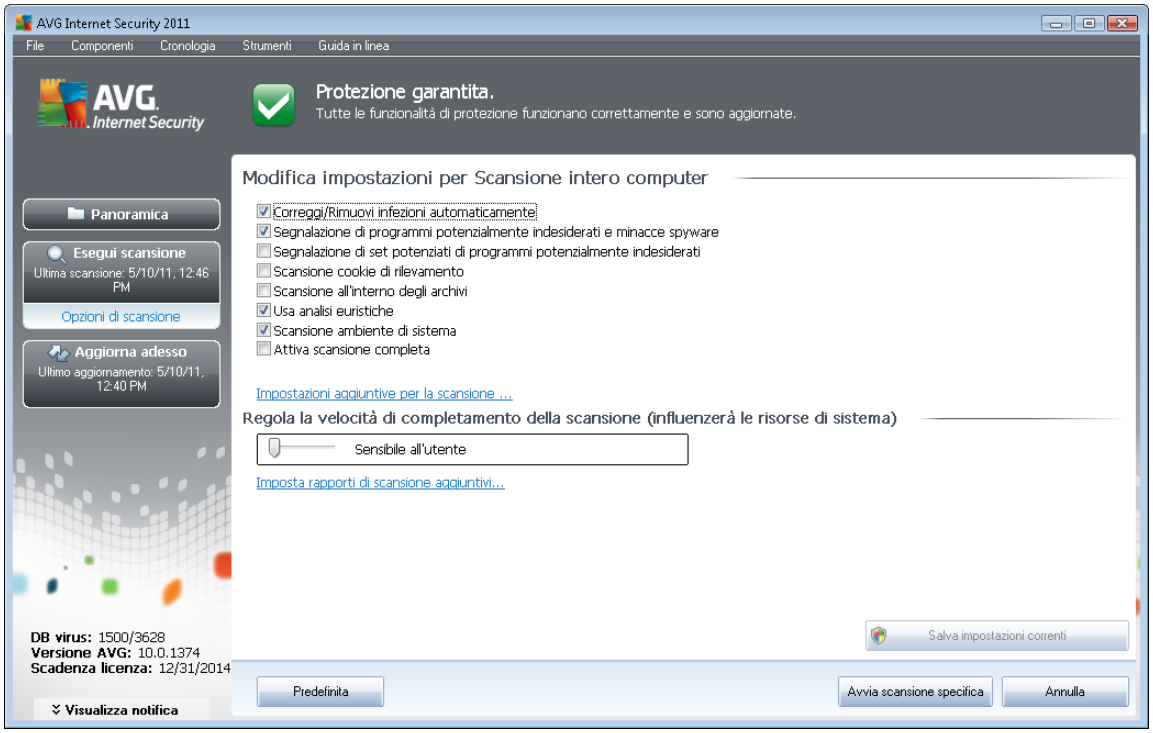
Avvio della scansione

È possibile avviare la ***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***. Selezionare il collegamento ***Modifica impostazioni di scansione*** per accedere alla finestra di dialogo ***Modifica impostazioni di scansione per Scansione intero computer*** *(accessibile dall'interfaccia di scansione tramite il collegamento 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:

  - ***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, 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.

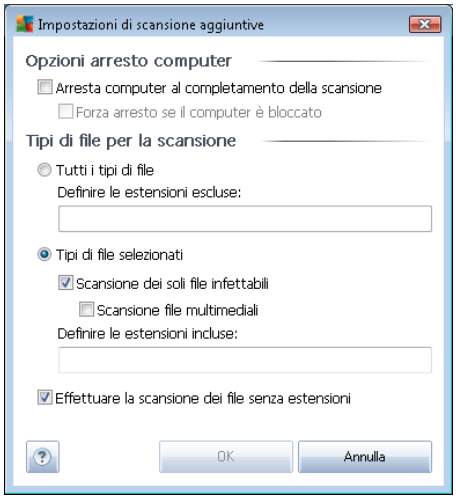
  - ***Segnalazione di set potenziati di programmi potenzialmente indesiderati*** (*disattivata per impostazione predefinita*): selezionare questa casella di controllo per rilevare pacchetti estesi di spyware, programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, 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*** (*disattivata per impostazione predefinita*): 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_** (*disattivata per impostazione predefinita*): 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_** (*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.
- **_Attiva scansione completa_** (*disattivata per impostazione predefinita*): in situazioni specifiche (*ad esempio se si sospetta che il computer sia stato infettato*) per maggiore sicurezza è possibile selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno anche le aree del computer che difficilmente vengono infettate. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.

- **_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:

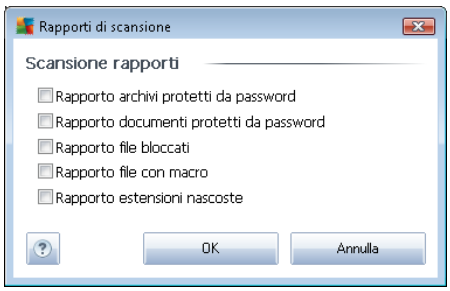
- ***Tutti i tipi di file*** con la possibilità di definire le eccezioni fornendo un elenco di estensioni di file separate da virgola da non sottoporre a scansione;

- ***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.

- ***Regola la velocità di completamento della scansione***: è possibile utilizzare il dispositivo di scorrimento per modificare la priorità del processo di scansione. Per impostazione predefinita, questa opzione è impostata sul livello *sensibile all'utente per l'utilizzo automatico delle risorse.* In alternativa, è possibile eseguire il processo di scansione più lentamente in modo da ridurre al minimo il carico sulle risorse di sistema (*utile quando è necessario lavorare al computer ma la durata della scansione non influisce*) o più velocemente con utilizzo delle risorse di sistema più elevato (*ad esempio quando l'utente è temporaneamente lontano dal computer*).

- ***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

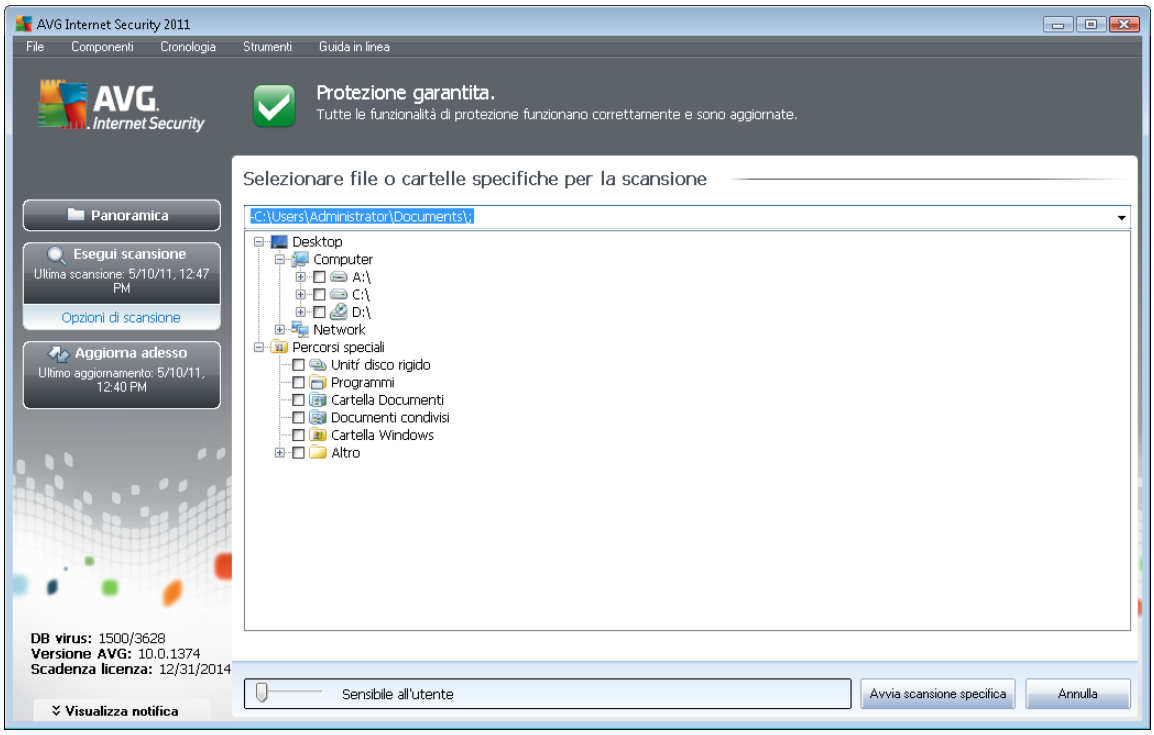
Scansione file o cartelle specifiche: consente di eseguire la scansione delle sole aree del computer selezionate per la scansione (*cartelle, dischi rigidi, dischi floppy, CD selezionati e così via*). L'avanzamento della scansione nel caso di rilevamento di virus e relativo trattamento è uguale a quello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

