AVG File Server 2011

Manuale per l'utente

Revisione documento 2011.01 (20. 9. 2010)

Copyright AVG Technologies CZ, s.r.o. Tutti i diritti riservati.
Tutti gli altri marchi appartengono ai rispettivi proprietari.

Questo prodotto utilizza l'algoritmo RSA Data Security, Inc. MD5 Message-Digest, Copyright (C) 1991-2, RSA Data Security, Inc. Creazione 1991.
Questo prodotto utilizza il codice dalla libreria C-SaCzech, Copyright (c) 1996-2001 Jaromir Dolecek (dolecek@ics.muni.cz).
Questo prodotto utilizza la libreria di compressione zlib, Copyright (c) 1995-2002 Jean-loup Gailly e Mark Adler
Questo prodotto utilizza la libreria di compressione libbzip2, Copyright (c) 1996-2002 Julian R. Seward.

Sommario

1. Introduzione

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

Complimenti per l'acquisto di AVG File Server 2011!

AVG File Server 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 File Server 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 File Server 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

AVG File Server 2011 © 2010 Copyright AVG Technologies CZ, s.r.o. Tutti i diritti riservati.

2. Requisiti per l'installazione di AVG

2.1. Sistemi operativi supportati

AVG File Server 2011 è destinato alla protezione di workstation/server che eseguono i seguenti sistemi operativi:

- Windows 2003 Server e Windows 2003 Server x64 Edition
- Windows 2008 Server e Windows 2008 Server x64 Edition

(ed eventuali Service Pack successivi per sistemi operativi specifici)

2.2. Requisiti hardware minimi e consigliati

Requisiti hardware minimi per **AVG File Server 2011**:

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

Requisiti hardware consigliati per **AVG File Server 2011**:

- CPU Intel Pentium da 1,8 GHz
- 512 MB di memoria RAM
- 600 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 File Server 2011.

Durante il processo di installazione verrà richiesto il numero di licenza. 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.

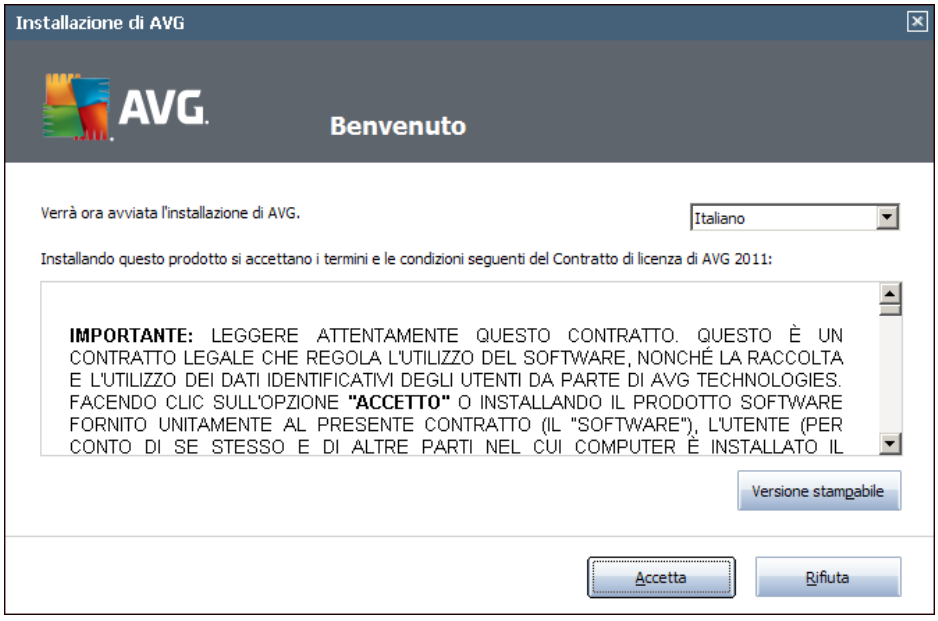
4. Processo di installazione di AVG

Per installare **AVG File Server 2011** nel computer è necessario disporre del file di installazione più recente. È possibile utilizzare il file di installazione nel CD in dotazione con il prodotto; tuttavia questo file potrebbe non essere aggiornato. Pertanto, è consigliabile procurarsi il file di installazione più recente in linea. È possibile scaricare il file dal sito Web di AVG (http://www.avg.com), 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:



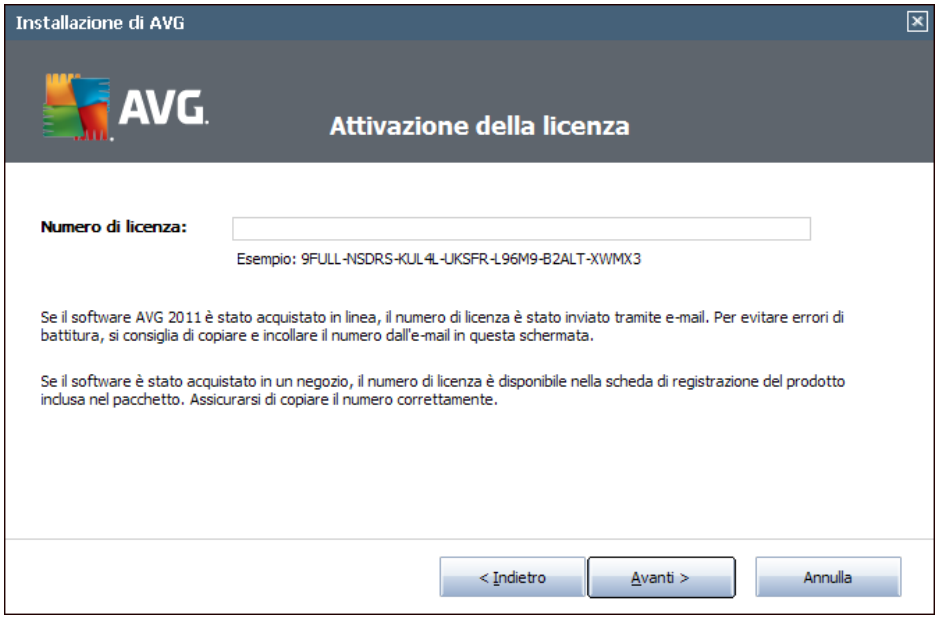
Attenzione: *in questa fase viene selezionata la lingua per il processo di installazione. La lingua selezionata verrà installata come lingua predefinita per l'interfaccia utente di AVG, insieme all'inglese che viene installato automaticamente. Per installare lingue aggiuntive per l'interfaccia utente, specificarle nella finestra di dialogo* ***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 File Server 2011** . Il numero di licenza sarà contenuto nel messaggio e-mail di conferma ricevuto dopo l'acquisto in linea di **AVG File Server 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

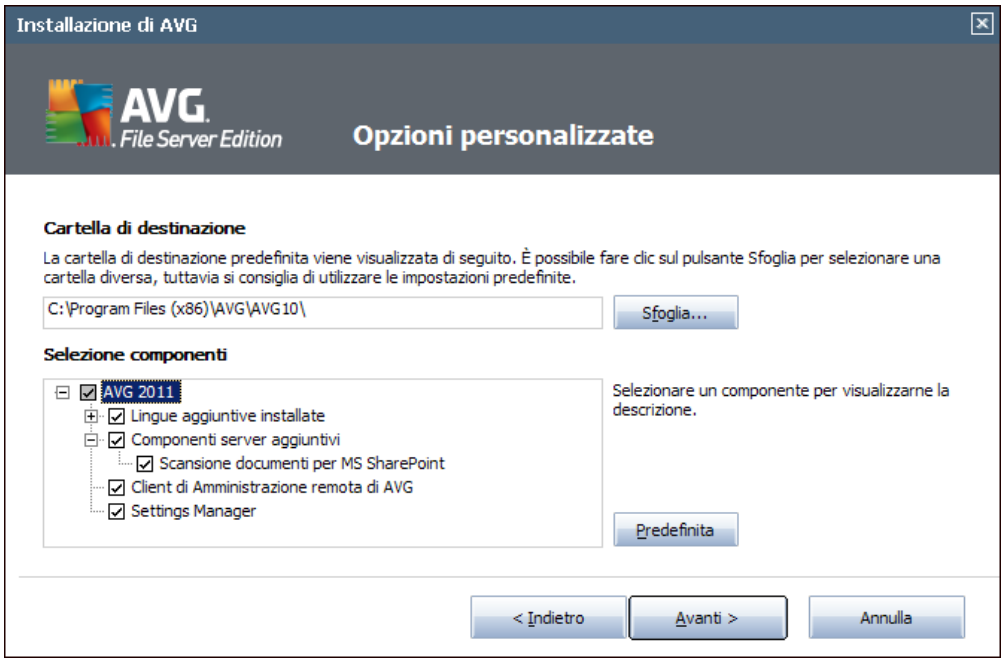
La finestra di dialogo ***Selezionare il tipo di installazione*** offre due opzioni di installazione: ***Installazione rapida*** e ***Installazione personalizzata***.

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 ***Avanzamento dell'installazione***.

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***.

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 File Server 2011** deve essere installato. Per impostazione predefinita, AVG viene installato nella cartella dei programmi che si trova nell'unità C:. Se la cartella non esiste, in una nuova finestra di dialogo verrà richiesto di confermare che si consente a AVG di creare tale cartella. Se si desidera modificare questa posizione, utilizzare il pulsante ***Sfoglia*** per visualizzare la struttura dell'unità e selezionare la cartella pertinente.

Selezione componenti

La sezione ***Selezione componenti*** visualizza una panoramica di tutti i componenti di **AVG File Server 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.

- ***Selezione lingua***

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

- ***Componenti server aggiuntivi - Scansione documenti per MS SharePoint***

  Questo componente esegue la scansione dei documenti memorizzati in MS SharePoint e protegge da possibili minacce. Si tratta di una parte fondamentale di **AVG File Server 2011**, pertanto si consiglia di installarlo.

- ***AVG Amministrazione remota Client***

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

- ***Settings Manager***

  AVG Settings Manager è una piccola applicazione che consente di configurare in modo rapido e semplice le installazioni di AVG locali (anche quelle che non vengono eseguite con Amministrazione remota). Utilizza file di configurazione (in formato .pck) che possono essere creati facilmente utilizzando AVG Settings Manager in qualsiasi computer su cui sia installata l'applicazione AVG. È quindi possibile copiare questi file su qualsiasi dispositivo rimovibile e utilizzarli su tutti i computer. Naturalmente questo è valido anche per AVG Settings Manager stesso. Per ulteriori informazioni su questa applicazione, fare clic **qui**.

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

4.5. Avanzamento dell'installazione

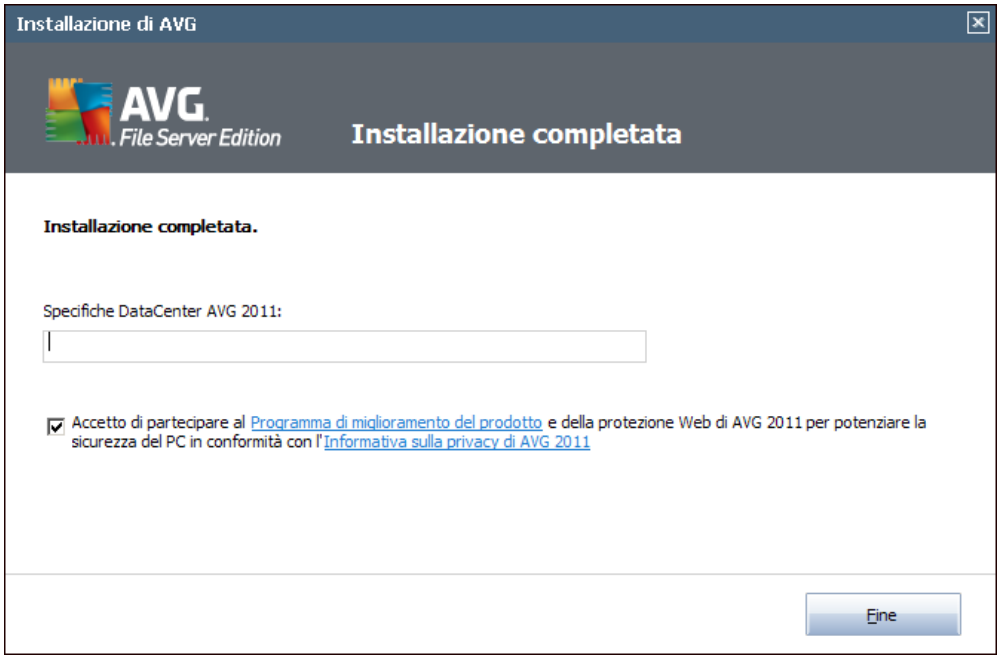
Nella finestra di dialogo ***Avanzamento dell'installazione*** viene visualizzato l'avanzamento del processo di installazione. Non è necessario alcun intervento da parte dell'utente.

Dopo il completamento del processo di installazione, il database dei virus e il programma verranno aggiornati automaticamente. Si passerà quindi alla successiva finestra di dialogo.

4.6. Installazione completata

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

Se in precedenza è stata selezionata l'installazione di AVG Amministrazione remota Client (vedere Opzioni personalizzate), la finestra di dialogo appare con la seguente interfaccia:



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).

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.

5. Dopo l'installazione

5.1. Registrazione del prodotto

Una volta completata l'installazione di **AVG File Server 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
- dal menu ***Start/Programmi/AVG 2011/Interfaccia utente di 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 File Server 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. Configurazione predefinita di AVG

La configurazione predefinita (*ovvero la modalità di impostazione dell'applicazione dopo l'installazione*) di **AVG File Server 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 File Server 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 >>

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 File Server 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 File Server 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
- ***Componenti server***: visualizza una panoramica dei componenti di protezione disponibili e del relativo stato - dettagli >>
- ***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 >>
- ***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 >>
- ***Amministrazione remota*** viene visualizzata solo se durante il processo di installazione è stato richiesto di installare questo componente.
- ***Anti-Rootkit*** rileva i programmi e le tecnologie che tentano di camuffare i malware - dettagli >>

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***

- ***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 File Server 2011** registrate.

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 File Server 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 File Server 2011**. In genere è consigliabile mantenere le impostazioni dell'applicazione predefinite dal fornitore del software.

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 le minacce***: consente di aprire l'***Enciclopedia dei virus*** in rete in cui è possibile trovare informazioni dettagliate sul virus identificato
- ***Download di AVG Rescue CD***: consente di aprire il browser Web in corrispondenza della pagina del download di AVG Rescue CD.
- ***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 File Server 2011***, le ultime due voci appaiono come* ***Acquista ora*** *e* ***Attiva****, consentendo di acquistare subito la versione completa del programma. Per* **AVG File Server 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 File Server 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 prestare attenzione alle relative proprietà/impostazioni. Non sono presenti problemi gravi in AVG e probabilmente è stato già deciso di

disattivare alcuni componenti per qualche ragione. La protezione di AVG è ancora attiva. Tuttavia, prestare attenzione alle 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.

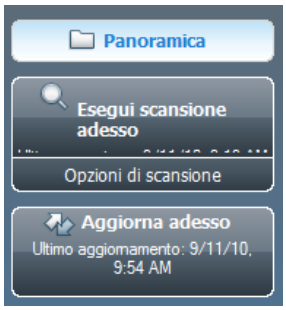
Se AVG non è impostato per prestazioni ottimali, un nuovo pulsante denominato Correggi (oppure Correggi tutto se il problema riguarda più componenti) appare accanto alle informazioni sullo stato della protezione. Selezionare il pulsante per avviare un processo automatico di controllo e configurazione 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 eseguire il comando ***Esegui scansione adesso*** per avviare di nuovo la stessa scansione oppure seguire il collegamento ***Scansione computer*** 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***>>

- ***Componenti server***: questo collegamento indirizza alla ***panoramica Componenti server***.

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

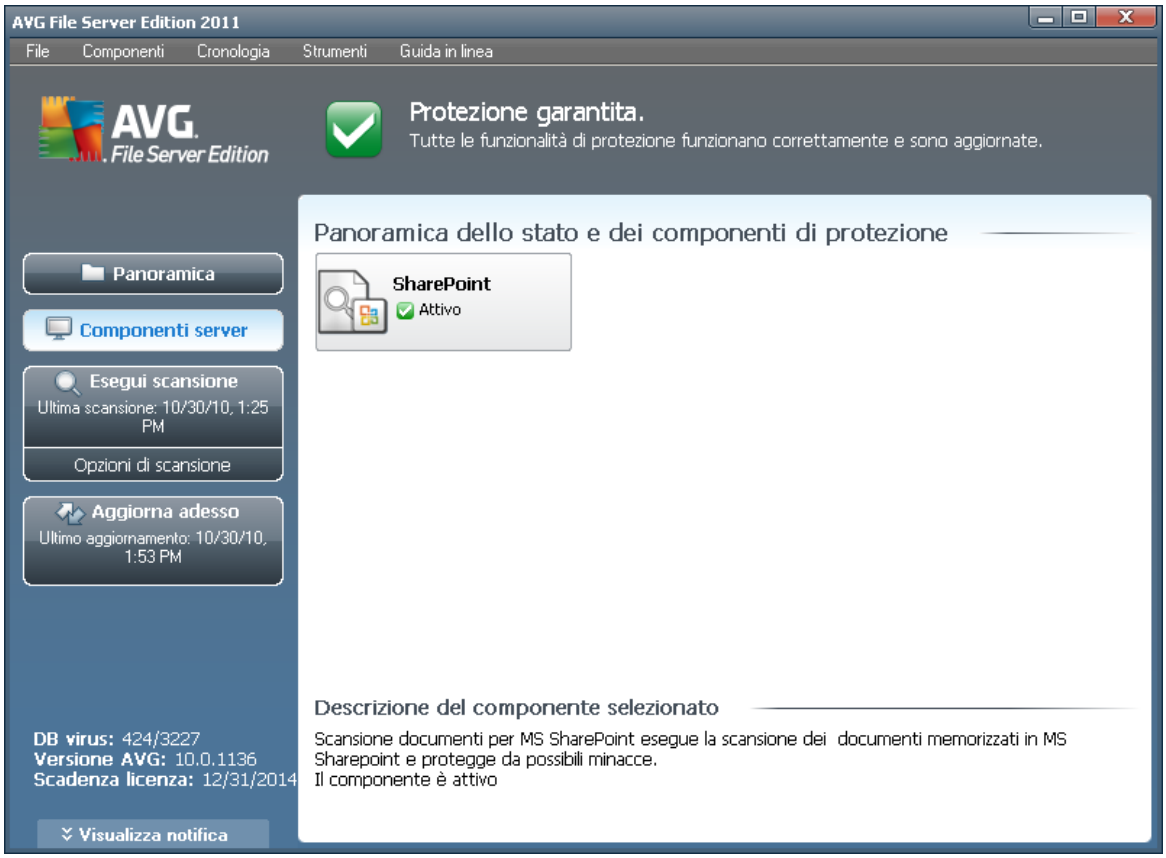
- Descrizione di un componente selezionato

In **AVG File Server 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 >>

6.5. Componenti server



La sezione ***Componenti server*** 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 File Server 2011** la sezione ***Componenti server*** contiene informazioni sui seguenti componenti:

- ***SharePoint*** esegue la scansione dei documenti memorizzati in MS SharePoint e protegge da possibili minacce - dettagli >>

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

6.6. 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:

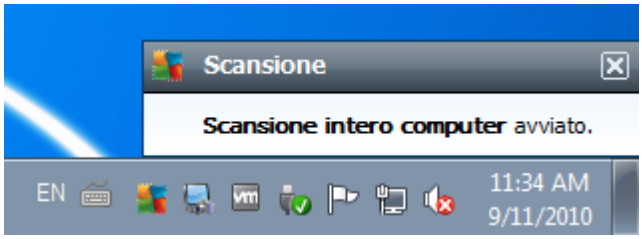
- ***Virus DB***: contiene informazioni sulla versione correntemente installata del database dei virus
- ***Versione AVG***: contiene informazioni sulla versione AVG installata *(il formato del numero è 10.0.xxxx, dove 10.0 indica la versione della linea del prodotto e xxxx indica il numero di build)*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

6.7. Icona della barra delle applicazioni

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



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

- ***Apri interfaccia utente di AVG***: fare clic sull'opzione per aprire Interfaccia utente di AVG
- ***Scansioni***: fare clic per aprire il menu di scelta rapida delle scansioni predefinite (*Scansione intero computer*, *Scansione file o cartelle specifiche*, *Scansione Anti-Rootkit*) e selezionare la scansione richiesta, che verrà avviata immediatamente
- ***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

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.