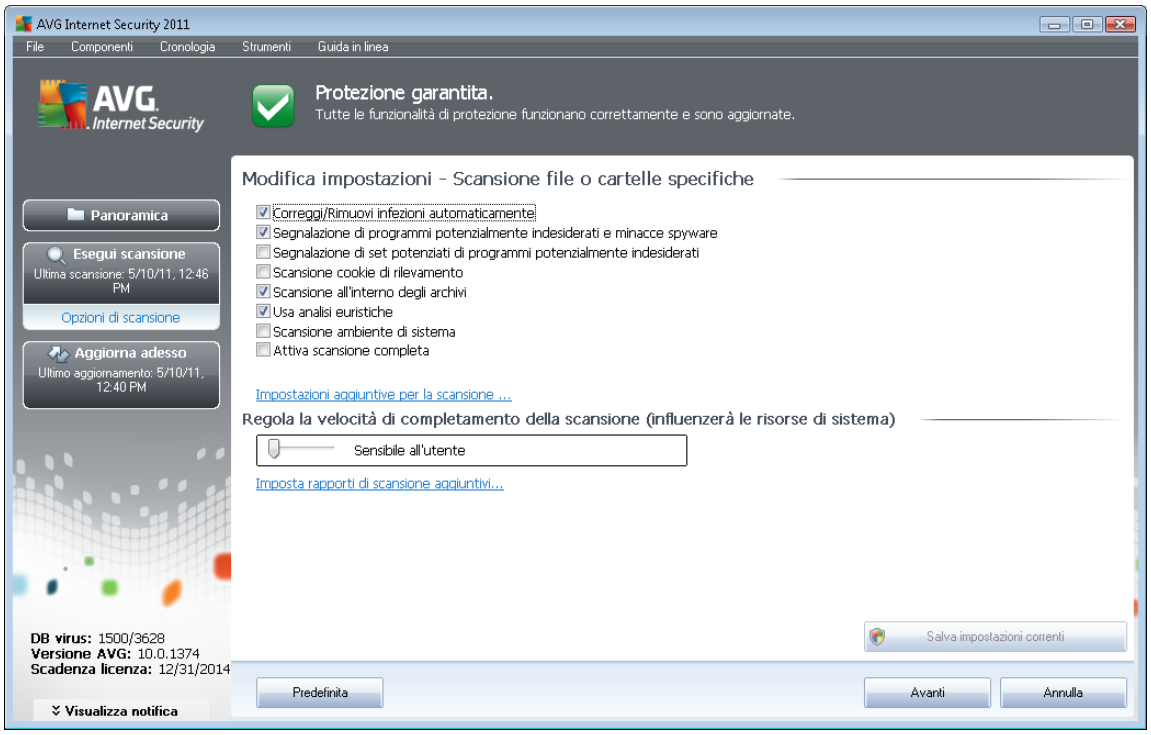
È possibile sottoporre a scansione una specifica cartella escludendo tutte le sottocartelle relative; a questo scopo scrivere un segno meno "**-**" davanti al percorso generato automaticamente (*vedere la schermata*). Per escludere l'intera cartella dalla scansione, utilizzare il parametro "**!**".

Infine, per avviare la scansione, selezionare 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***. Selezionare 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***: dall'elenco dei parametri di scansione è possibile attivare/disattivare parametri specifici in base alle esigenze:

    - ***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, 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*** (*disattivata per impostazione predefinita*): selezionare questa casella di controllo 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_** (*disattivata per impostazione predefinita*): 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*).

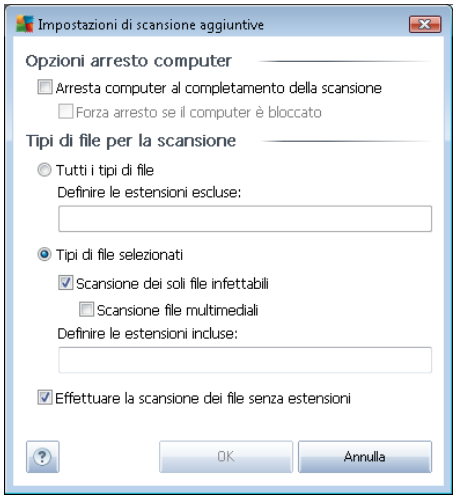
- **_Scansione all'interno degli archivi_** (*attivata per impostazione predefinita*): questo parametro stabilisce che la scansione deve controllare tutti i file anche quelli inclusi all'interno di un archivio, quale ZIP, RAR e così via

- **_Usa analisi euristiche_** (*disattivata 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_** (*disattivata per impostazione predefinita*): la scansione verrà eseguita anche sulle aree di sistema del computer.

- **_Attiva scansione completa_** (*disattivata per impostazione predefinita*): in situazioni specifiche (*ad esempio se si sospetta che il computer sia stato infettato*) per maggiore sicurezza è possibile selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno anche le aree del computer che difficilmente vengono infettate. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.

- **_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:



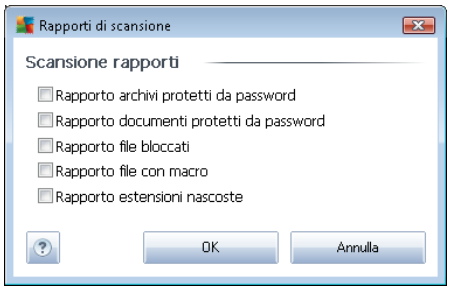
- **_Opzioni arresto computer_**: consente di decidere se il computer deve essere arrestato automaticamente al termine del processo di scansione. Dopo aver confermato questa opzione (**_Arresta computer al completamento della scansione_**), viene attivata una nuova opzione che consente l'arresto del 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, questa opzione è impostata sul livello *sensibile all'utente per l'utilizzo automatico delle risorse.* In alternativa, è possibile eseguire il processo di scansione più lentamente in modo da ridurre al minimo il carico sulle risorse di sistema (*utile quando è necessario lavorare al computer ma la durata della scansione non influisce*) o più velocemente con utilizzo delle risorse di sistema più elevato (*ad esempio quando l'utente è temporaneamente lontano dal computer*).

- ***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*

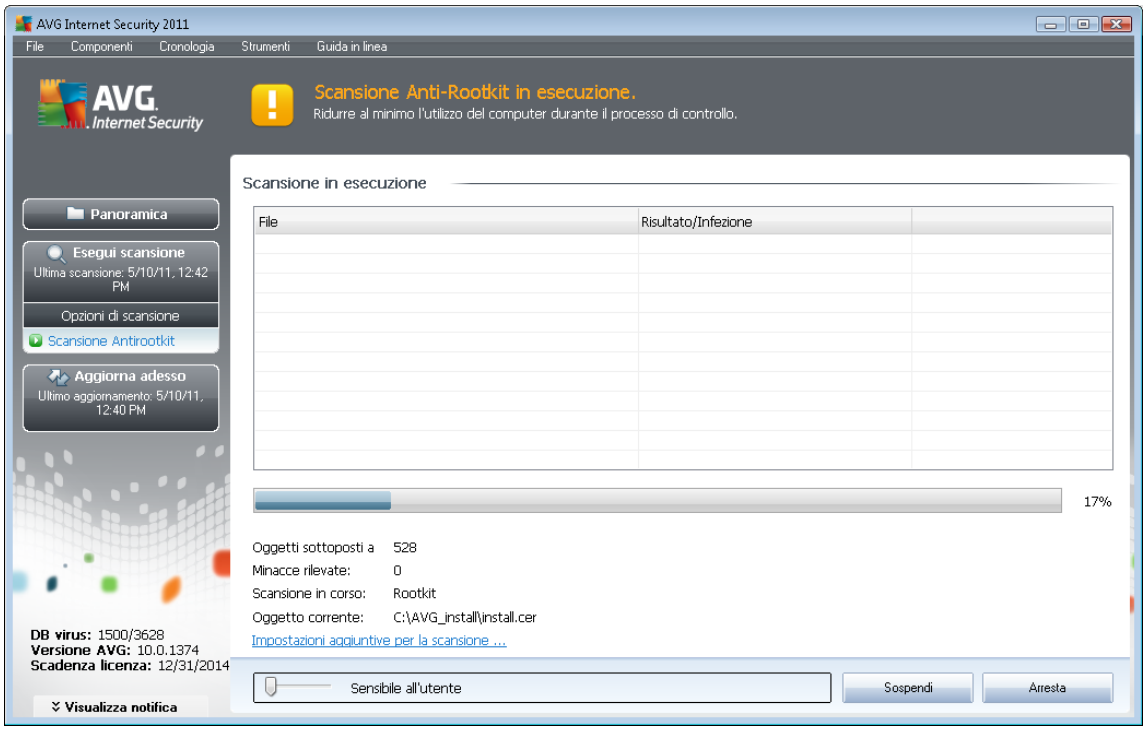
sulla configurazione corrente di Scansione file o cartelle specifiche).

11.2.3. Scansione Anti-Rootkit

La scansione Anti-Rootkit ricerca sul computer la presenza di eventuali rootkit (*programmi e tecnologie in grado di coprire l'attività dei malware nel computer*). Se viene rilevato un rootkit, ciò non significa necessariamente che il computer sia infetto. In alcuni casi, specifici driver o sezioni di applicazioni regolari possono venire rilevati erroneamente come rootkit.

Avvio della scansione

È possibile avviare la scansione Anti-Rootkit 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.



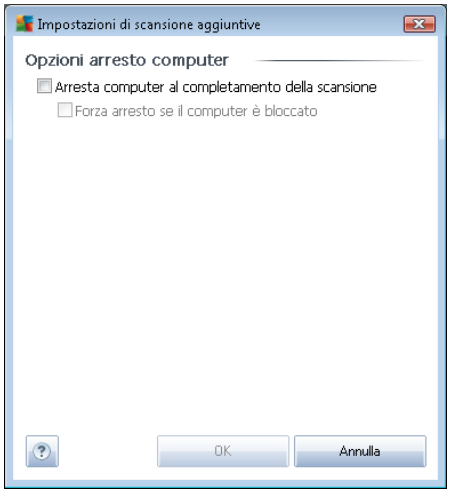
Modifica della configurazione della scansione

La scansione Anti-Rootkit viene sempre avviata in base alle impostazioni predefinite e la modifica dei parametri di scansione è accessibile solo dalla finestra di dialogo ***Impostazioni AVG avanzate / Anti-Rootkit***. Nell'interfaccia di scansione è disponibile la seguente configurazione, ma solo mentre la scansione è in esecuzione:

- ***Scansione automatica***: è possibile utilizzare il dispositivo di scorrimento per modificare la

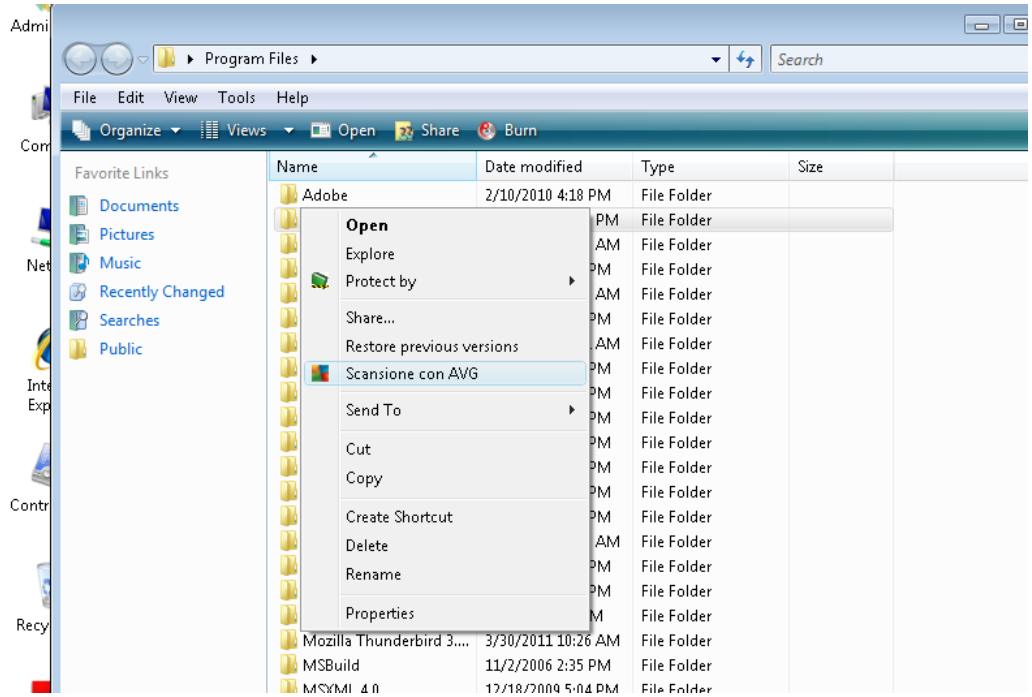
priorità del processo di scansione. Per impostazione predefinita, questa opzione è impostata sul livello *sensibile all'utente per l'utilizzo automatico delle risorse.* In alternativa, è possibile eseguire il processo di scansione più lentamente in modo da ridurre al minimo il carico sulle risorse di sistema (*utile quando è necessario lavorare al computer ma la durata della scansione non influisce*) o più velocemente con utilizzo delle risorse di sistema più elevato (*ad esempio quando l'utente è temporaneamente lontano dal computer*).

- ***Impostazioni di scansione aggiuntive***: questo collegamento apre una nuova finestra di dialogo ***Impostazioni di scansione aggiuntive*** in cui è possibile definire eventuali condizioni per l'arresto del computer correlate alla ***scansione Anti-Rootkit*** (***Arresta computer al completamento della scansione*** *o eventualmente* ***Forza arresto se il computer è bloccato***):



11.3. Scansione in Esplora risorse

Oltre alle scansioni predefinite avviate per l'intero computer o per le aree selezionate, **AVG Internet Security 2011** 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 da riga di comando

In **AVG Internet Security 2011** è possibile eseguire la scansione dalla riga di comando. Ad esempio, è possibile utilizzare questa opzione sui 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 con la maggior parte dei parametri forniti nell'interfaccia utente grafica di AVG.

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 devono 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 di 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 la panoramica dei parametri da 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, alta/ (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)
- ***/ARCBOMBSW*** Segnala file di archivio ricompressi

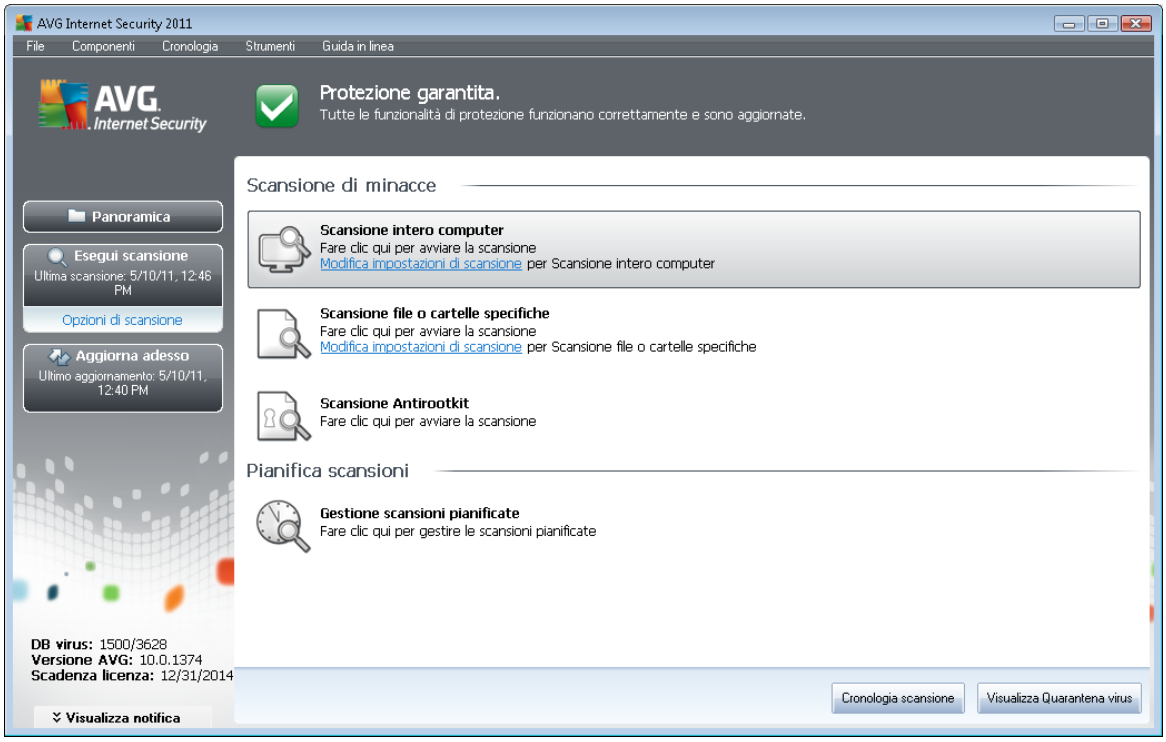
11.5. Pianificazione di scansioni

AVG Internet Security 2011 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 sia protetto da possibili infezioni e non è necessario preoccuparsi dell'avvio della

scansione.