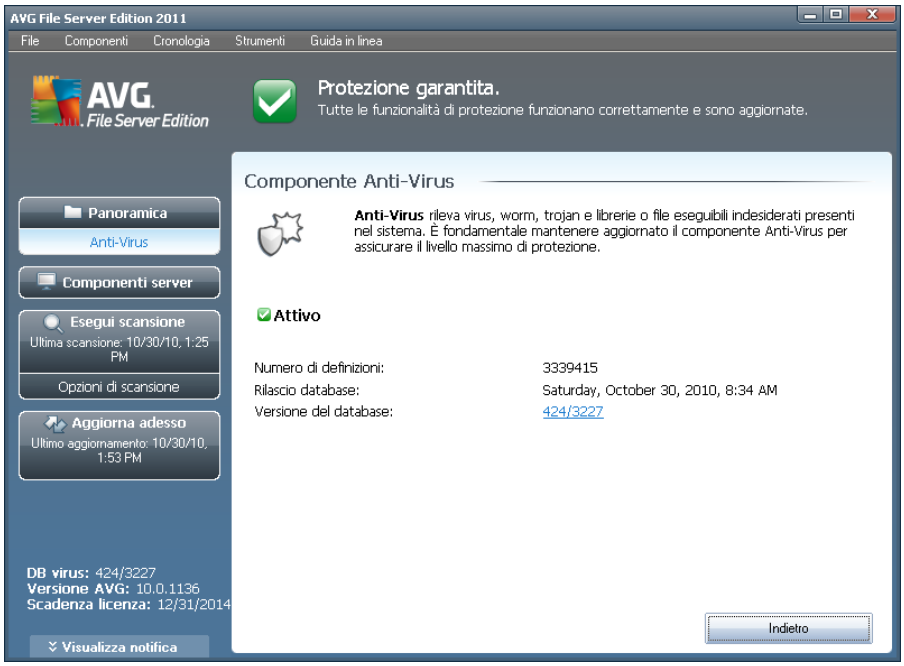
La funzione principale della protezione antivirus è impedire l'esecuzione di virus noti sul computer.

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

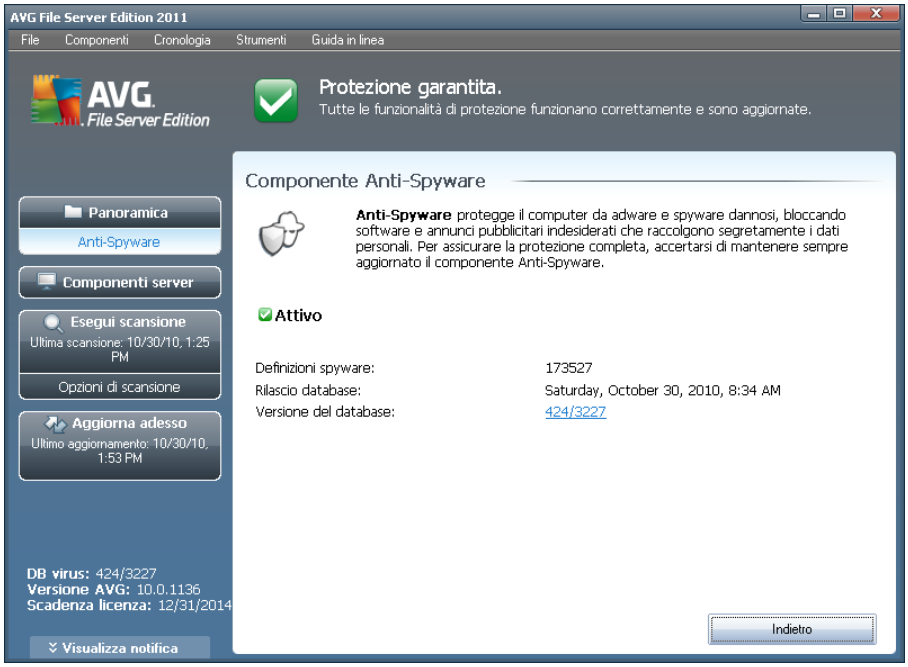
In genere, per spyware si intende un particolare tipo di malware, ovvero un software che raccoglie informazioni dal computer senza informarne l'utente e senza richiederne l'autorizzazione. Alcune applicazioni spyware possono anche essere installate

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 File Server 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. Resident Shield

7.3.1. Principi di Resident Shield

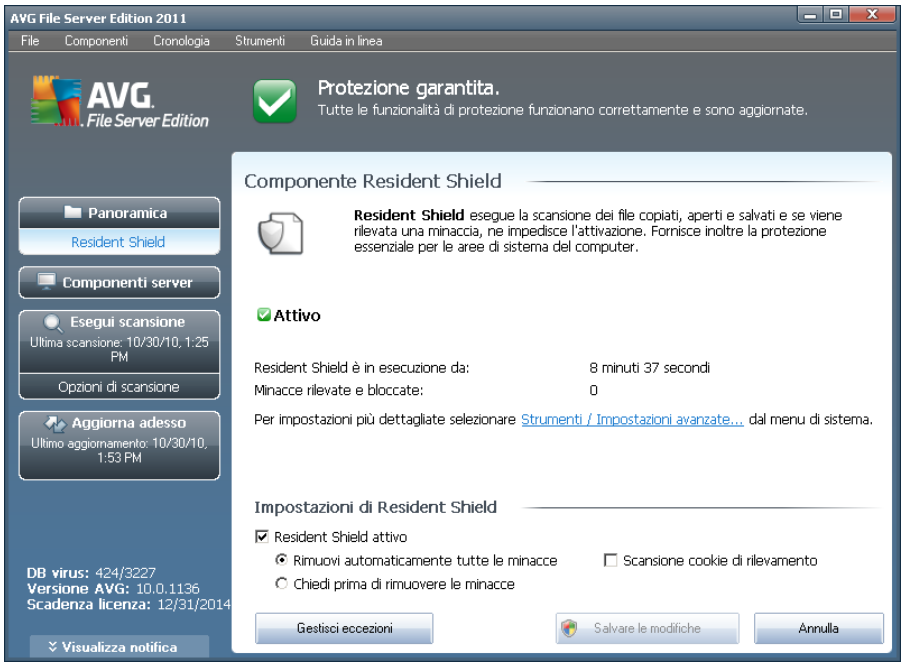
Il componente ***Resident Shield*** fornisce al computer una protezione continua. Esegue la scansione di ogni singolo file che viene aperto, salvato o copiato e sorveglia le aree di sistema del computer. Quando ***Resident Shield*** rileva un virus durante l'accesso a un file, arresta l'operazione in 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.

7.3.2. 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.*

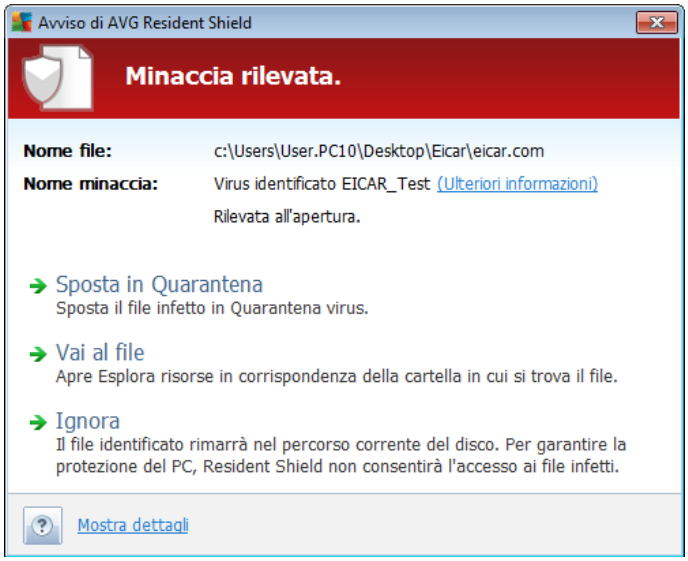
Pulsanti di controllo

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*).

7.3.3. 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:

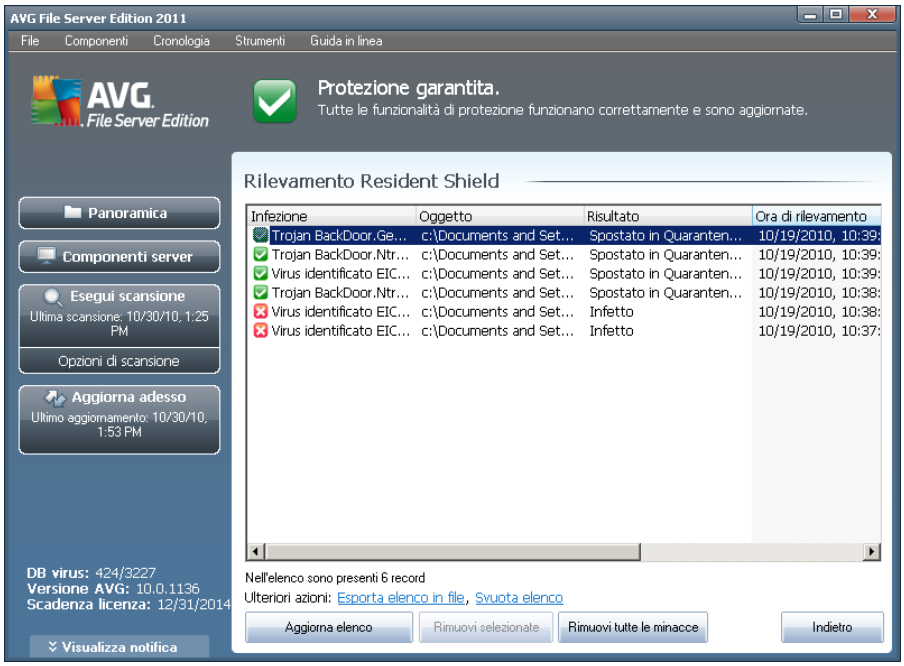
Tenere presente che, in base a condizioni specifiche (tipo e posizione del file infetto), non tutte le opzioni sono sempre disponibili.

- ***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

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*).

7.4. Gestore aggiornamenti

7.4.1. 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*.

7.4.2. 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 quando e a che ora è stato eseguito

l'aggiornamento del database

- ***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 per che giorno e per che ora è stato pianificato il 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 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.*

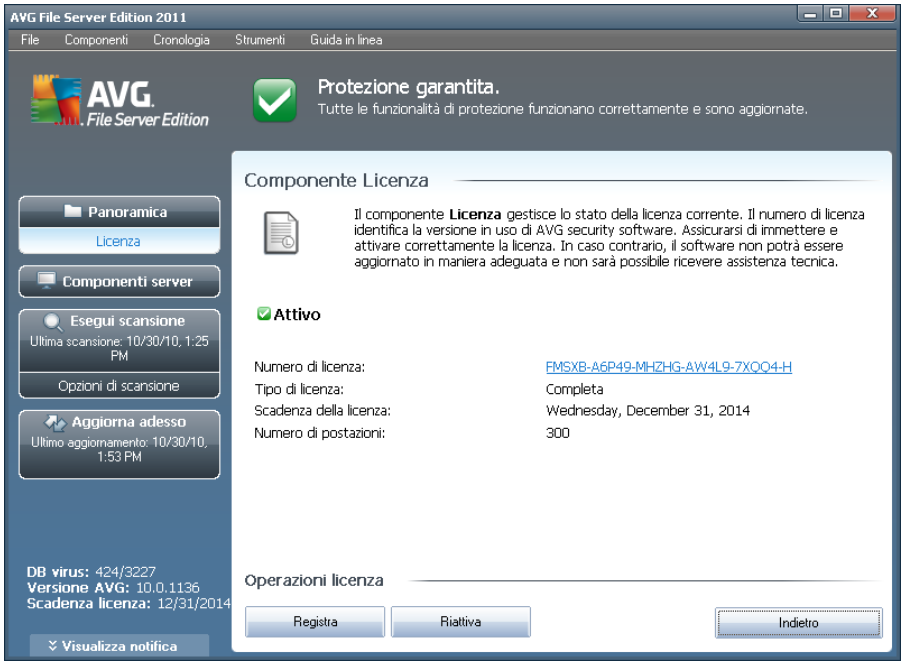
Pulsanti di controllo

I pulsanti di controllo disponibili nell'interfaccia di ***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*).

7.5. 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 File Server 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 File Server 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

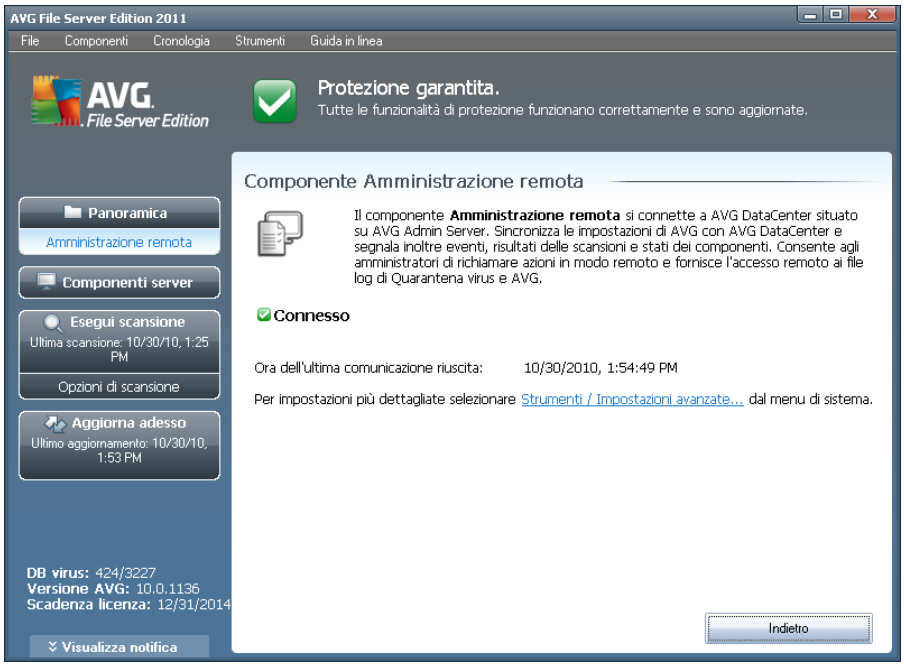
registrano il prodotto AVG possono ricevere assistenza tecnica gratuita.

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

7.6. Amministrazione remota



Il componente ***Amministrazione remota*** viene visualizzato nell'interfaccia utente di **AVG File Server 2011** solo se è stata installata la versione Network 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*).

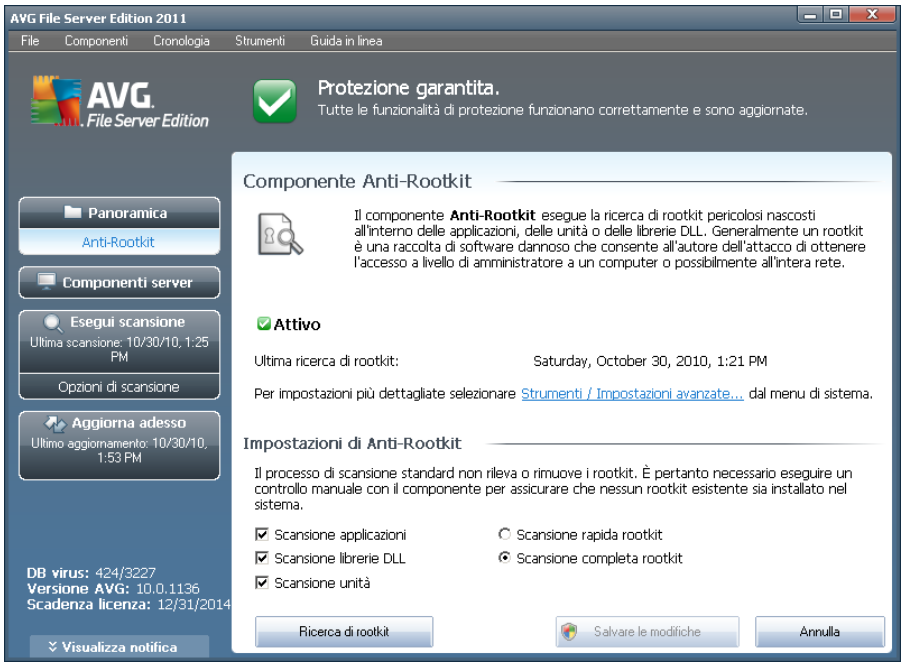
7.7. Anti-Rootkit

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.

7.7.1. 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.

7.7.2. 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

8. AVG Settings Manager

AVG Settings Manager è uno strumento adatto soprattutto alle piccole reti che consente di copiare, modificare e distribuire la configurazione di AVG. È possibile salvare la configurazione in un dispositivo portatile (unità flash USB e così via), quindi applicarla manualmente alle workstation desiderate.