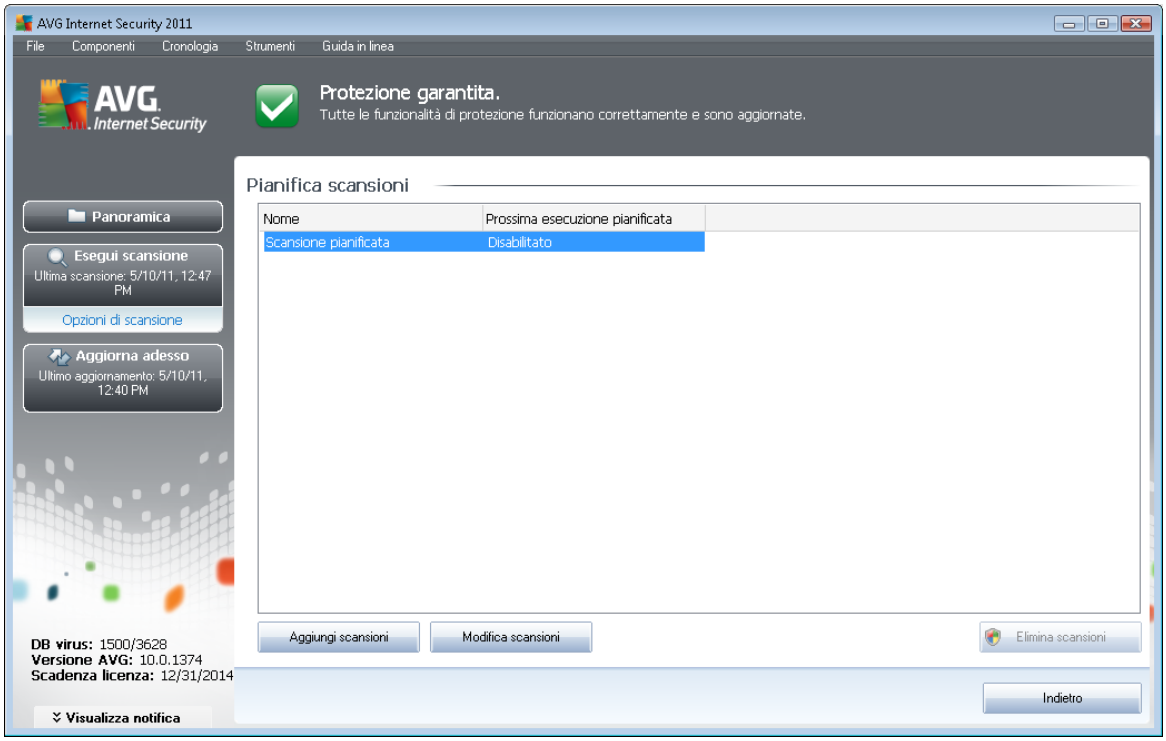
Scansione intero computer deve essere avviata regolarmente, almeno una volta alla settimana. Tuttavia, se possibile, avviare la scansione dell'intero computer ogni giorno, come impostato nella configurazione predefinita della pianificazione della scansione. Se il computer è sempre acceso, è possibile 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 di 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.

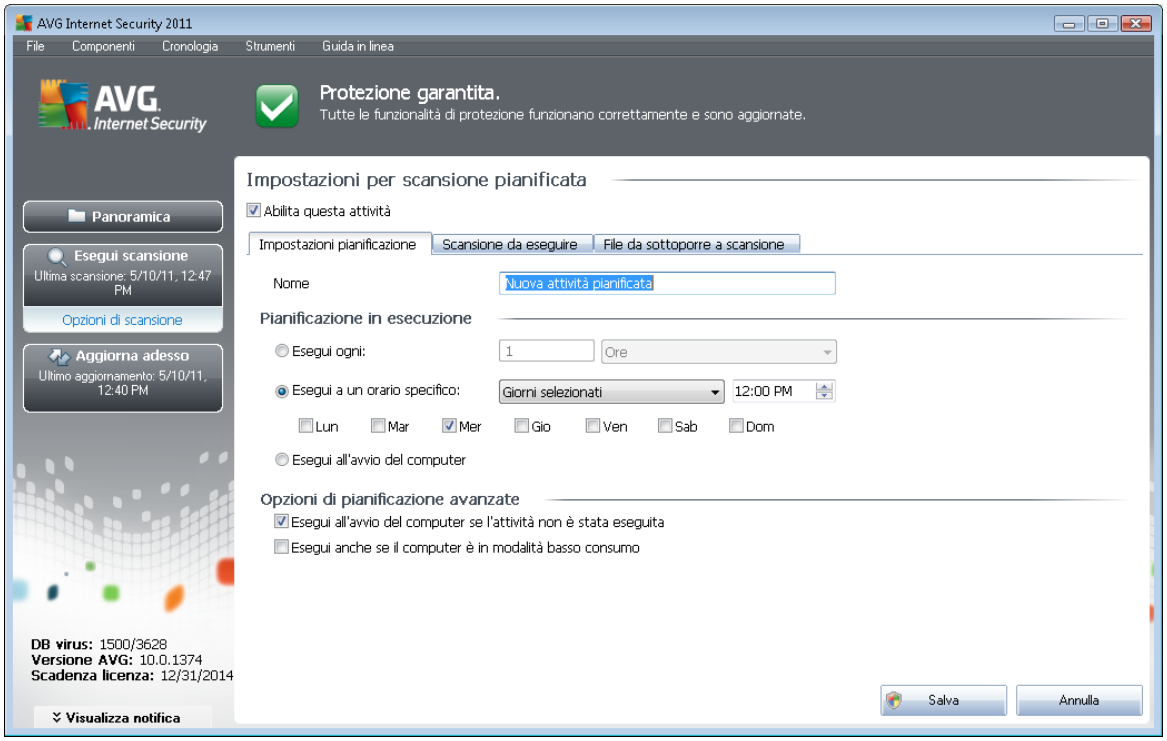
- ***Modifica pianificazione scansione***: il pulsante può essere utilizzato solo se è stato selezionato in precedenza un controllo esistente dall'elenco dei controlli pianificati. In tal caso il pulsante è visualizzato come attivo e, selezionandolo, si passa alla finestra di dialogo ***Impostazioni 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 selezionando il pulsante di controllo. Tuttavia, è possibile rimuovere solo i controlli personali; non è possibile eliminare ***Pianificazione scansione intero computer*** preimpostata 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***. 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.

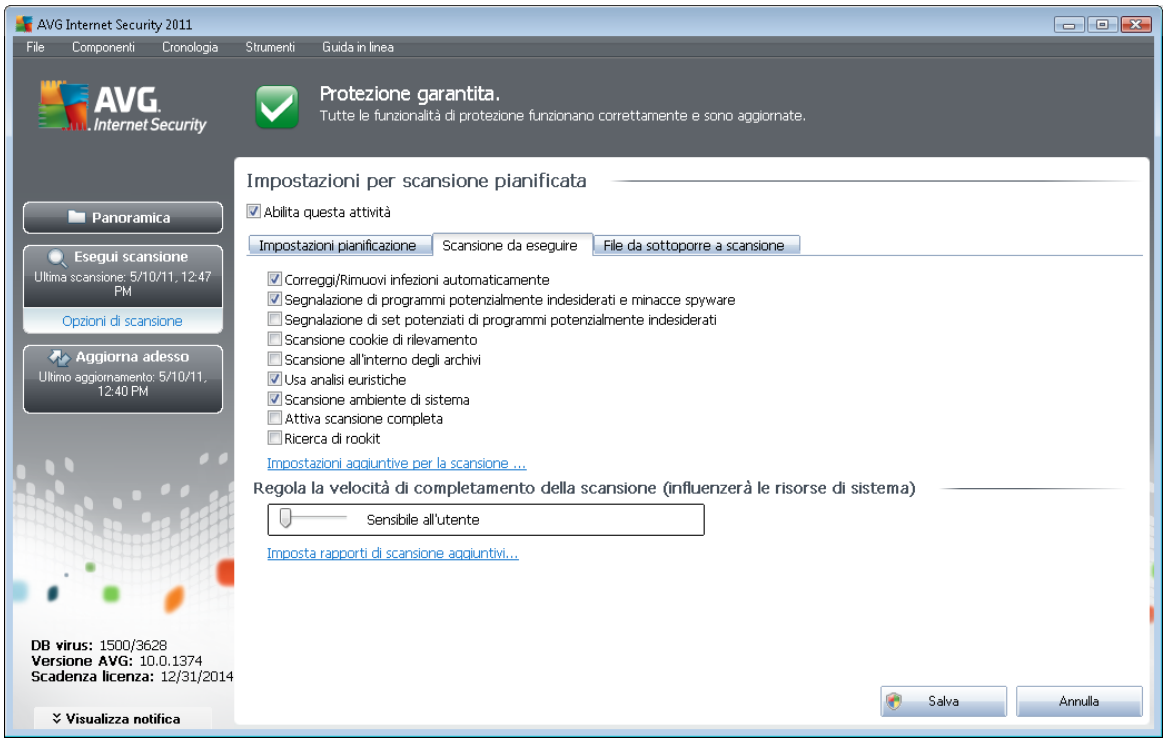
Pulsanti di controllo delle impostazioni per la finestra di dialogo della scansione pianificata