Lo strumento è incluso nell'installazione di AVG ed è disponibile tramite il menu Start di Windows:

Tutti i programmi/AVG 2011/AVG Settings Manager

- ***Modifica la configurazione AVG di questo computer***

  Utilizzare questo pulsante per aprire una finestra di dialogo con le impostazioni avanzate dell'installazione AVG locale. Tutte le modifiche apportate qui verranno applicate inoltre all'installazione AVG locale.

- ***Carica e modifica il file di configurazione di AVG***

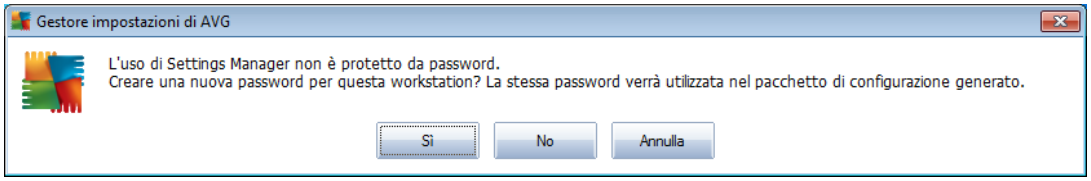
  Se si dispone già di un file di configurazione di AVG (.pck), utilizzare questo pulsante per aprire il file per la modifica. Dopo aver confermato le modifiche tramite il pulsante ***OK*** o ***Applica***, il file conterrà le nuove impostazioni.

- ***Applica configurazione dal file a AVG su questo computer***

  Utilizzare questo pulsante per aprire un file di configurazione di AVG (.pck) e applicarlo all'installazione locale di AVG.

- ***Memorizza la configurazione AVG locale in un file***

Utilizzare questo pulsante per salvare il file di configurazione di AVG (.pck) dell'installazione locale di AVG. Se non è stata impostata una password per le azioni consentite, potrebbe venire visualizzata la seguente finestra di dialogo:



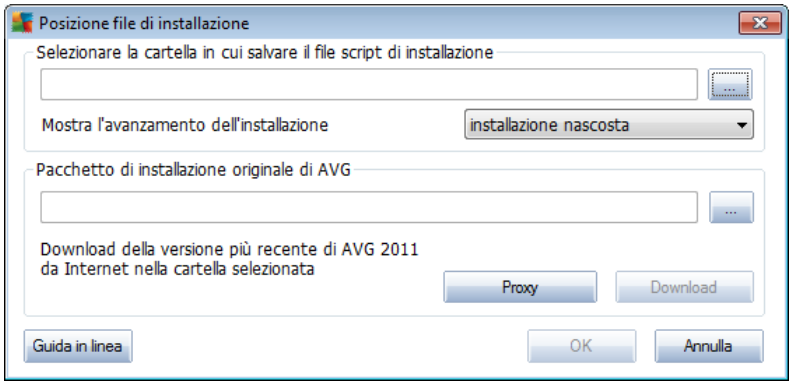
Rispondere ***Sì*** se si desidera impostare subito la password per accedere a Elementi consentiti, quindi immettere le informazioni richieste e confermare la scelta. Rispondere ***No*** per ignorare la creazione della password e procedere con il salvataggio della configurazione di AVG locale su file.

- ***Clona installazione AVG***

  Questa opzione consente di ottenere una copia dell'installazione AVG locale creando un pacchetto di installazione con opzioni personalizzate. Il clone include la maggior parte delle impostazioni AVG con le seguenti eccezioni:

  - Impostazioni della lingua
  - Impostazioni audio
  - Configurazione del firewall
  - Elenco elementi consentiti ed eccezioni ai programmi potenzialmente indesiderati del componente Identity Protection.

  Per procedere selezionare innanzitutto la cartella in cui salvare lo script di installazione.



  Quindi, dal menu a discesa, selezionare una delle seguenti opzioni:

  - ***Installazione nascosta***: non verrà visualizzata alcuna informazione durante il processo di installazione.

- ***Mostra l'avanzamento dell'installazione***: l'installazione non richiederà alcun intervento da parte dell'utente, ma l'avanzamento sarà completamente visibile.

- ***Mostra l'installazione guidata***: l'installazione sarà visibile e l'utente dovrà confermare manualmente tutti i passaggi.

Utilizzare il pulsante ***Download*** per scaricare il più recente pacchetto di installazione di AVG disponibile dal sito Web di AVG nella cartella selezionata oppure spostare manualmente il pacchetto di installazione di AVG in tale cartella.

È possibile utilizzare il pulsante ***Proxy*** per definire un server proxy se richiesto dalla rete per una connessione corretta.

Facendo clic su ***OK*** si avvia il processo di clonazione che dovrebbe terminare in breve tempo. Potrebbe inoltre venire visualizzata una finestra di dialogo che richiede di impostare una password per gli elementi consentiti (vedere sopra). Al termine, ***AvgSetup.bat*** dovrebbe essere disponibile nella cartella selezionata unitamente agli altri file. Se si esegue il file ***AvgSetup.bat***, AVG verrà installato secondo i parametri selezionati in precedenza.

9. Componenti di AVG Server

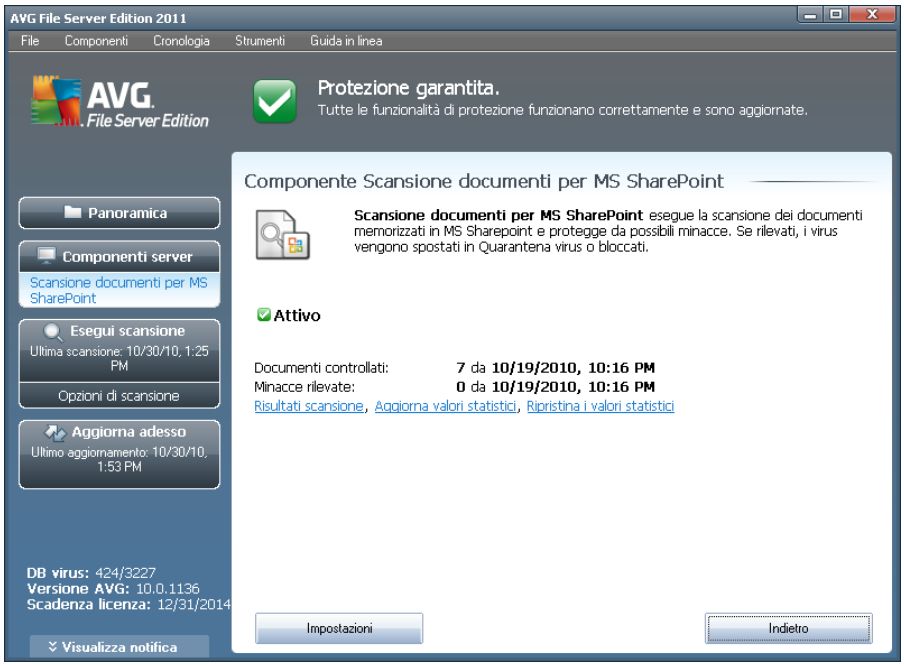
9.1. Scansione documenti per MS SharePoint

9.1.1. Principi di Scansione documenti

Lo scopo del componente server ***Scansione documenti per MS SharePoint*** è quello di analizzare i documenti memorizzati in MS SharePoint. Se vengono rilevati virus, questi vengono spostati in Quarantena virus o completamente rimossi.

Microsoft SharePoint è una raccolta di prodotti ed elementi software che include, tra l'altro, funzioni di collaborazione basate su Internet Explorer, moduli per la gestione dei processi, moduli di ricerca e una piattaforma per la gestione di documenti. SharePoint può essere utilizzato per ospitare siti Web che accedono alle aree di lavoro condivise, agli archivi informazioni e ai documenti.

9.1.2. Interfaccia di Scansione documenti



Oltre a una panoramica dei dati statistici più importanti e alle informazioni sullo stato corrente del componente (*Il componente è attivo*), l'interfaccia di ***Scansione documenti per MS SharePoint*** offre una breve panoramica delle statistiche del componente:

- ***Documenti controllati***: numero di documenti controllati a partire da una determinata data
- ***Minacce rilevate***: numero delle infezioni rilevate a partire da una determinata data

Queste statistiche possono essere aggiornate in qualsiasi momento facendo clic sul collegamento***Aggiorna valori statistici***. I nuovi dati verranno visualizzati praticamente subito. Per impostare tutti i valori statistici su zero, fare clic sul collegamento ***Reimposta valori statistici***. Infine fare clic sul collegamento ***Risultati scansione*** per visualizzare una nuova finestra di dialogo contenente un elenco di risultati della scansione. Ordinare i dati nell'elenco mediante i pulsanti di opzione e/o le schede.

Pulsanti di controllo

I pulsanti di controllo disponibili nell'interfaccia di ***Scansione documenti per MS SharePoint*** sono i seguenti:

- ***Impostazioni***: apre una nuova finestra di dialogo in cui è possibile regolare vari parametri correlati alle prestazioni di scansione antivirus sui documenti di ***Scansione documenti per MS SharePoint*** (per ulteriori informazioni su questa finestra di dialogo, consultare i capitoli ***Impostazioni avanzate di Scansione documenti per MS SharePoint*** e/o ***Azioni di rilevamento***).

- ***Indietro***: selezionare questo pulsante per tornare all'***interfaccia dei componenti server*** predefinita.

10. AVG per SharePoint Portal Server

Questo capitolo illustra la gestione di AVG in ***MS SharePoint Portal Server***, che può essere considerato come un tipo particolare di file server.

10.1. Manutenzione del programma

AVG per SharePoint Portal Server utilizza l'interfaccia di scansione antivirus Microsoft SP VSAPI 1.4 per la protezione del server da potenziali infezioni da virus. Gli oggetti presenti sul server vengono controllati per rilevare l'eventuale presenza di malware quando gli utenti li scaricano dal server e/o li caricano sul server. La configurazione della protezione antivirus può essere impostata utilizzando l'interfaccia ***Amministrazione centrale*** di SharePoint Portal Server. In ***Amministrazione centrale*** è inoltre possibile visualizzare e gestire il file log di **AVG per SharePoint Portal Server** .

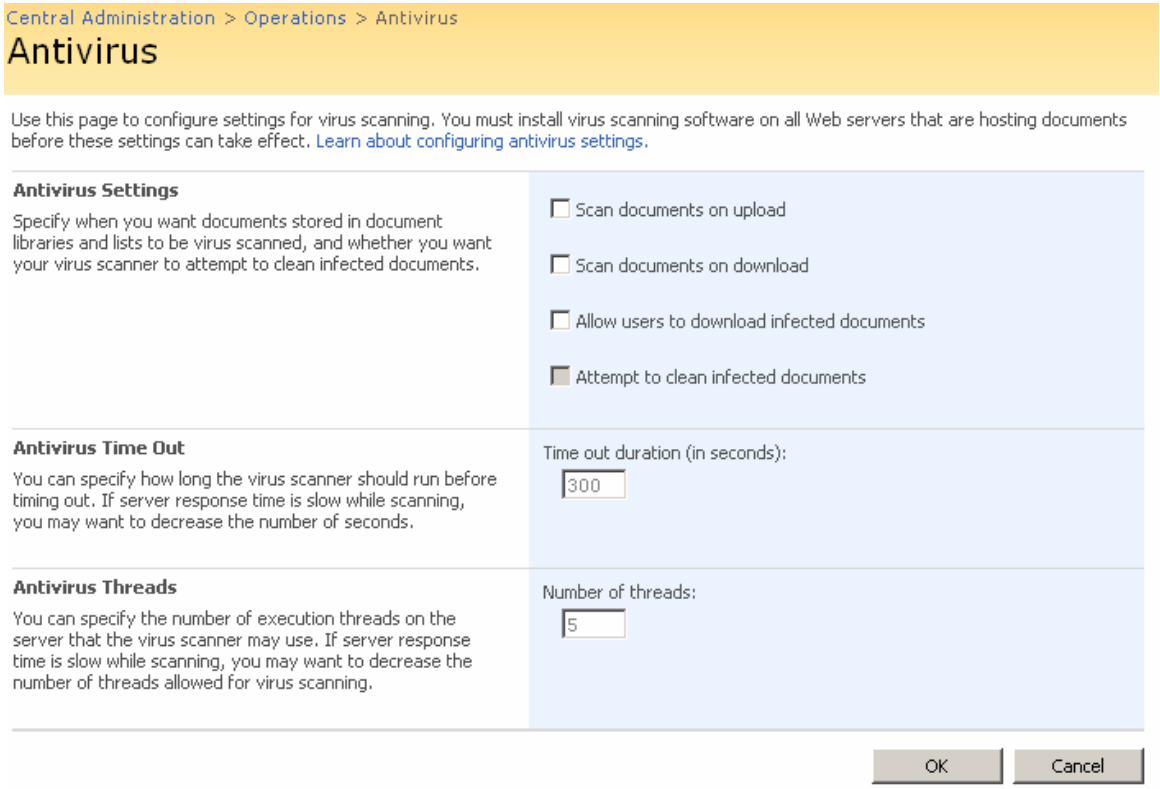
È possibile avviare ***Amministrazione centrale di SharePoint Portal Server*** se è stato effettuato l'accesso al computer su cui viene eseguito il server. L'interfaccia di amministrazione è basata sul Web (*come l'interfaccia utente di SharePoint Portal Server*) ed è possibile aprirla utilizzando l'opzione ***Amministrazione centrale SharePoint*** disponibile nella cartella ***Programmi/Microsoft Office Server*** (in base alla versione anche ***SharePoint Portal Server***) del menu ***Start*** di Windows oppure accedendo a ***Strumenti di amministrazione*** e selezionando ***Amministrazione centrale Sharepoint***.

È inoltre possibile accedere alla pagina Web di ***Amministrazione centrale di SharePoint Portal Server*** in modo remoto utilizzando i dati di accesso e l'URL appropriati.

10.2. Configurazione di AVG per SPPS - SharePoint 2007

In ***Amministrazione centrale di SharePoint 3.0*** è possibile configurare rapidamente le azioni e i parametri delle prestazioni del programma di scansione **AVG per SharePoint Portal Server**. Scegliere l'opzione ***Amministrazione*** nella sezione ***Amministrazione centrale***. Verrà visualizzata una nuova finestra di dialogo. Selezionare la voce ***Impostazioni antivirus*** nella sezione ***Configurazione protezione***.

Verrà quindi visualizzata la seguente finestra:

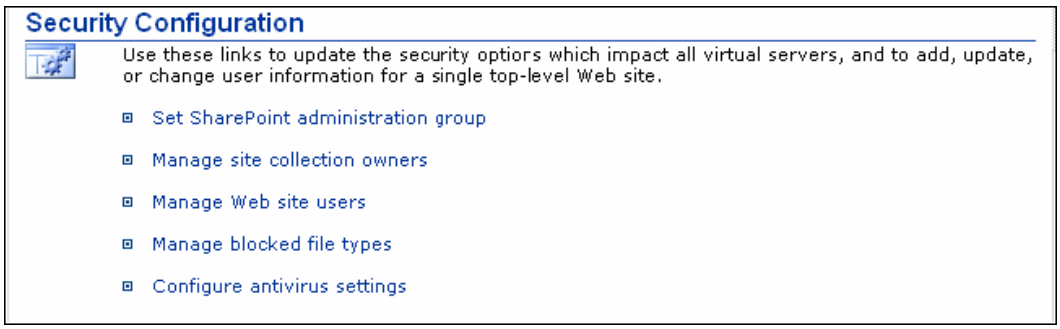


È possibile configurare varie funzioni per le prestazioni e azioni per la scansione antivirus di **AVG per SharePoint Portal Server** qui:

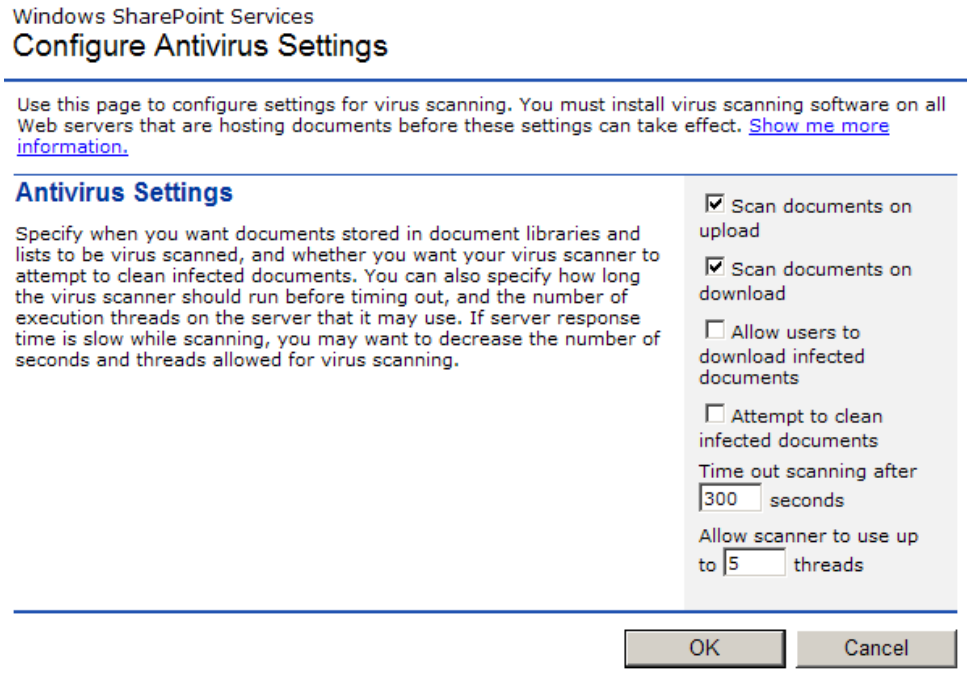
- ***Esegui ricerca virus nei documenti al momento del caricamento***: attiva/disattiva la scansione dei documenti in fase di caricamento
- ***Esegui ricerca virus nei documenti al momento del download***: attiva/disattiva la scansione dei documenti in fase di download
- ***Consenti agli utenti il download dei documenti che contengono un virus***: consente/impedisce agli utenti di scaricare documenti infetti
- ***Tenta pulizia dei documenti che contengono un virus***: attiva/disattiva la correzione automatica dei documenti infetti (ove possibile)
- ***Timeout*** (*secondi*): numero massimo di secondi durante i quali il processo di scansione antivirus verrà eseguito dopo un singolo avvio (diminuire il valore se la risposta del server sembra rallentata durante la scansione dei documenti)
- ***Numero di thread***: è possibile specificare il numero di thread di scansione antivirus che possono essere eseguiti simultaneamente; l'aumento del numero può velocizzare la scansione grazie al livello più elevato di parallelismo, tuttavia può inoltre aumentare il tempo di risposta del server

10.3. Configurazione di AVG per SPPS - SharePoint 2003

In ***Amministrazione centrale di SharePoint Portal Server*** è possibile configurare rapidamente le azioni e i parametri delle prestazioni del programma di scansione **AVG per SharePoint Portal Server**. Scegliere l'opzione ***Configura impostazioni antivirus*** nella sezione ***Configurazione protezione***:



Verrà quindi visualizzata la seguente finestra:



È possibile configurare varie funzioni per le prestazioni e azioni per la scansione antivirus di **AVG per SharePoint Portal Server** qui:

- ***Esegui ricerca virus nei documenti al momento del caricamento***: attiva/disattiva la scansione dei documenti in fase di caricamento
- ***Esegui ricerca virus nei documenti al momento del download***: attiva/disattiva la scansione dei documenti in fase di download

- ***Consenti agli utenti il download dei documenti che contengono un virus***: consente/impedisce agli utenti di scaricare documenti infetti

- ***Tenta pulizia dei documenti che contengono un virus***: attiva/disattiva la correzione automatica dei documenti infetti (ove possibile)

- ***Timeout***: numero massimo di secondi durante i quali il processo di scansione antivirus verrà eseguito dopo un singolo avvio (*diminuire il valore se la risposta del server sembra rallentata durante la scansione dei documenti*)

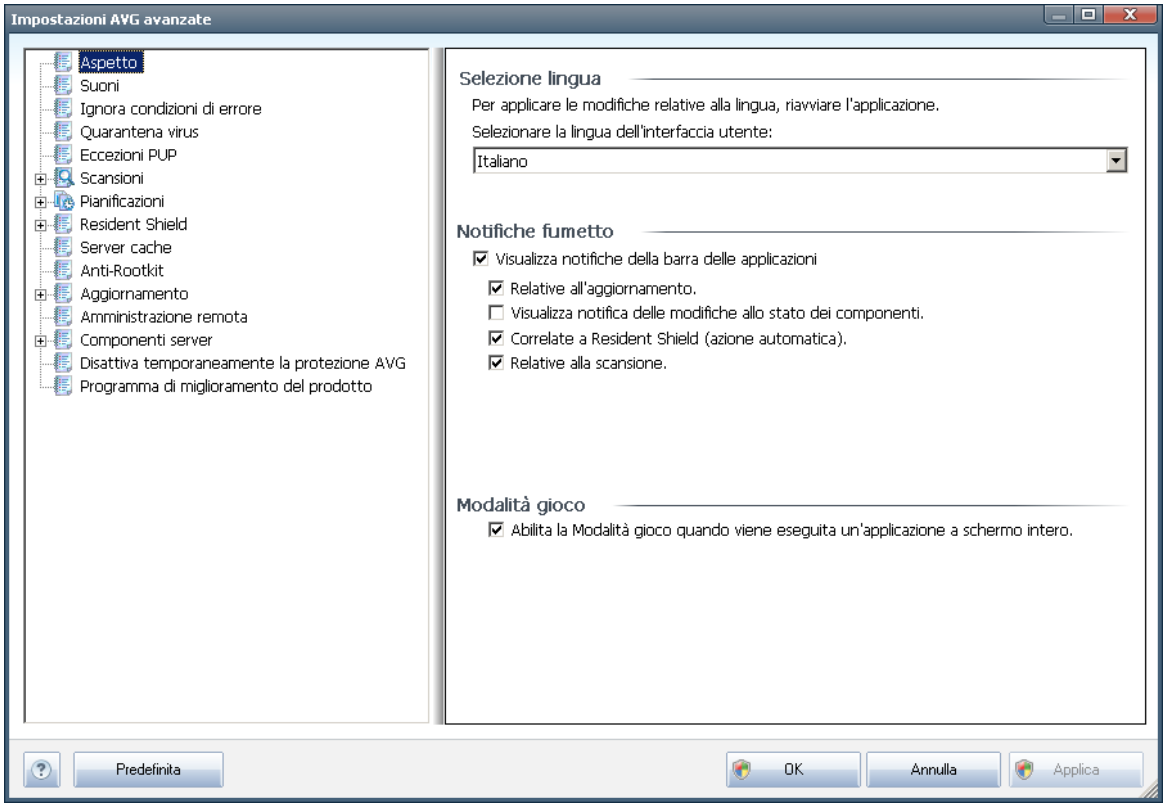
- ***Usa max. X processi secondari per la scansione documenti***: la X specifica il numero di thread di scansione antivirus che possono essere eseguiti simultaneamente; l'aumento del numero può velocizzare la scansione grazie al livello più elevato di parallelismo, tuttavia può aumentare inoltre il tempo di risposta del server

11. Impostazioni AVG avanzate

Le opzioni di configurazione avanzata di **AVG File Server 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.

11.1. Aspetto

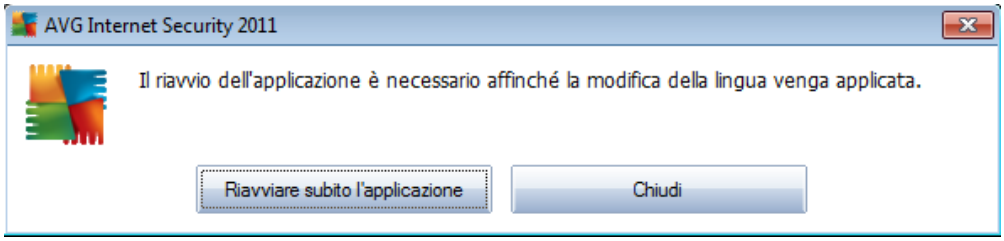
La prima voce della struttura di esplorazione, ***Aspetto***, fa riferimento alle impostazioni generali dell'Interfaccia utente di AVG e ad alcune opzioni di base del comportamento dell'applicazione:



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*).

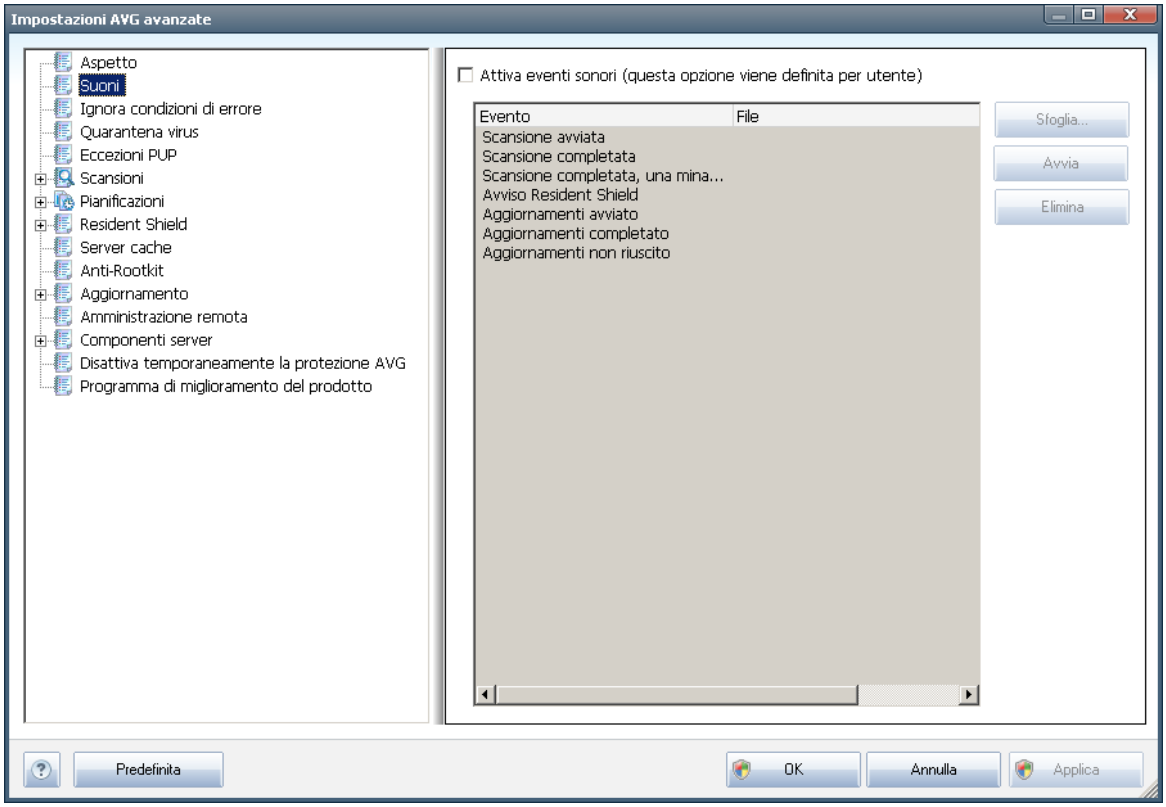
- ***Visualizza notifiche della barra delle applicazioni relative alla scansione***: consente di decidere se visualizzare le informazioni relative all'avvio automatico, all'avanzamento e ai risultati della scansione pianificata.

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*).

11.2. 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:

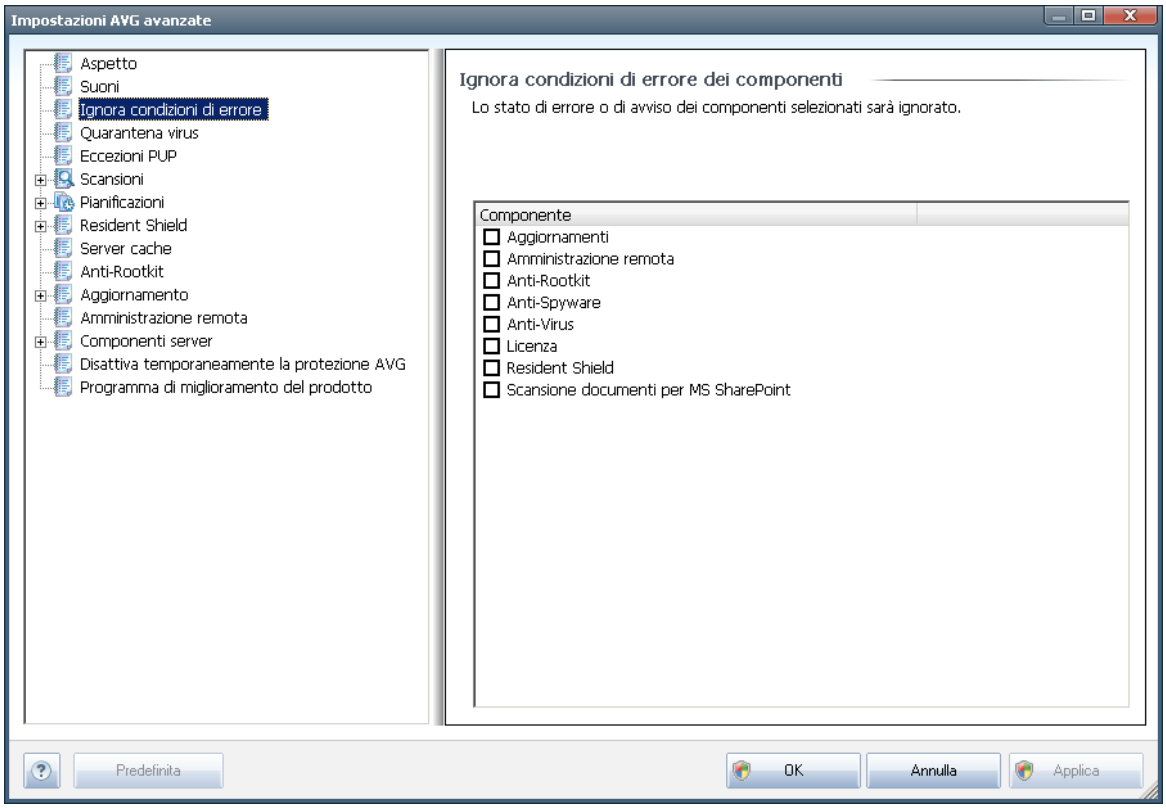


Quindi, selezionare l'evento pertinente dall'elenco e ricercare nel disco rigido (tramite ***Sfoglia***) un suono appropriato da assegnare all'evento. Per ascoltare il suono selezionato, evidenziare l'evento nell'elenco e fare clic sul pulsante ***Avvia***. Utilizzare il pulsante ***Elimina*** per rimuovere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

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

11.3. 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:



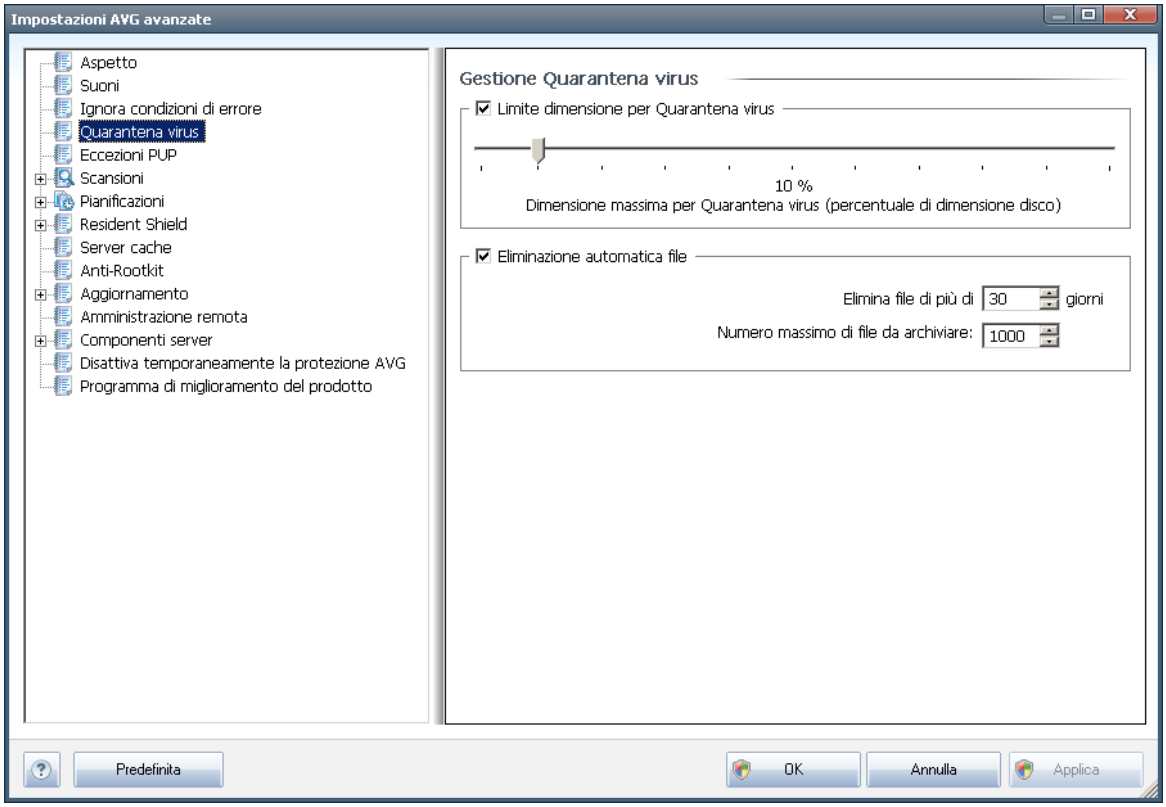
Per impostazione predefinita, in questo elenco non è selezionato alcun componente. Ciò significa che se per un qualsiasi componente si verifica uno stato di errore, se ne verrà immediatamente informati tramite:

- ***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.

11.4. Quarantena virus



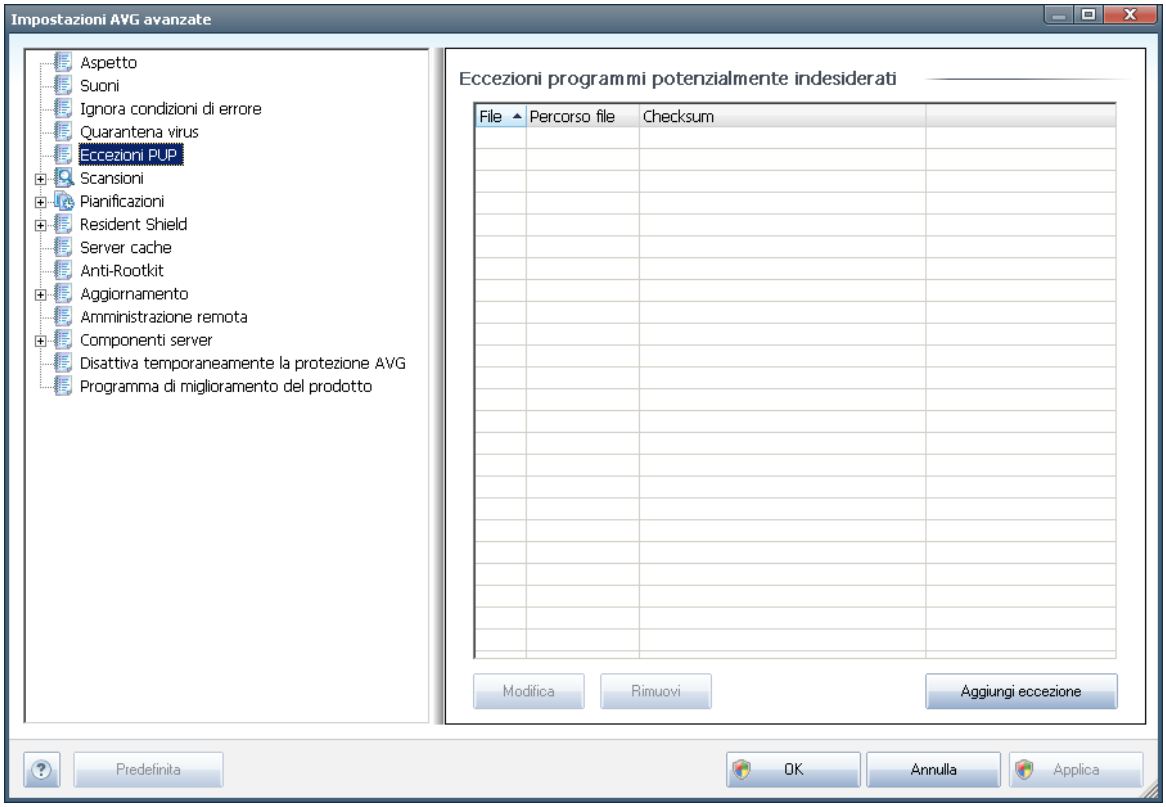
La finestra di dialogo ***Gestione Quarantena virus*** consente di definire diversi parametri relativi alla gestione degli oggetti archiviati in ***Quarantena virus***:

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

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

11.5. Eccezioni PUP

AVG File Server 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:

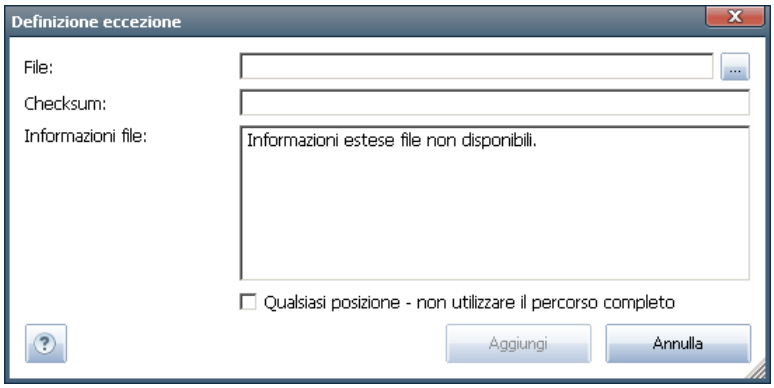
- ***File***: fornisce il nome della rispettiva applicazione
- ***Percorso file***: mostra la posizione dell'applicazione
- ***Checksum***: visualizza la "firma" univoca del file prescelto. Questo checksum è una stringa di caratteri generata automaticamente che consente a AVG di distinguere in modo inequivocabile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

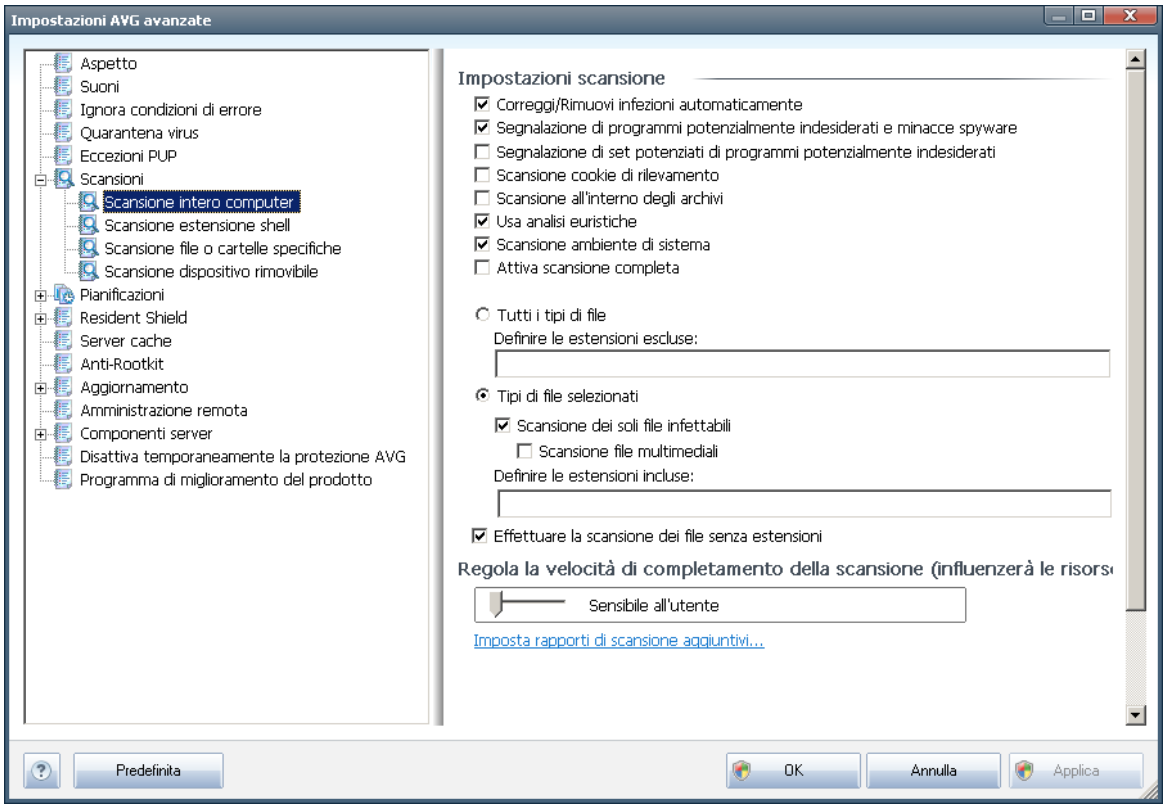
11.6. Scansioni

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

11.6.1. 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.

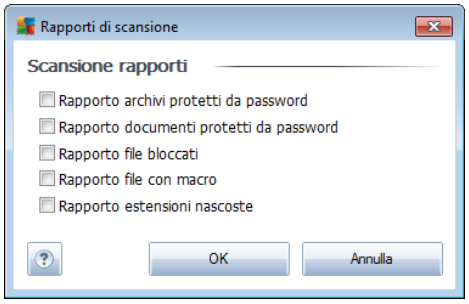
- Facoltativamente, è possibile sottoporre a scansione i file senza estensione tramite ***Effettuare la scansione dei file senza estensioni***: questa opzione è attivata per impostazione predefinita e si consiglia di non modificare questa impostazione a meno che non siano presenti motivi validi per farlo.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

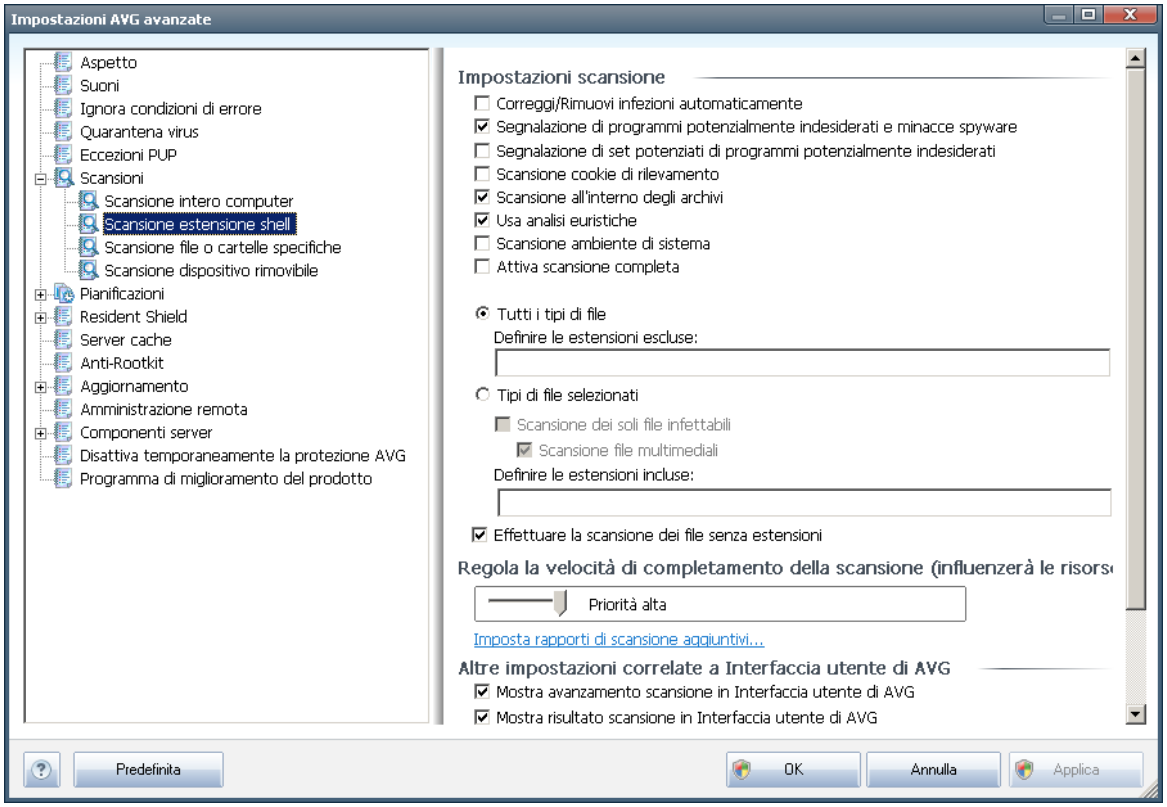
Imposta rapporti di scansione aggiuntivi...

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:



11.6.2. 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***:



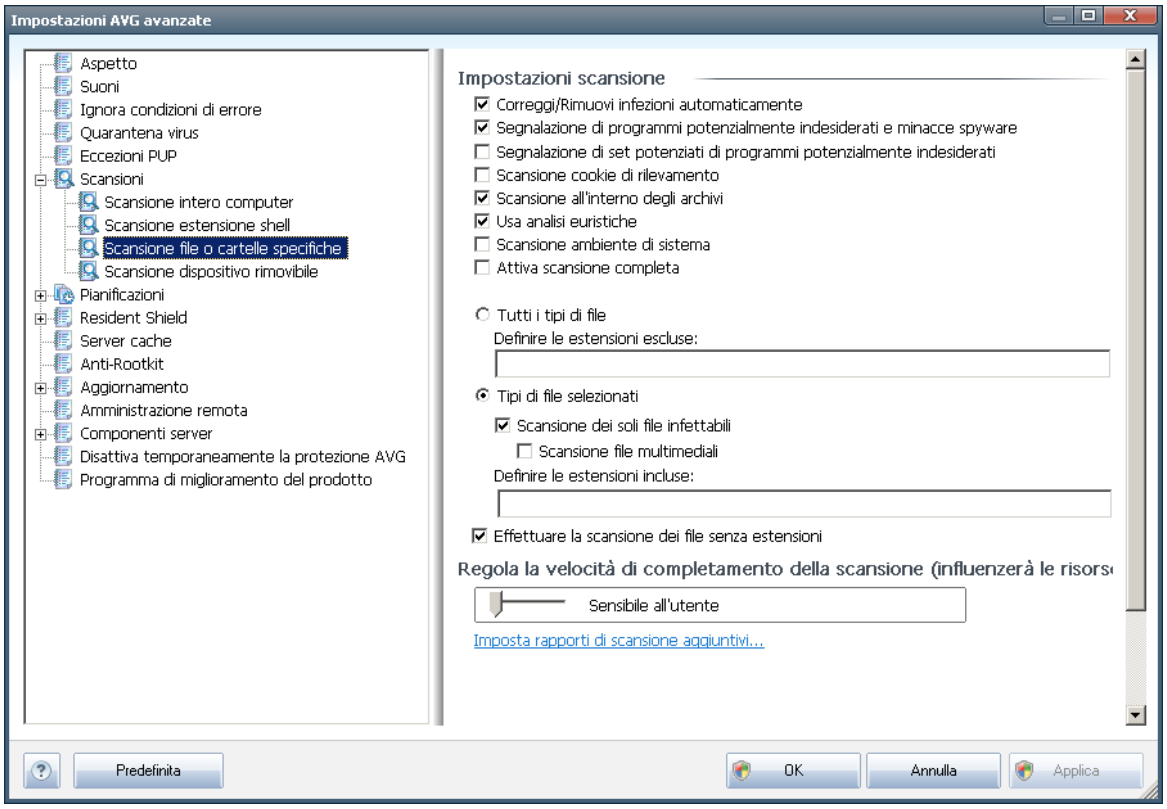
L'elenco dei parametri è identico a quello disponibile per ***Scansione intero computer***. Tuttavia, le impostazioni predefinite sono diverse (*ad esempio, per impostazione predefinita Scansione intero computer non controlla gli archivi ma esamina l'ambiente di sistema, viceversa per Scansione estensione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

11.6.3. 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***:

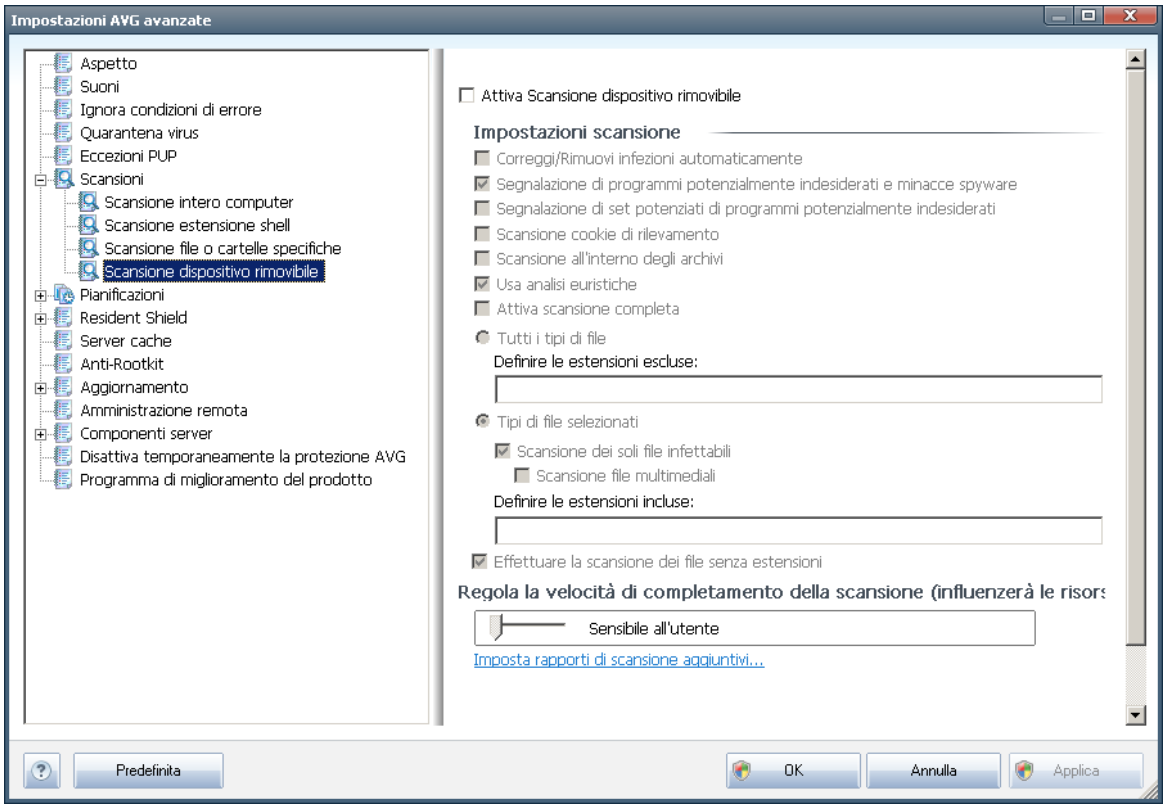


Tutti i parametri impostati in questa finestra di dialogo di configurazione si applicano solo alle aree selezionate per la scansione con il comando ***Scansione file o cartelle specifiche***!

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

11.6.4. 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****.*

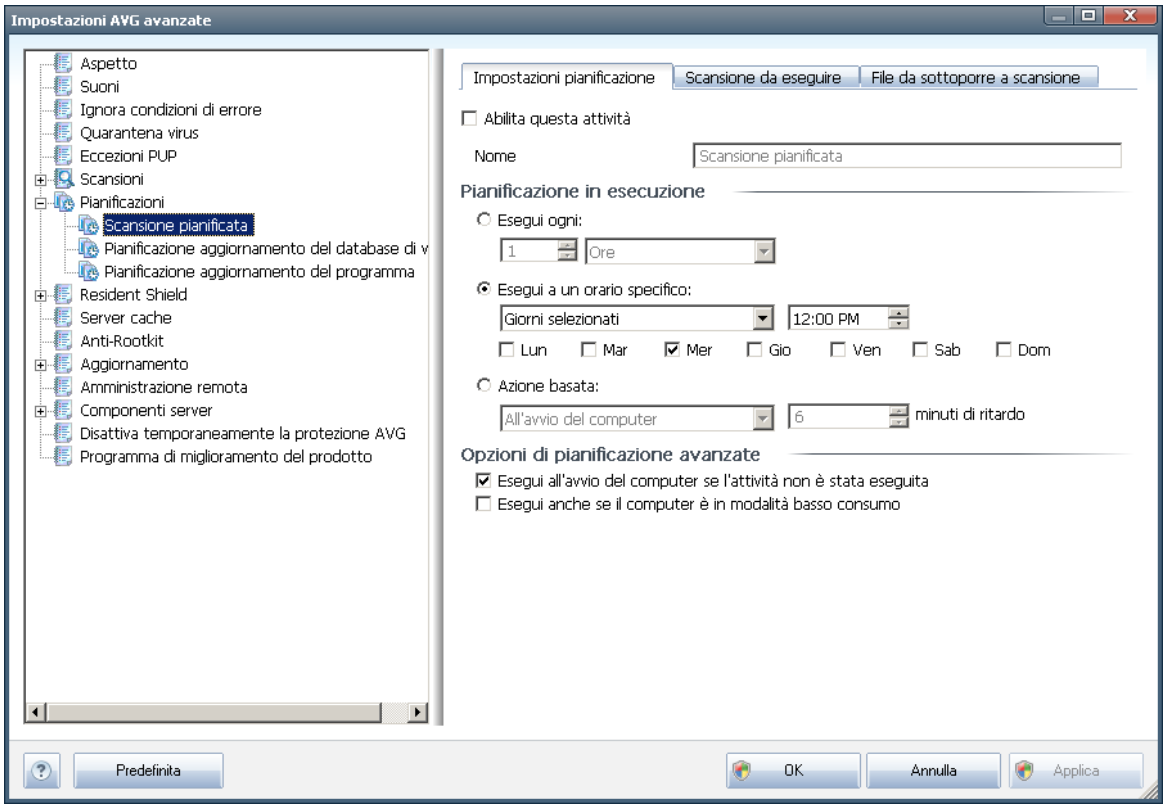
11.7. Pianificazioni

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

- Scansione pianificata
- Pianificazione aggiornamento del database di virus
- Pianificazione aggiornamento del programma

11.7.1. Scansione pianificata

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



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

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

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

della scansione dei file e delle cartelle selezionati.