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 non esista un motivo valido 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 della presenza di un virus e si dovrà decidere l'azione da intraprendere sull'infezione rilevata. L'azione consigliata consiste nello spostare 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*** (*disattivata per impostazione predefinita*): selezionare questa casella di controllo 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*** (*disattivata 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*** (*disattivata 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.

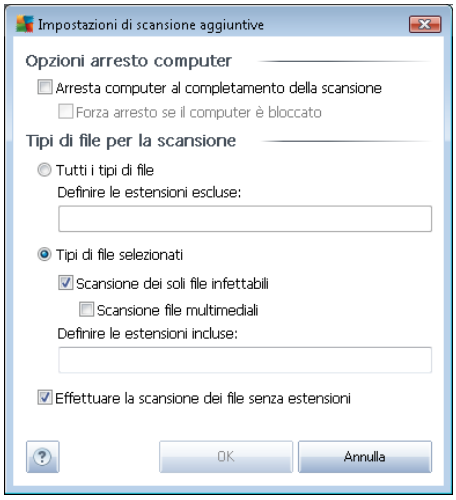
- ***Usa analisi euristiche*** (*attivata per impostazione predefinita*): l'analisi euristica (*emulazione dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale*) sarà uno dei metodi utilizzati per il rilevamento di virus durante la scansione.

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

- ***Attiva scansione completa*** (*disattivata per impostazione predefinita*): in situazioni specifiche (*ad esempio se si sospetta che il computer sia stato infettato*) per maggiore sicurezza è possibile selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno anche le aree del computer che difficilmente vengono infettate. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.

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;

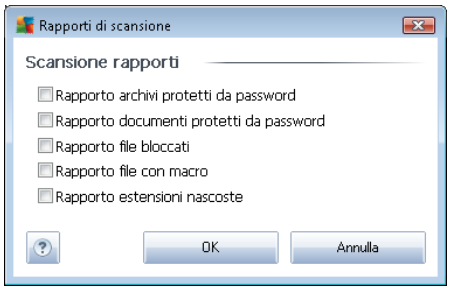
  - ***Tipi di file selezionati***: è possibile specificare che si desidera sottoporre a scansione solo file potenzialmente infettabili (*i file che non possono essere infettati non verranno sottoposti a scansione, ad esempio alcuni file di testo normale o altri file non eseguibili*), inclusi i file multimediali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

- ***Regola la velocità di completamento della scansione***: è possibile utilizzare il dispositivo di scorrimento per modificare la priorità del processo di scansione. Per impostazione predefinita, questa opzione è impostata sul livello *sensibile all'utente per l'utilizzo automatico delle risorse.* In alternativa, è possibile eseguire il processo di scansione più lentamente in modo da ridurre al minimo il carico sulle risorse di sistema (*utile quando è necessario lavorare al computer ma la durata della scansione non influisce*) o più velocemente con utilizzo delle risorse di sistema più elevato (*ad esempio quando l'utente è*

temporaneamente lontano dal computer).

- ***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 esista un motivo valido per modificare l'impostazione della scansione, si consiglia di mantenere la configurazione predefinita. Le eventuali modifiche alla configurazione devono essere eseguite solo da utenti esperti. Per ulteriori opzioni di configurazione della scansione vedere la finestra di dialogo* ***Impostazioni avanzate*** *accessibile dalla voce del menu di sistema* ***Strumenti / Impostazioni avanzate****.*

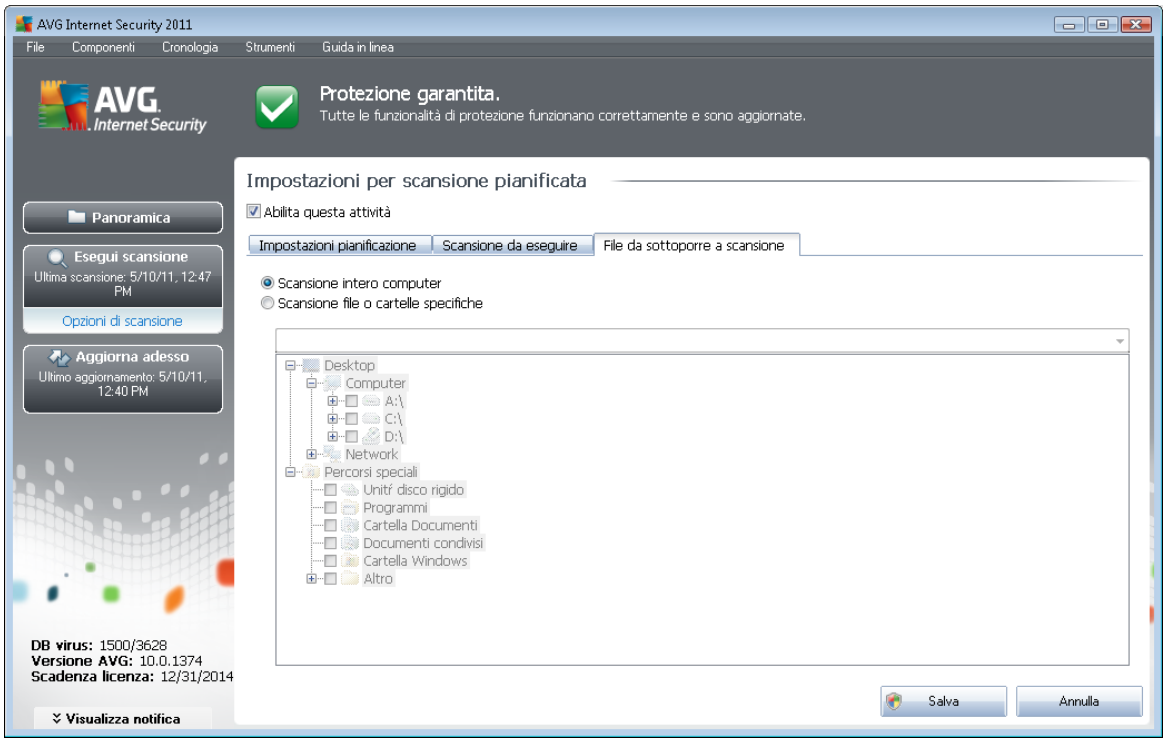
Pulsanti di controllo

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\
    - *nella versione a 64 bit* C:\Programmi (x86)
- ***Cartella Documenti***

- *per Windows XP:* C:\Documents and Settings\utente predefinito\Documenti\
- *per Windows Vista/7*: C:\Users\utente\Documenti\

- ***Documenti condivisi***
  - *per Windows XP*: C:\Documents and Settings\All Users\Documenti condivisi\
  - *per Windows Vista/7*: C:\Users\Public\Documenti condivisi\