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

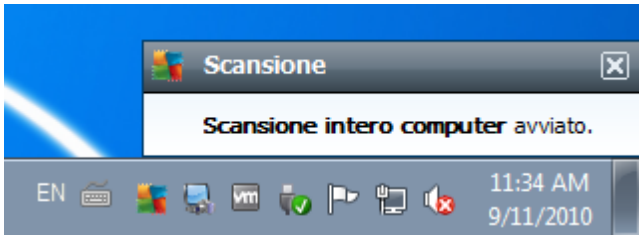
Pianificazione in esecuzione

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

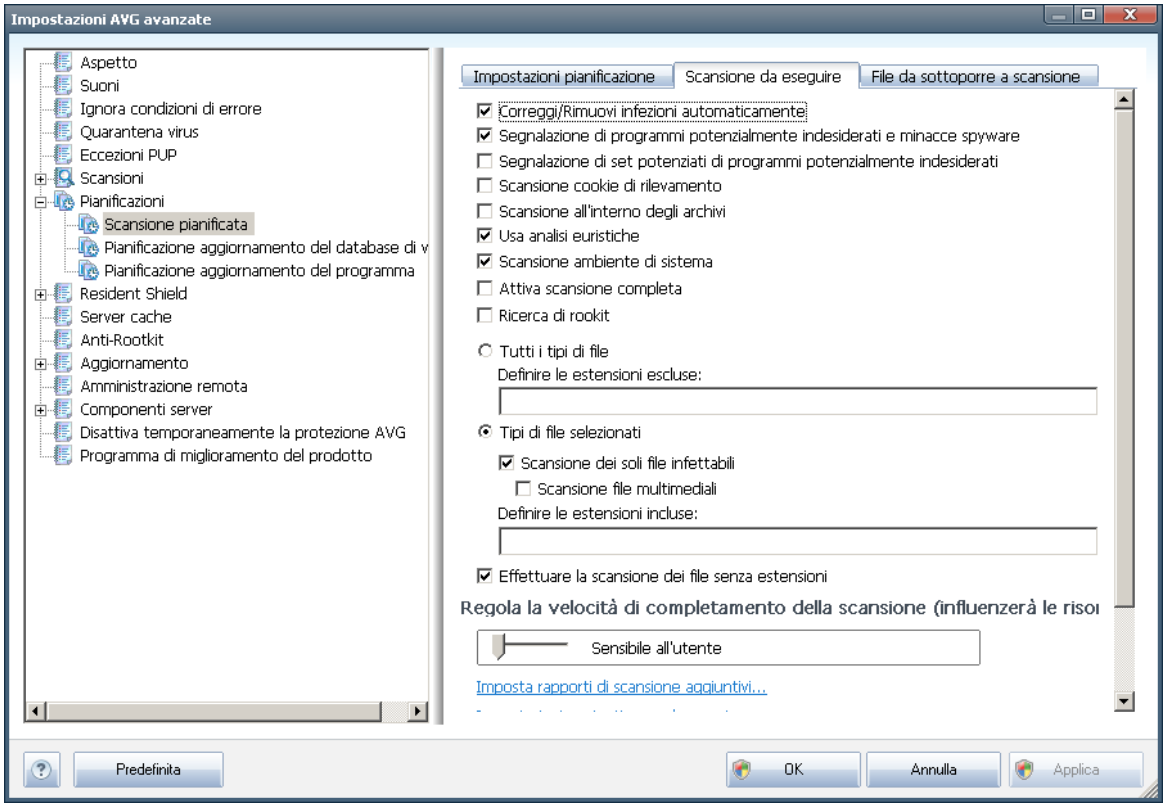
Opzioni di pianificazione avanzate

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

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



Viene quindi visualizzata una nuova icona AVG nella barra delle applicazioni (*completamente colorata e con una 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.

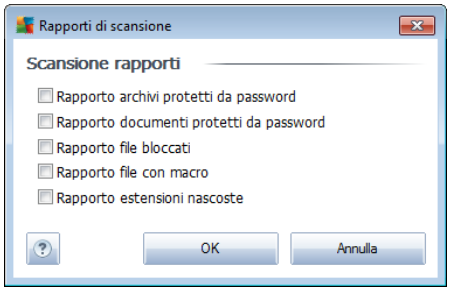
- Facoltativamente, è possibile sottoporre a scansione i file senza estensione tramite ***Effettuare la scansione dei file senza estensioni***: questa opzione è attivata per impostazione predefinita e si consiglia di non modificare questa impostazione a meno che non siano presenti motivi validi per farlo.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

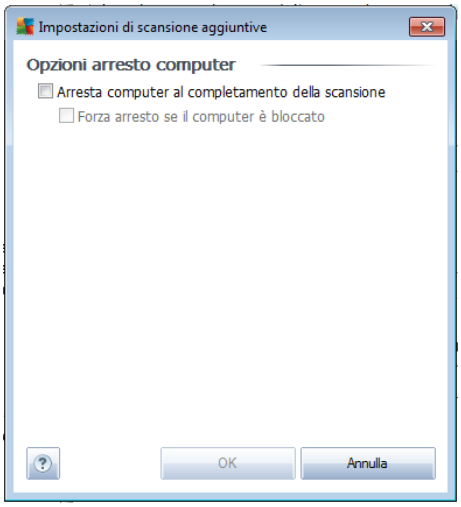
Imposta rapporti di scansione aggiuntivi

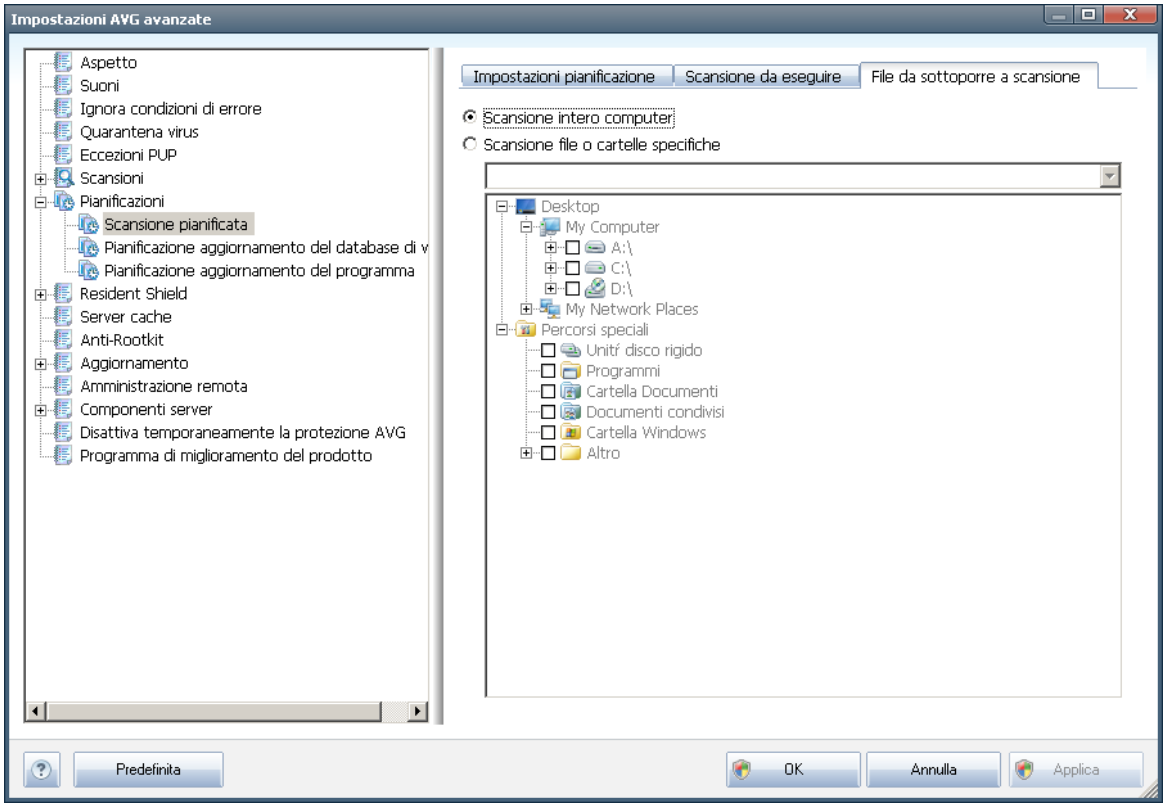
Fare clic sul collegamento ***Imposta rapporti di scansione aggiuntivi...*** per aprire una finestra di dialogo autonoma denominata ***Rapporti di scansione*** in cui è possibile selezionare diversi elementi per definire i tipi di rilevamenti da segnalare:



Impostazioni di scansione aggiuntive

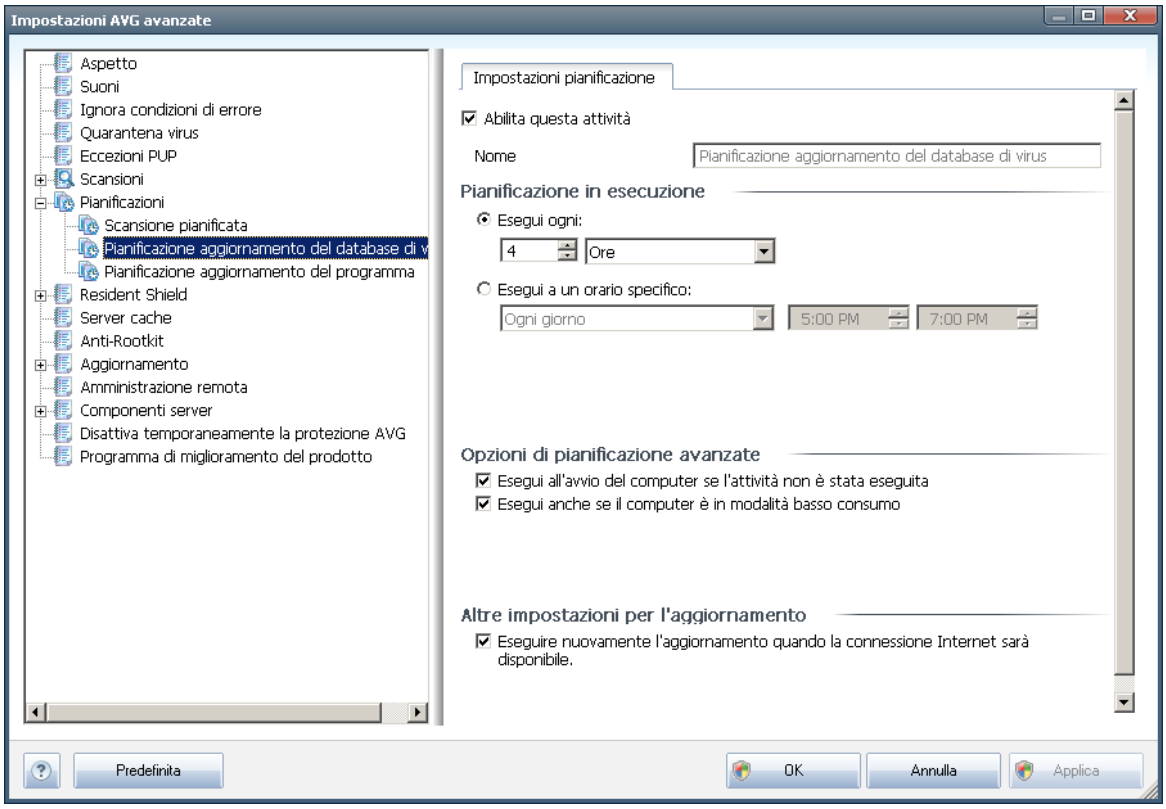
Fare clic su ***Impostazioni di scansione aggiuntive...*** per aprire una nuova finestra di dialogo ***Opzioni arresto computer*** in cui è possibile decidere se il computer deve essere arrestato in modo automatico al termine del processo di scansione. Dopo aver confermato questa opzione (***Arresta 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.

11.7.2. Pianificazione dell'aggiornamento del database dei virus



Nella scheda ***Impostazioni attività*** è possibile selezionare/deselezionare la voce ***Abilita questa attività*** per disattivare temporaneamente l'aggiornamento del database dei virus pianificato e riattivarlo secondo le necessità. La pianificazione dell'aggiornamento di base del database dei virus viene eseguita all'interno del componente ***Gestore aggiornamenti***. Da questa finestra di dialogo è possibile impostare alcuni parametri dettagliati della pianificazione dell'aggiornamento del database di virus. Nel campo di testo ***Nome*** (*disattivato per tutte le pianificazioni predefinite*) è presente il nome assegnato alla pianificazione in oggetto dal fornitore del programma.

Pianificazione in esecuzione

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

Opzioni di pianificazione avanzate

Questa sezione consente di definire le circostanze in cui deve o non deve essere

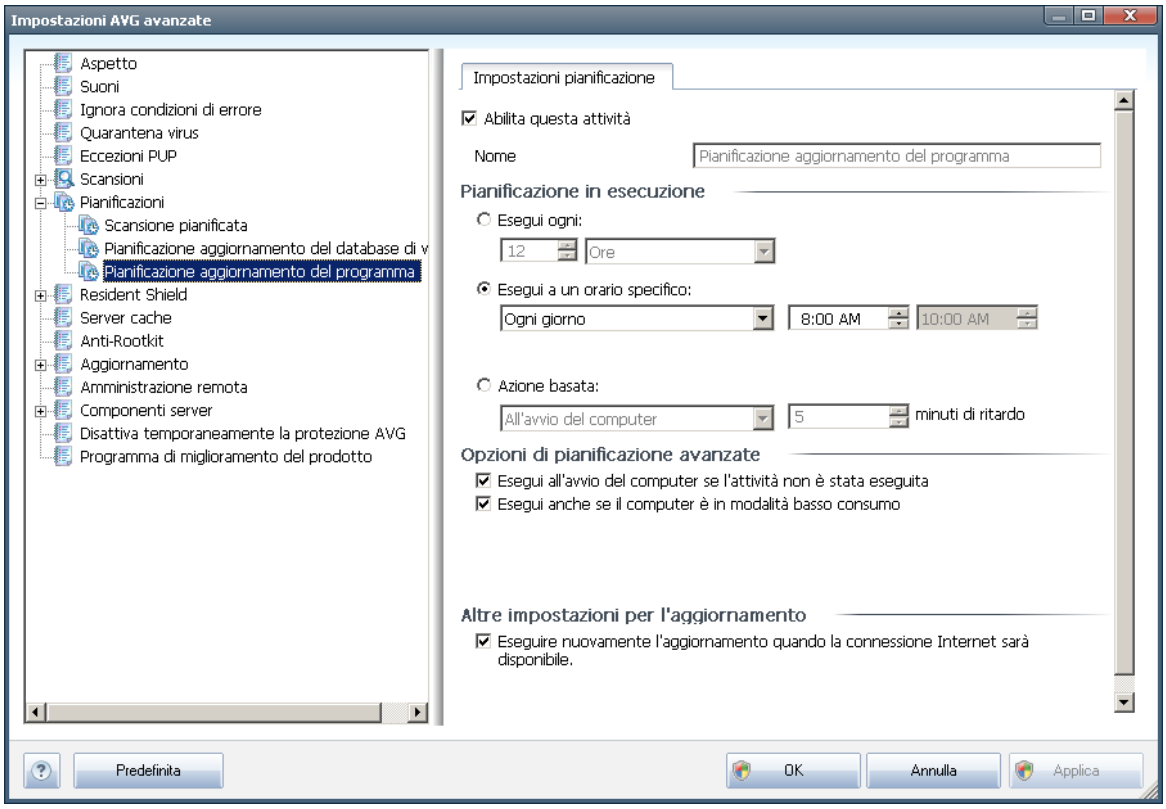
avviato l'aggiornamento del database dei virus se il computer si trova in modalità basso consumo oppure se è completamente spento.

Altre impostazioni per l'aggiornamento

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

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

11.7.3. Pianificazione dell'aggiornamento del programma



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

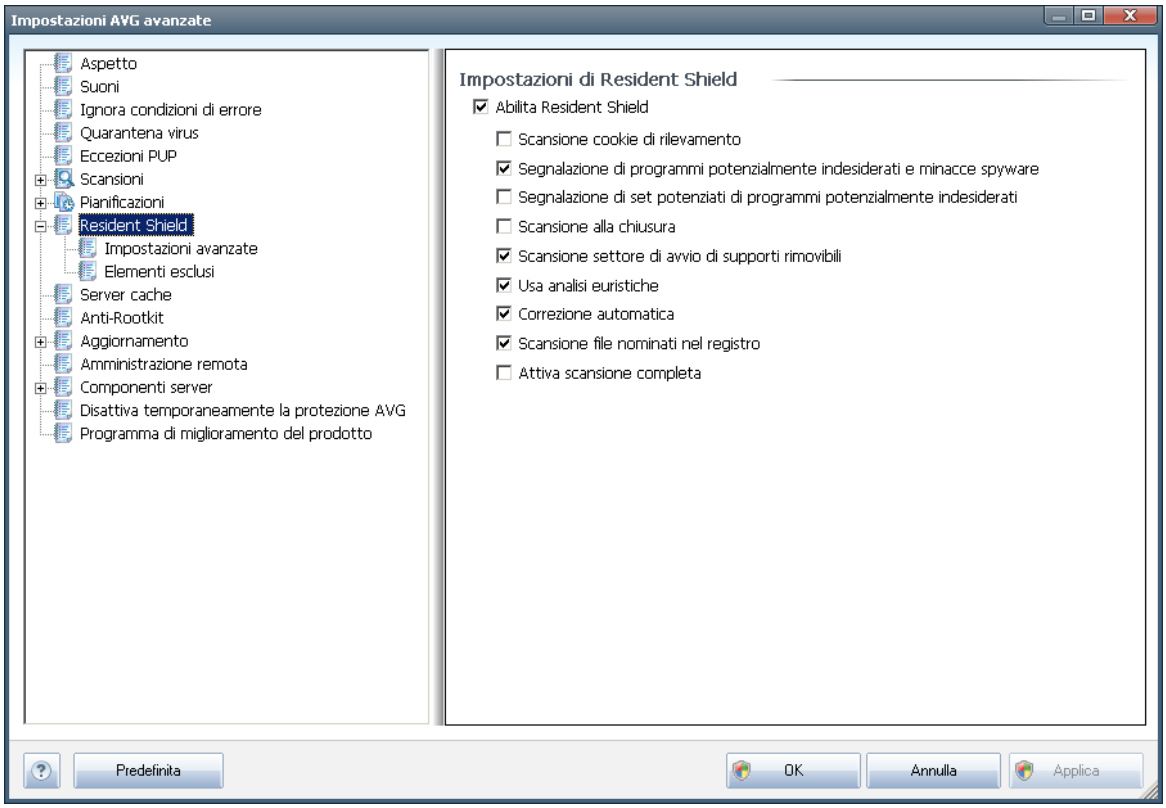
Selezionare l'opzione ***Eseguire nuovamente l'aggiornamento quando la connessione Internet sarà disponibile*** per assicurarsi che, se la connessione Internet si interrompesse e il processo di aggiornamento non riuscisse, tale processo venga avviato di nuovo subito dopo il ripristino della connessione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

11.8. 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*)

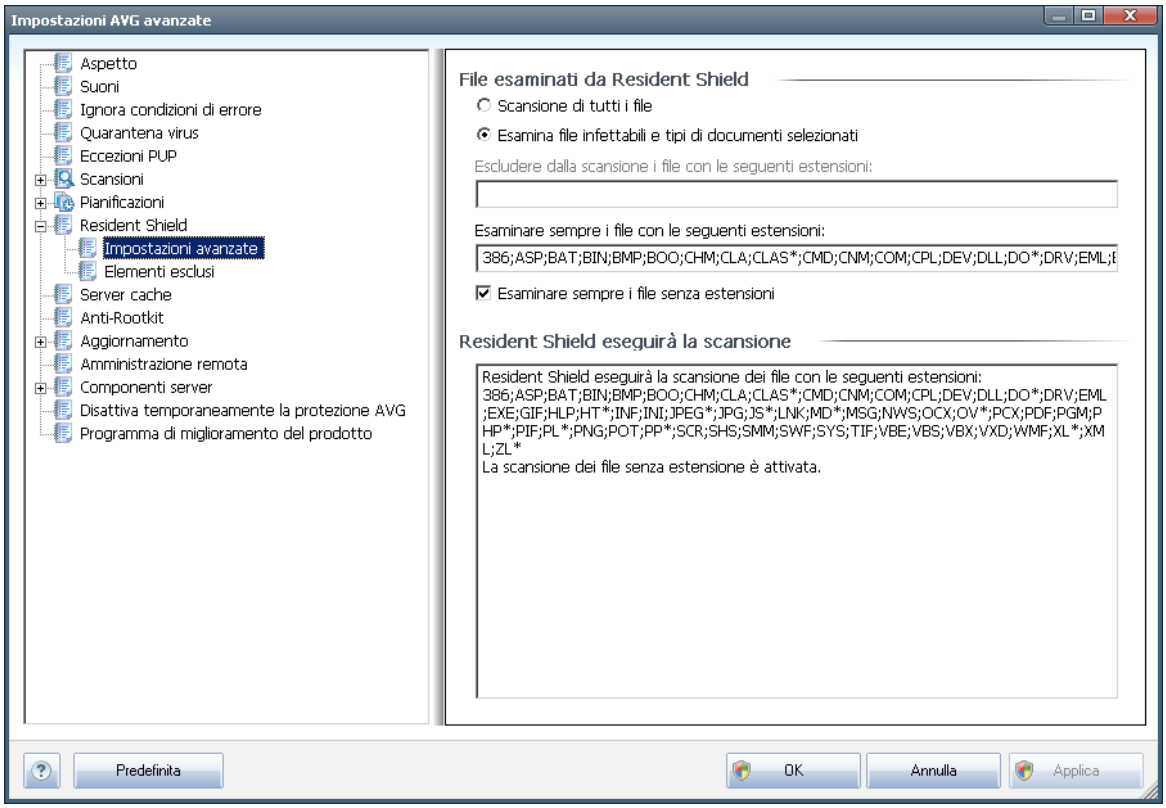
- ***Correggi automaticamente*** (*disattivata per impostazione predefinita*): tutte le infezioni rilevate verranno corrette automaticamente se è disponibile una soluzione e tutte le infezioni che non possono essere corrette verranno rimosse.

- ***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.

11.8.1. Impostazioni avanzate

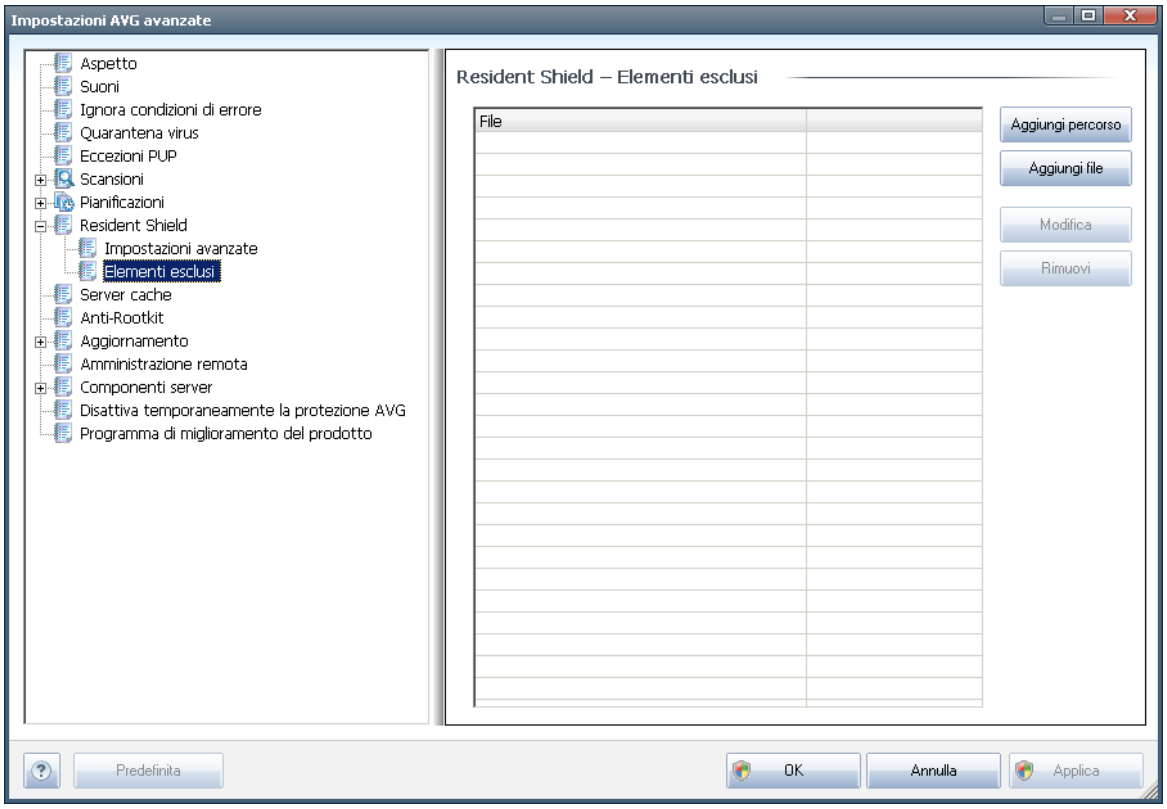
Nella finestra di dialogo ***File esaminati da Resident Shield*** è possibile configurare i file che verranno sottoposti a scansione (*in base a estensioni specifiche*):



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***.

11.8.2. 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***.

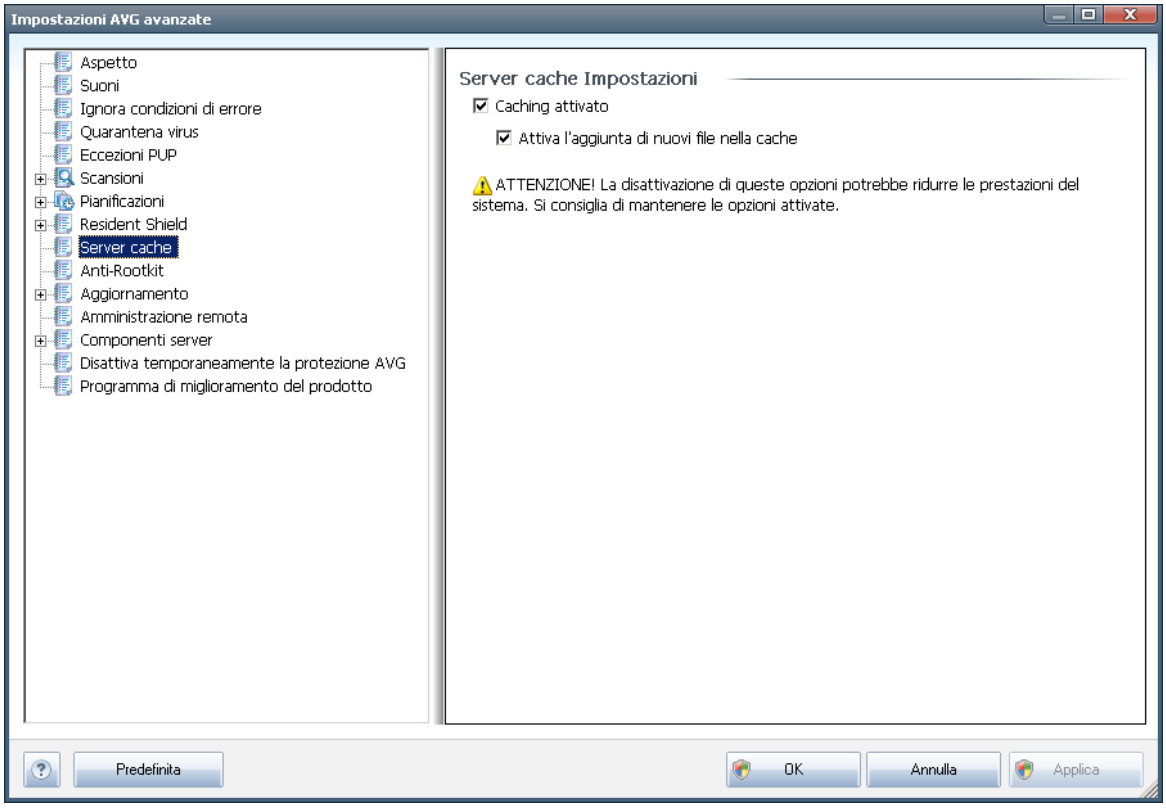
Se non è essenziale, si consiglia di non escludere alcun elemento.

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

11.9. 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.



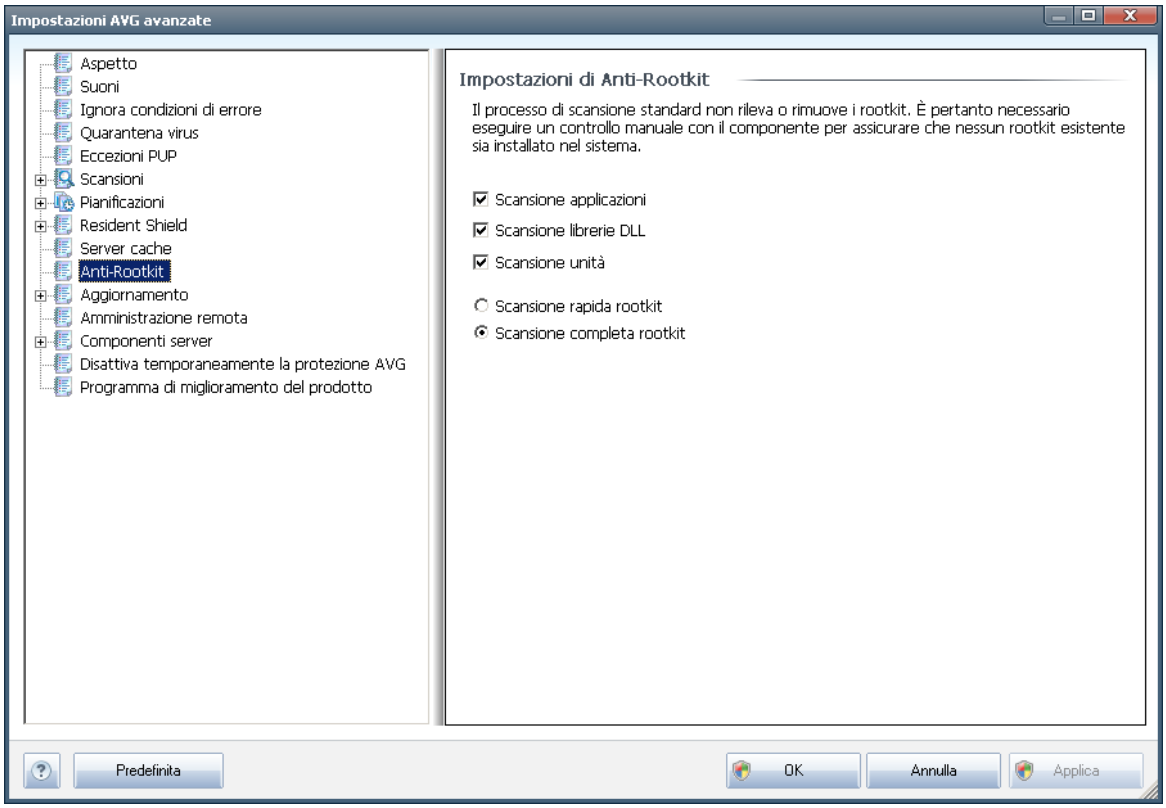
La finestra di dialogo di impostazione offre due opzioni:

- ***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.

11.10. 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:

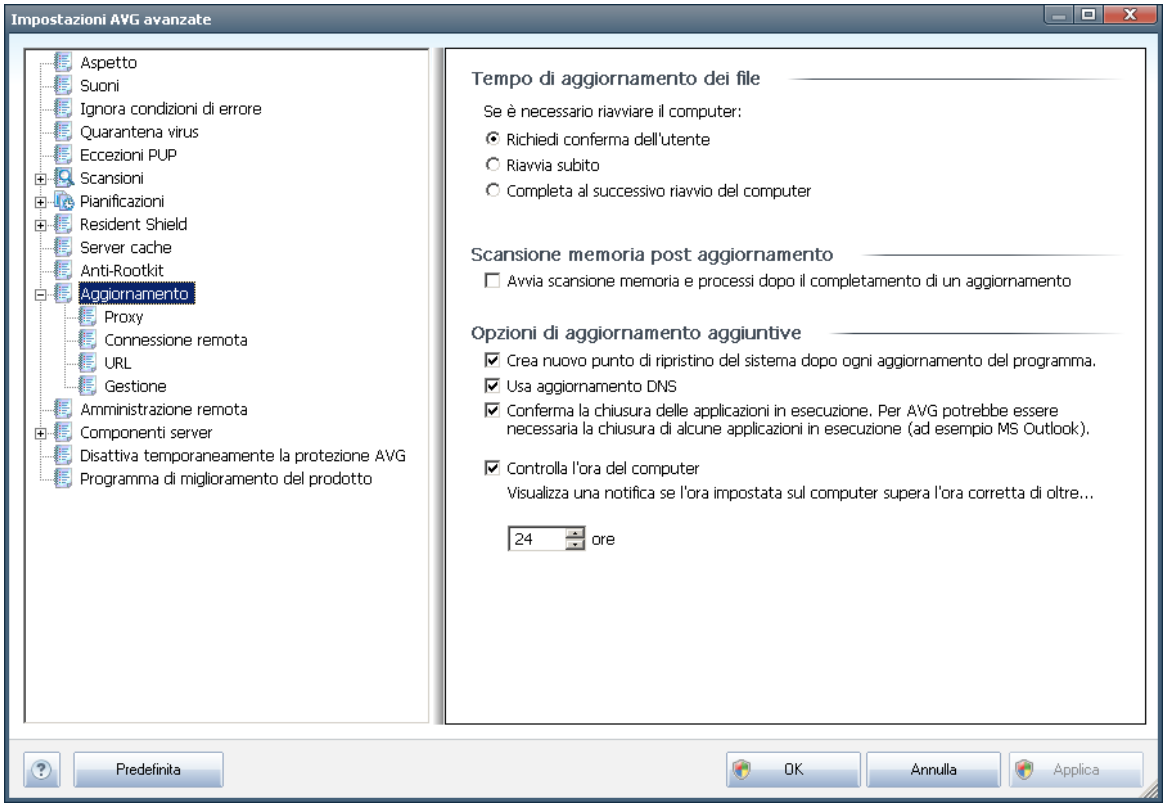
- ***Scansione applicazioni***
- ***Scansione librerie DLL***
- ***Scansione unità***

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*)

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

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

- ***Richiedi conferma dell'utente***: verrà richiesto di approvare un riavvio del PC necessario per finalizzare il processo di 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 riavvio successivo del computer. È bene ricordare che questa opzione è consigliata solo se si è sicuri che il computer viene riavviato regolarmente, almeno una volta al giorno

Scansione memoria post aggiornamento

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

Opzioni di aggiornamento aggiuntive

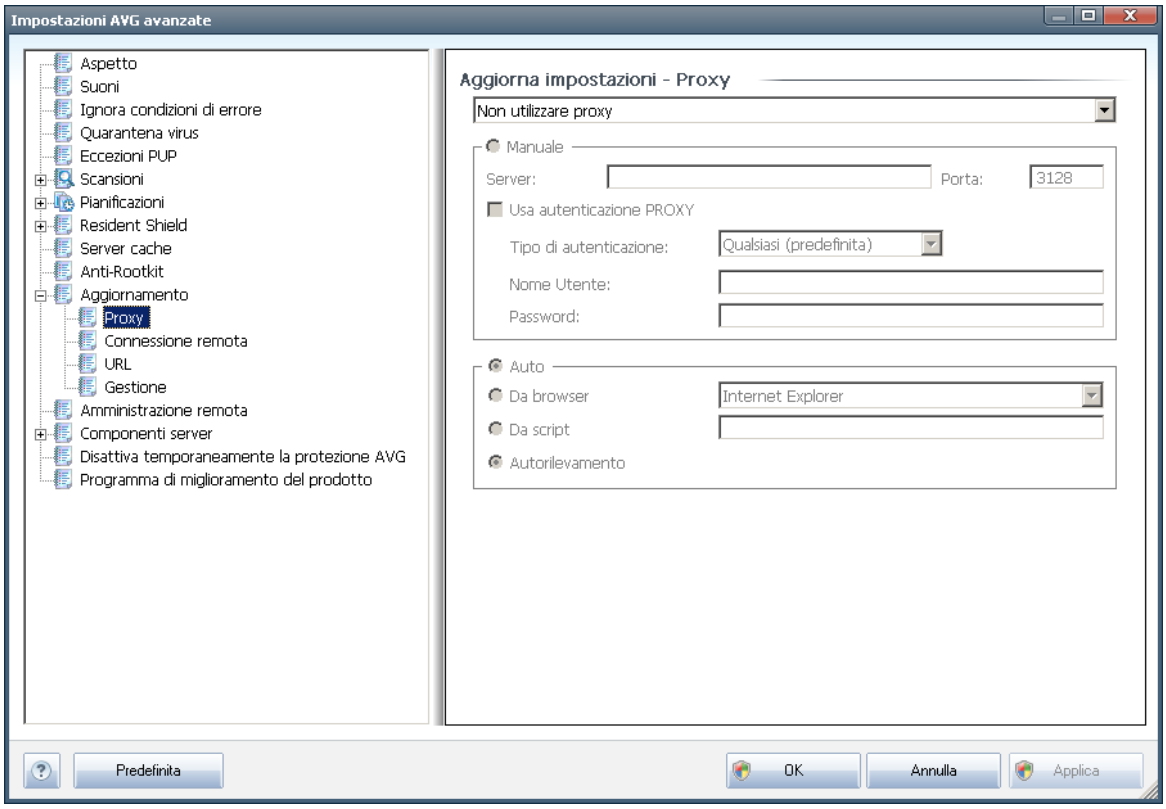
- ***Crea nuovo punto di ripristino del sistema durante ogni aggiornamento del programma***: prima dell'avvio di ciascun aggiornamento del programma AVG viene creato un punto di ripristino del sistema. Se il processo di aggiornamento non ha esito positivo e il sistema operativo si blocca, è possibile 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***: selezionare questa casella di controllo per confermare che si desidera utilizzare il metodo di rilevamento dei file di aggiornamento che elimina le quantità di dati trasferite tra il server di aggiornamento e il client AVG;