- ***Cartella Windows***: C:\Windows\

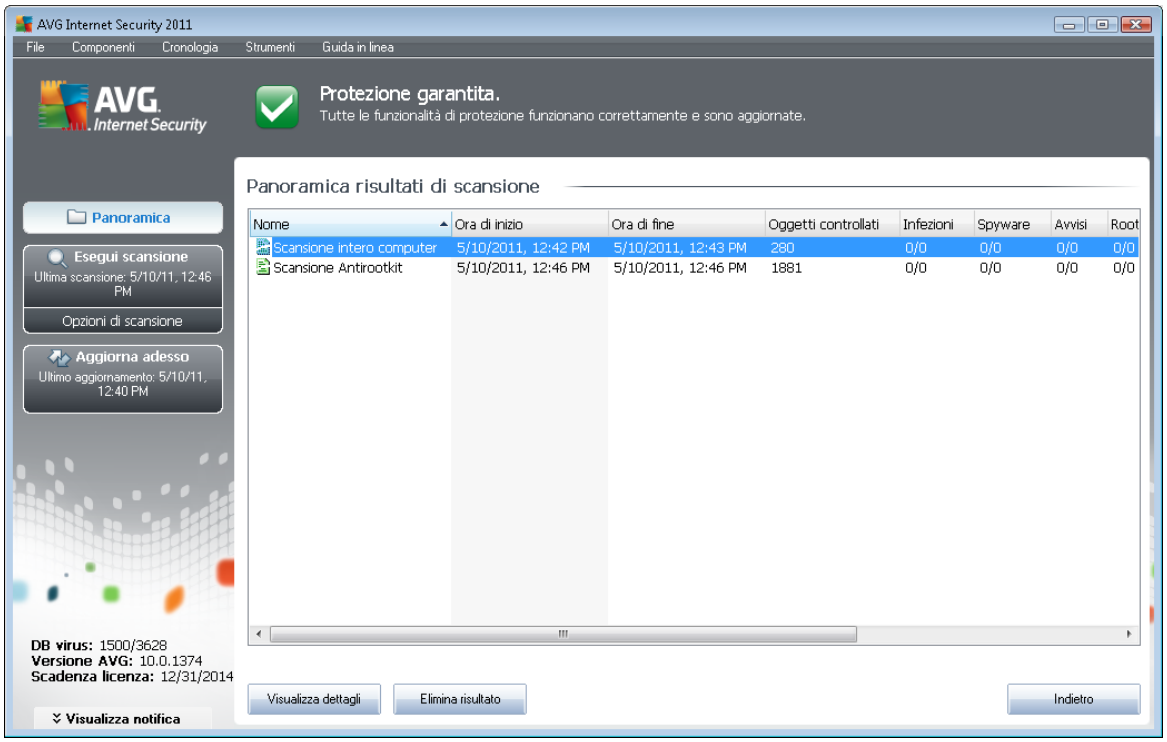
- ***Altro***
  - *Unità di sistema*: disco rigido su cui è installato il sistema operativo (solitamente C:)
  - *Cartella di sistema*: C:\Windows\System32\
  - *Cartella file temporanei*: C:\Documents and Settings\utente\Local\ (*Windows XP*) oppure C:\Users\utente\AppData\Local\Temp\ (*Windows Vista/7*)
  - *File temporanei di Internet*: C:\Documents and Settings\utente\Local Settings\Temporary Internet Files\ (*Windows XP*); oppure C:\Users\utente\AppData\Local\Microsoft\Windows\Temporary Internet Files (*Windows Vista/7*)

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.

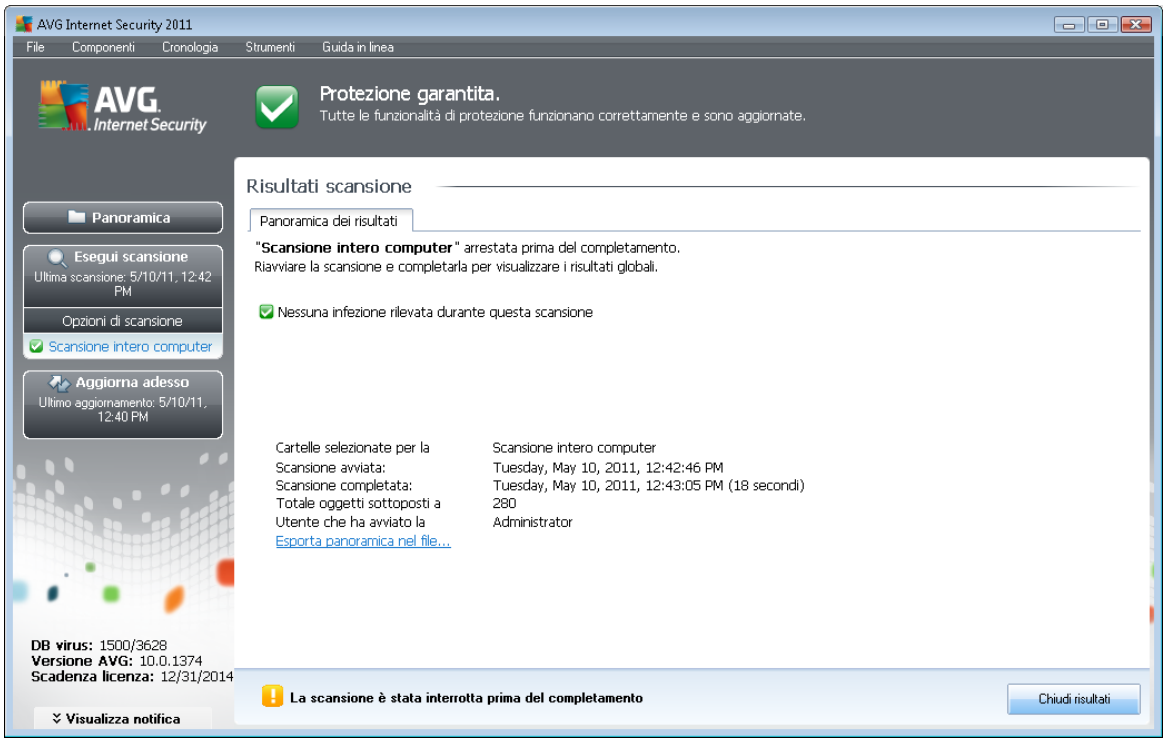
La finestra di dialogo è suddivisa in altre schede:

- ***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

- ***Rootkit***: questa scheda viene visualizzata solo se durante la scansione sono stati rilevati rootkit

- ***Informazioni:*** questa scheda viene visualizzata solo se sono state rilevate alcune potenziali minacce non classificabili in nessuna delle categorie suddette; nella scheda viene visualizzato un messaggio di avviso sul rilevamento. 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

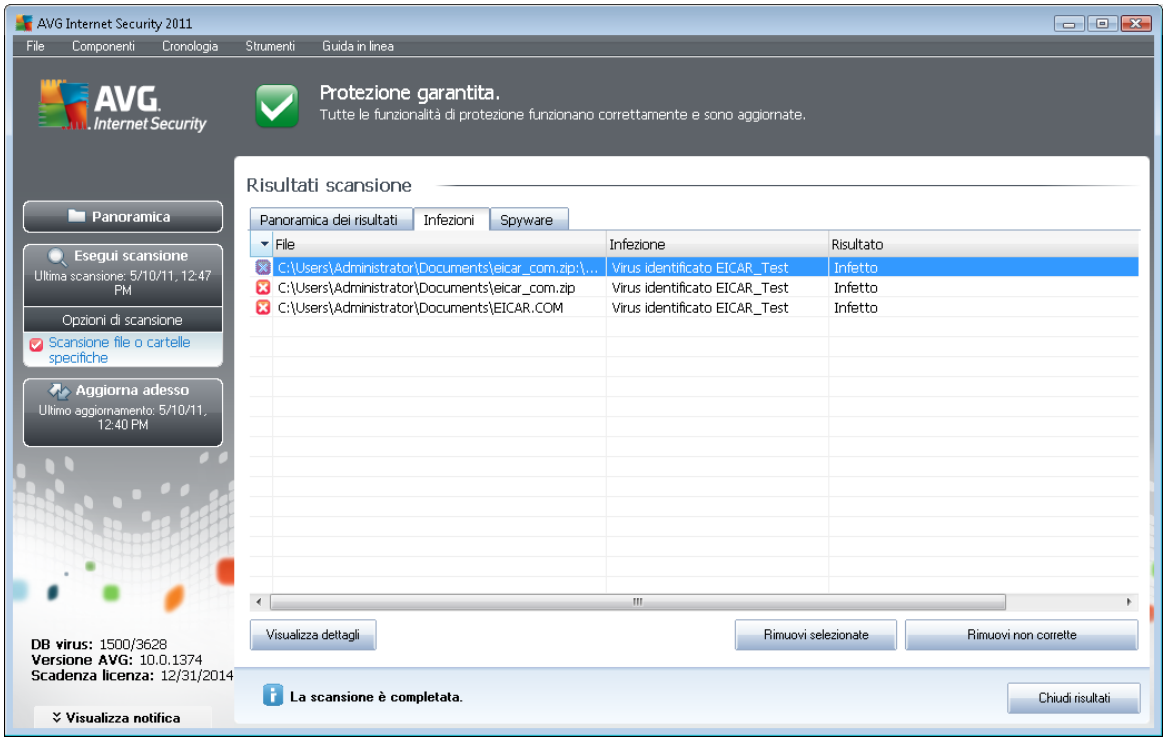
- numero di infezioni da virus / spyware che non è possibile rimuovere o correggere

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 bloccato pertanto AVG non è in grado di sottoporlo a scansione

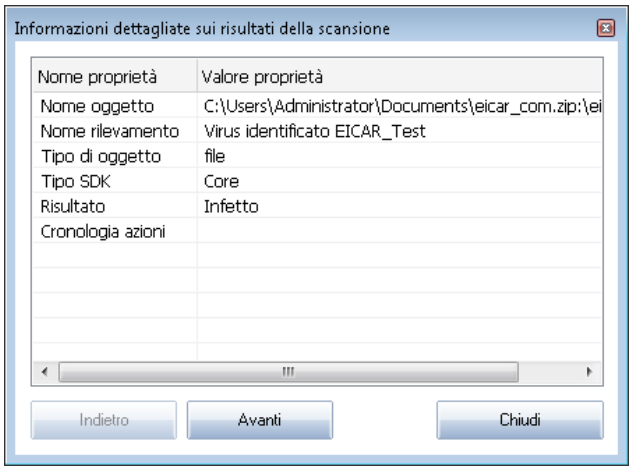
- ***Oggetto potenzialmente pericoloso***: l'oggetto è stato rilevato come potenzialmente pericoloso ma non infetto (*potrebbe contenere macro, ad esempio*); l'informazione deve essere considerata solo come un avviso

- ***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 relativa alle ***informazioni dettagliate sull'oggetto***:



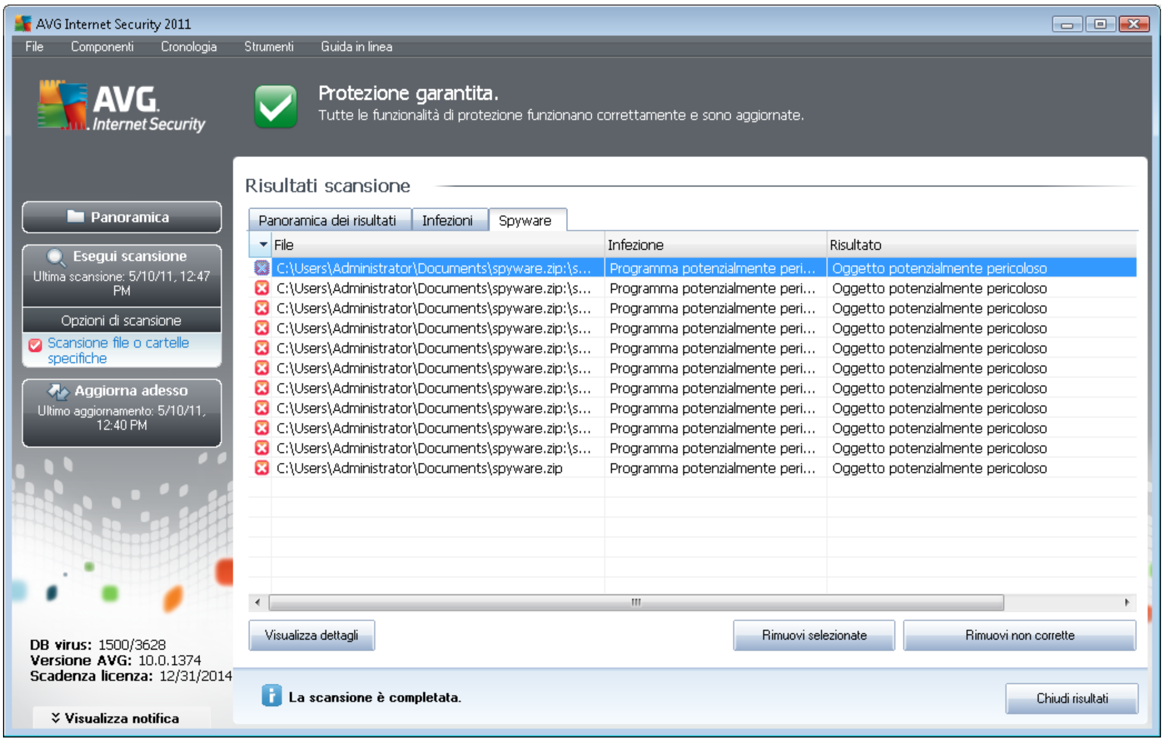
  In questa finestra di dialogo sono disponibili informazioni dettagliate sull'oggetto infetto rilevato (*ad esempio nome e posizione dell'oggetto infetto, tipo di oggetto, tipo di SDK, risultato del rilevamento e cronologia delle azioni correlate all'oggetto rilevato*). I pulsanti ***Indietro*** / ***Avanti*** consentono di visualizzare informazioni su rilevamenti specifici. Utilizzare il pulsante ***Chiudi*** per chiudere questa finestra di dialogo.

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

- ***Rimuovi non corrette***: questo pulsante consente di eliminare tutti gli oggetti rilevati che non possono essere corretti né 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 sono stati rilevati [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 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 pertanto AVG non è in grado di sottoporlo a scansione

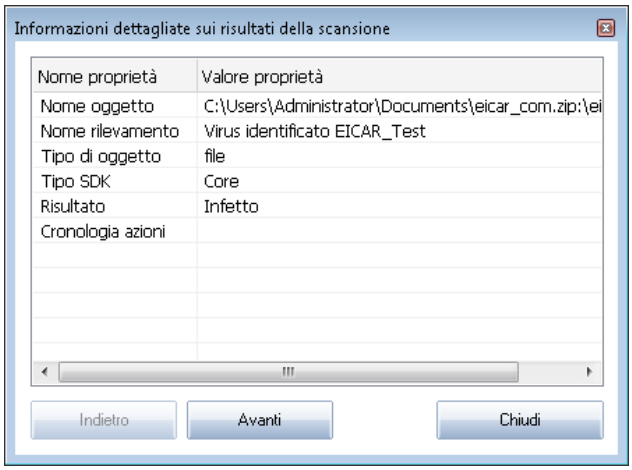
- ***Oggetto potenzialmente pericoloso***: l'oggetto è stato rilevato come potenzialmente pericoloso ma non infetto (potrebbe contenere macro, ad esempio); l'informazione deve essere considerata solo come un avviso

- ***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 relativa alle ***informazioni dettagliate sull'oggetto***:



  In questa finestra di dialogo sono disponibili informazioni dettagliate sull'oggetto infetto rilevato (*ad esempio nome e posizione dell'oggetto infetto, tipo di oggetto, tipo di SDK, risultato del rilevamento e cronologia delle azioni correlate all'oggetto rilevato*). I pulsanti ***Indietro*** / ***Avanti*** consentono di visualizzare informazioni su rilevamenti specifici. Utilizzare il pulsante ***Chiudi*** per uscire da questa finestra di dialogo.

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

- ***Rimuovi non corrette***: questo pulsante consente di eliminare tutti gli oggetti rilevati che non possono essere corretti né 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***.

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 dovrà assumere 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 di poter essere eseguiti in tutta sicurezza sui sistemi. Le tecniche utilizzate a questo scopo possono includere l'occultamento di processi in esecuzione dai 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*).

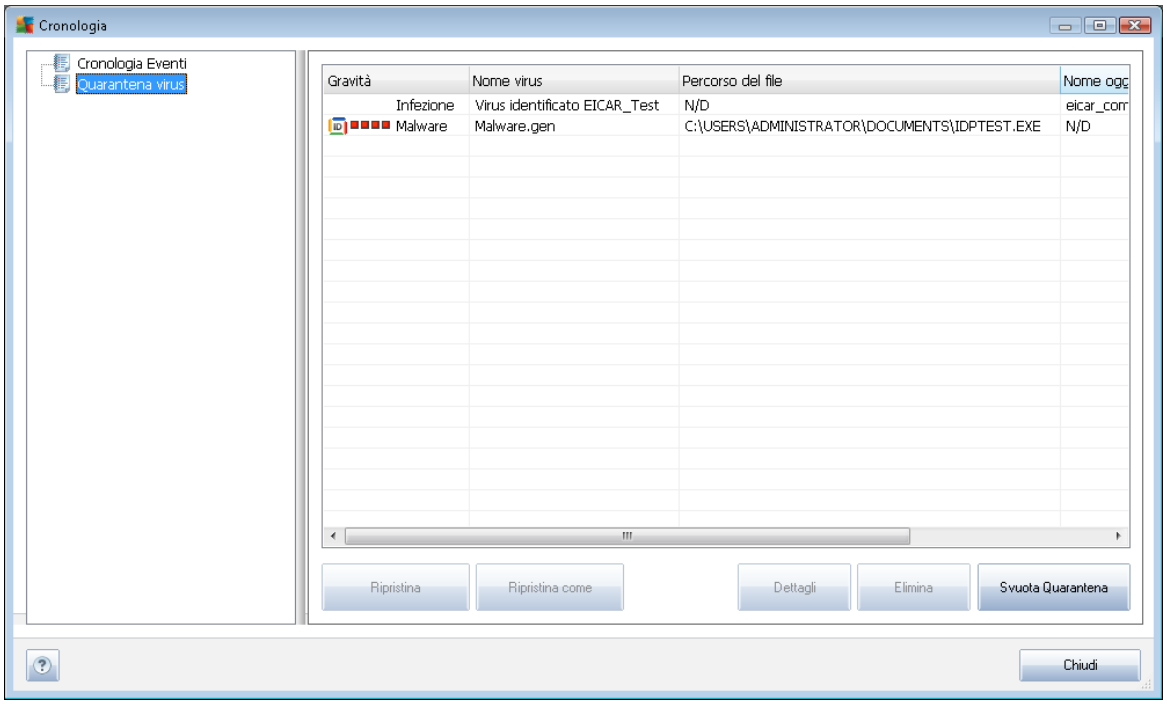
- ***Documenti con macro***: il documento segnalato contiene macro che possono essere dannose.

- ***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



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 elaborazione. 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 di ***Quarantena virus*** viene aperta in una finestra separata e offre una panoramica delle informazioni relative agli oggetti infetti messi in quarantena:

- ***Gravità***: se è stato installato il componente ***Identity Protection*** in **AVG Internet Security 2011**, questa sezione fornirà l'identificazione grafica della gravità del rilevamento in base a una scala a quattro livelli dal più sicuro (■□□□) al più pericoloso (■■■■) e informazioni sul tipo di infezione (*in base al livello di infezione; tutti gli oggetti elencati possono essere sicuramente 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*

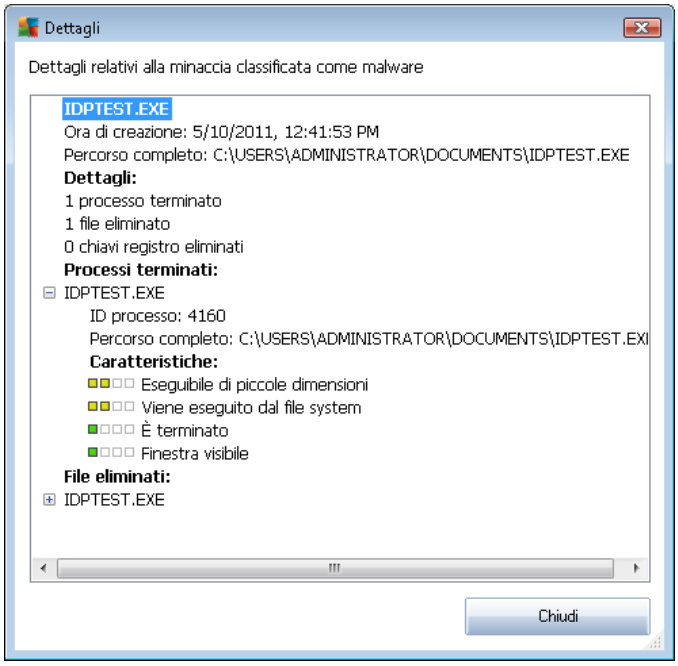
allegato e-mail che non corrisponde al contenuto effettivo dell'allegato), tale nome verrà visualizzato in questa colonna.

- ***Data di archiviazione***: data e ora del rilevamento e dell'inserimento in ***Quarantena virus***

Pulsanti di controllo

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

- ***Ripristina***: consente di ripristinare il file infetto nella posizione originale sul disco
- ***Ripristina come***: sposta il file infetto nella cartella selezionata
- ***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 ombreggiato e non attivo.



- ***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 immediatamente.

Poiché gli aggiornamenti di AVG non vengono rilasciati in base ad alcuna 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 o più spesso. Solo in questo modo è possibile assicurarsi che **AVG Internet Security 2011** venga mantenuto aggiornato anche durante la 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 si rende disponibile.

- ***In Aggiornamento programma*** sono contenuti le modifiche, le correzioni e i miglioramenti del programma.

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 viene effettuata alcuna operazione.

12.3. Processo di aggiornamento

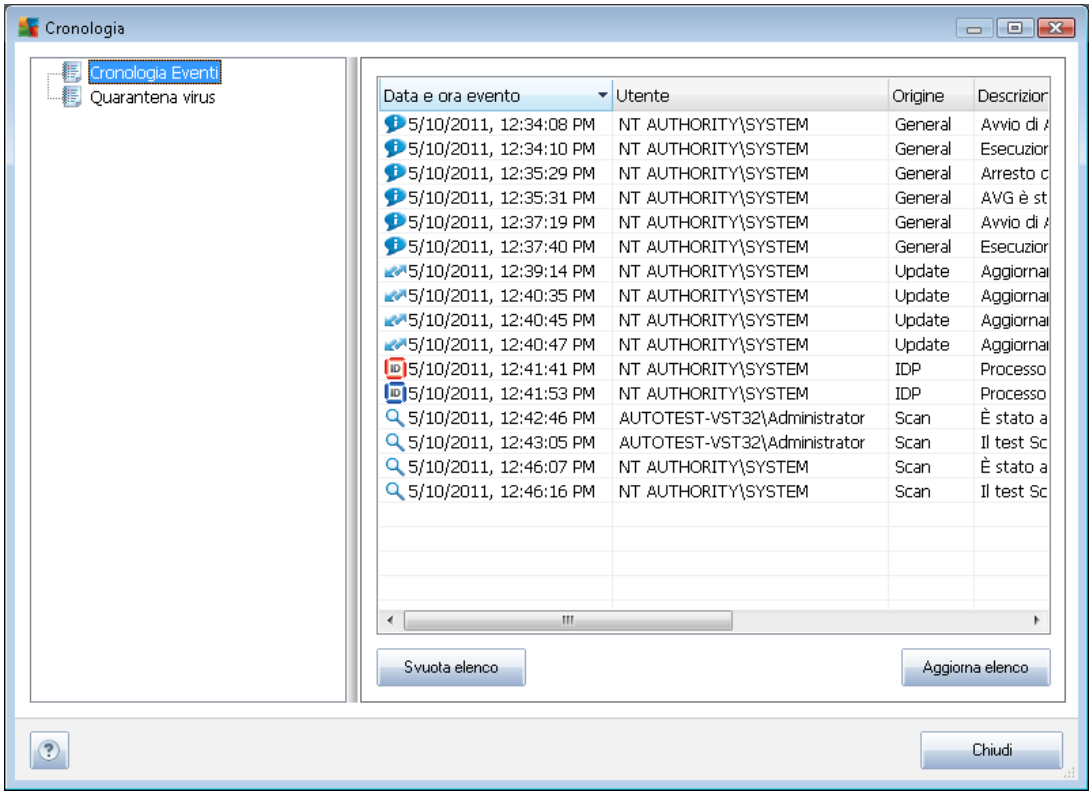
Il processo di aggiornamento può essere avviato immediatamente in base alle necessità dal collegamento rapido ***Aggiorna subito***. Questo collegamento è sempre disponibile da tutte le finestre di dialogo dell'interfaccia utente di AVG. Tuttavia, si consiglia di eseguire questi aggiornamenti a cadenza 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*** 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 Internet Security 2011**. Nella ***Cronologia*** 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 della scansione*) inclusa la posizione in cui si sono verificati
- Altri eventi importanti

Per ciascun evento vengono indicate le seguenti informazioni:

- ***Data e ora evento*** indica la data e l'ora esatte in cui si è verificato l'evento
- ***Utente*** indica chi ha dato inizio all'evento
- ***Origine*** indica il componente di origine o altre parti del sistema AVG che hanno attivato l'evento

- ***Descrizione evento*** offre un breve riepilogo dell'evento che si è verificato

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. Domande frequenti 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/).

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***.