- ***Conferma la chiusura delle applicazioni in esecuzione*** (*attiva per impostazione predefinita*) garantirà che nessuna applicazione in esecuzione venga chiusa senza autorizzazione, nel caso fosse necessario per la finalizzazione del processo di aggiornamento;

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

11.11.1. 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*)

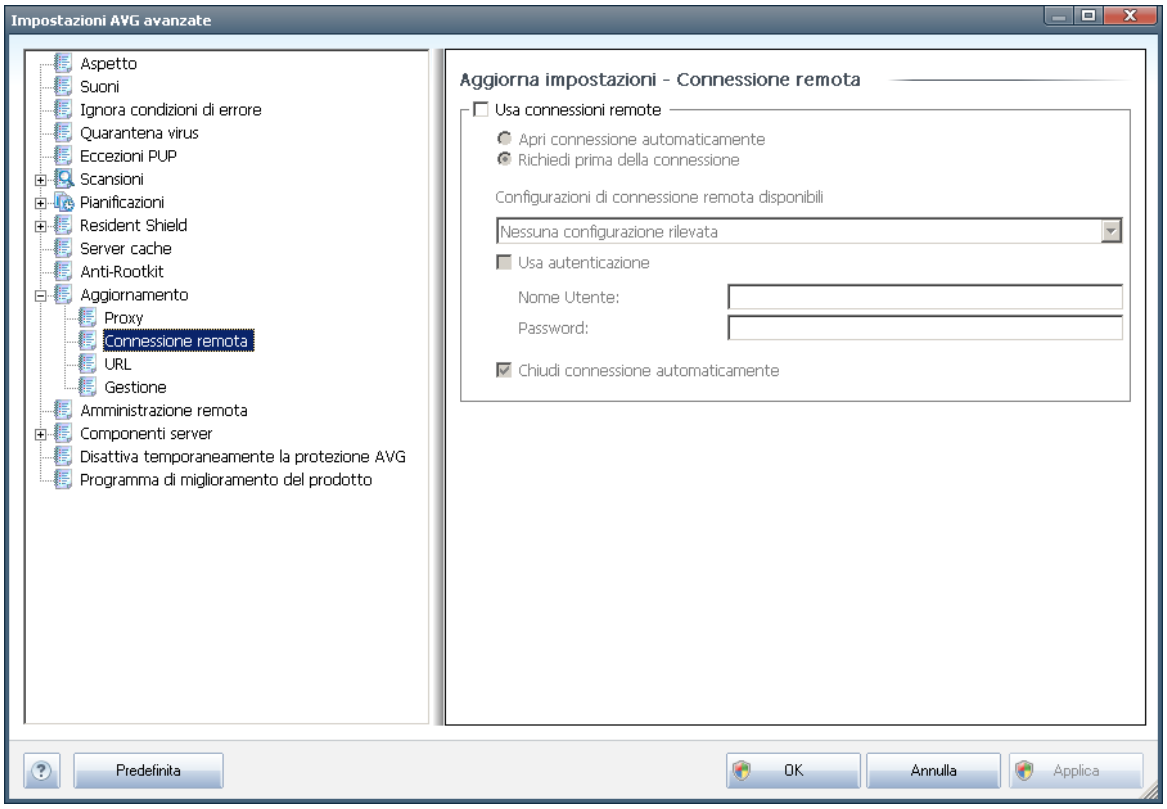
È anche possibile che sul server proxy siano state configurate regole specifiche per ciascun utente. Se il server proxy è impostato in questo modo, selezionare l'opzione ***Usa autenticazione PROXY*** per verificare che nome utente e password siano validi per la connessione a Internet tramite il server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

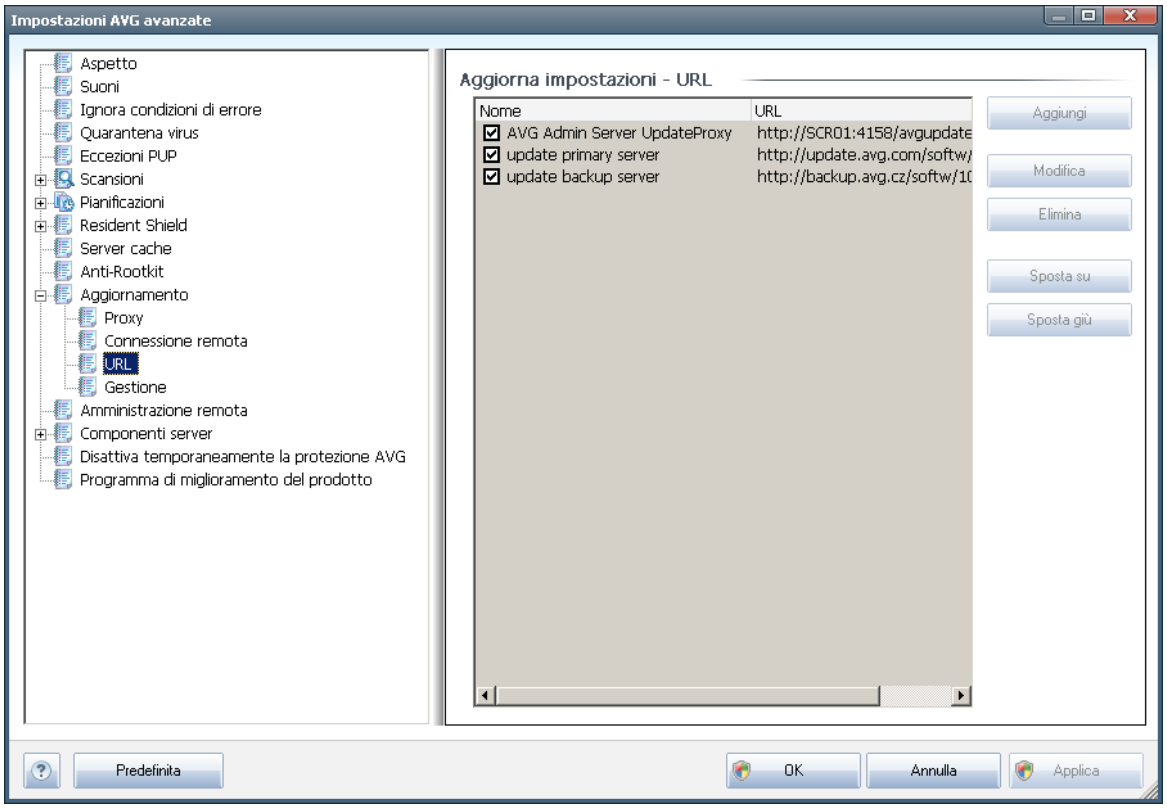
11.11.2. Connessione remota



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***).

11.11.3. URL

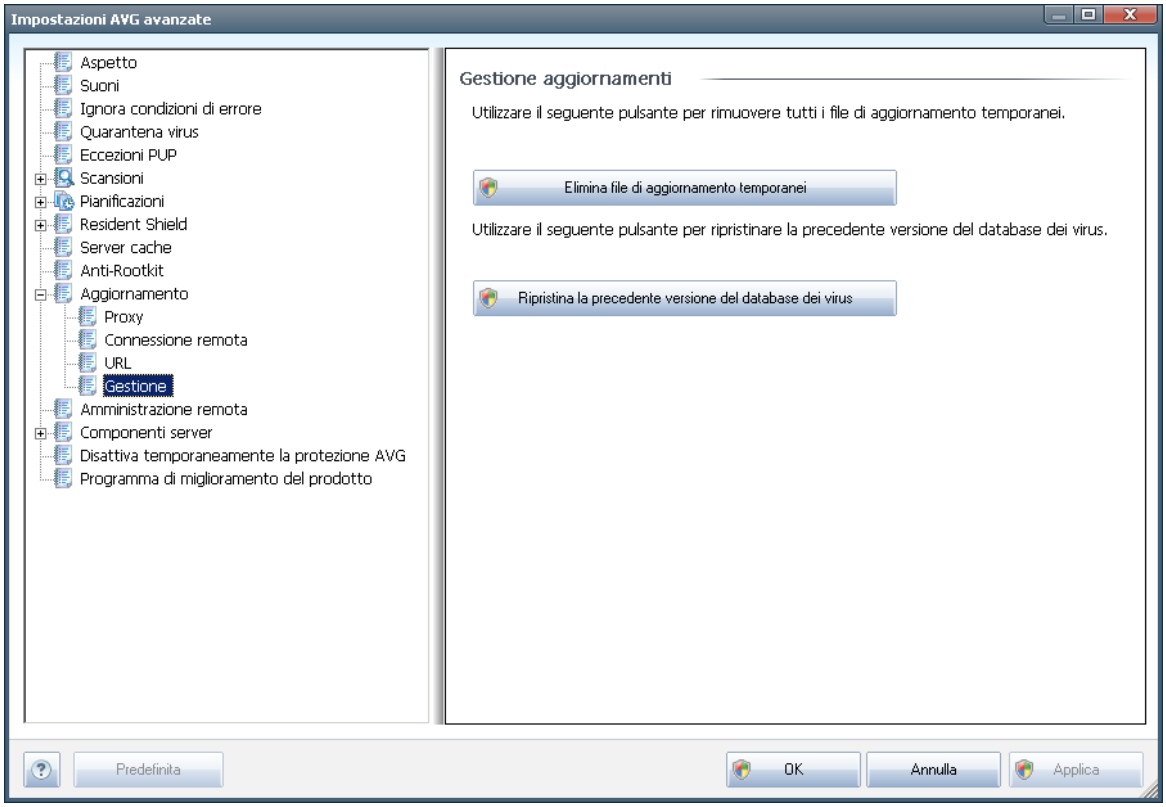


Nella finestra di dialogo ***URL*** è contenuto un elenco di indirizzi Internet da cui è possibile scaricare i file di aggiornamento. È possibile modificare l'elenco e i suoi elementi utilizzando i seguenti pulsanti di controllo:

- ***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

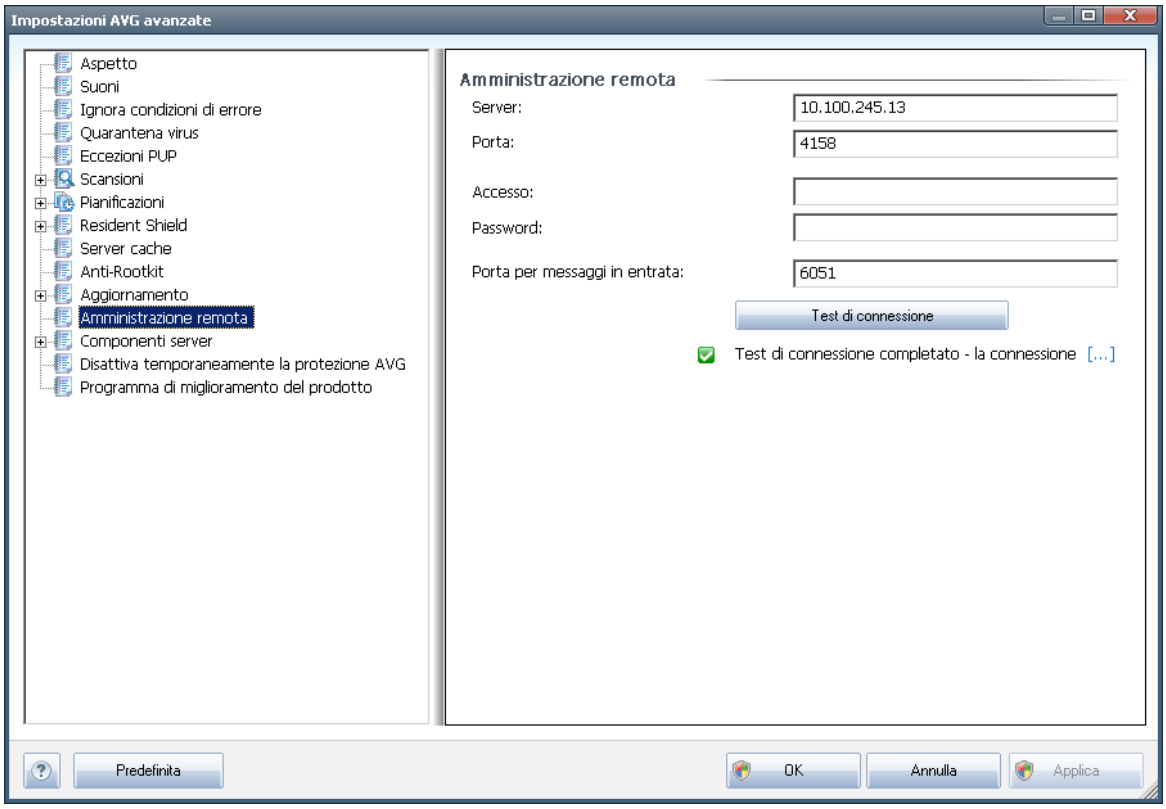
11.11.4. Gestione

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*)

11.12. Amministrazione remota



Le impostazioni di ***Amministrazione remota*** fanno riferimento alla connessione della workstation client AVG al sistema di amministrazione remota. Se si prevede di connettere la workstation corrispondente all'amministrazione remota, specificare i seguenti parametri:

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

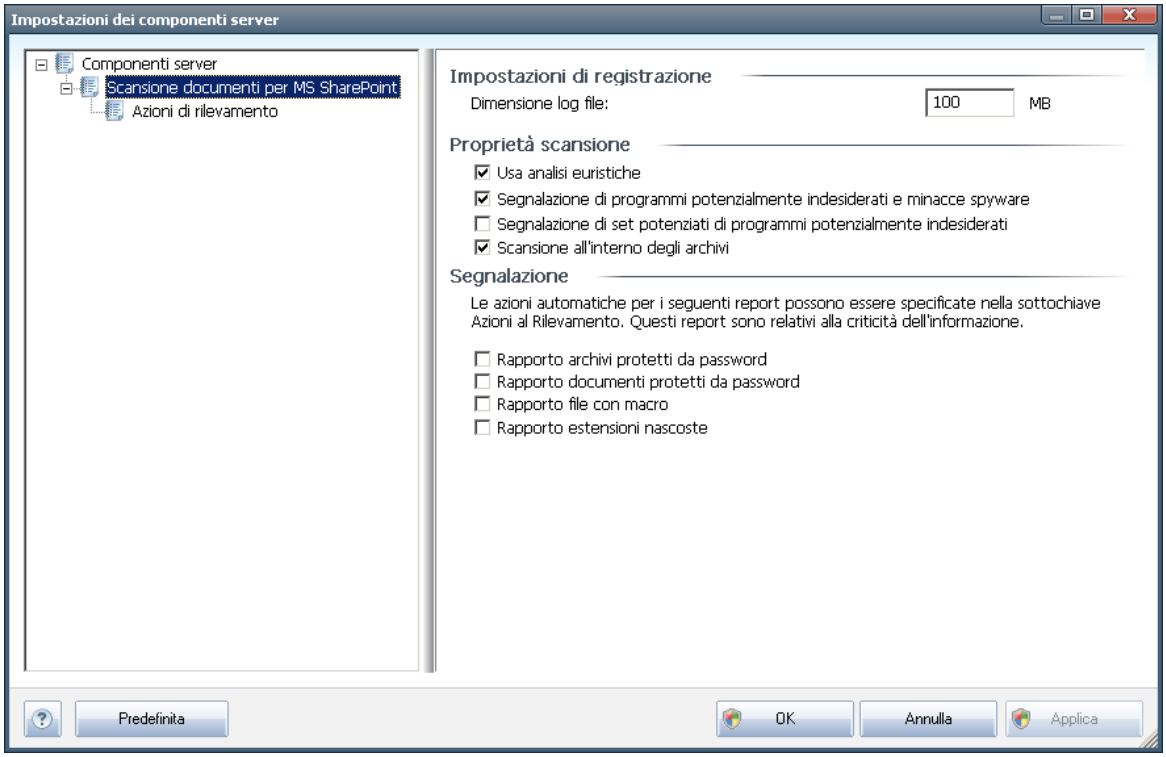
Il pulsante ***Test di connessione*** consente di verificare che tutti i dati indicati in alto siano validi e possano essere utilizzati per effettuare la connessione al DataCenter.

Nota: *per una descrizione dettagliata dell'amministrazione remota consultare la documentazione dei prodotti AVG Business Edition.*

11.13. Componenti server

11.13.1. Scansione documenti per MS SharePoint

In questa finestra di dialogo sono disponibili diverse opzioni preimpostate relative alle prestazioni della scansione antivirus dei documenti di ***Scansione documenti per MS SharePoint***. La finestra di dialogo è suddivisa in diverse sezioni:



Impostazioni di registrazione

Campo Dimensione log file: il file log contiene un registro dei vari eventi relativi a ***Scansione documenti per MS SharePoint***, ad esempio note di caricamento delle librerie del programma, eventi di rilevamento dei virus, avvisi per la risoluzione dei problemi e così via. Utilizzare il campo di testo per impostare la dimensione massima del file.

Proprietà scansione

- ***Usa analisi euristiche***: selezionare questa casella di controllo per utilizzare il metodo di rilevamento mediante analisi euristica durante la scansione dei

documenti. Se questa opzione è selezionata, è possibile filtrare i documenti non solo per estensione, ma anche in base al contenuto effettivo.

- ***Segnalazione di programmi potenzialmente indesiderati e minacce spyware***: selezionare questa casella di controllo per attivare il motore Anti-Spyware e rilevare e segnalare programmi potenzialmente indesiderati e sospetti durante la scansione dei documenti.

- ***Segnalazione di set potenziati di programmi potenzialmente indesiderati*** : selezionare questa casella per rilevare pacchetti estesi di spyware: programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi successivamente, oppure programmi che sono sempre innocui, ma potrebbero non essere desiderati (varie barre degli strumenti e così via). Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione e l'affidabilità del computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita. Nota: questa funzionalità di rilevamento è aggiuntiva rispetto alla precedente opzione. Pertanto, se si desidera la protezione dai tipi di spyware di base, mantenere sempre selezionata la precedente casella.

- ***Scansione all'interno degli archivi***: selezionare questa casella di controllo per eseguire la scansione del contenuto degli archivi.

Segnalazione

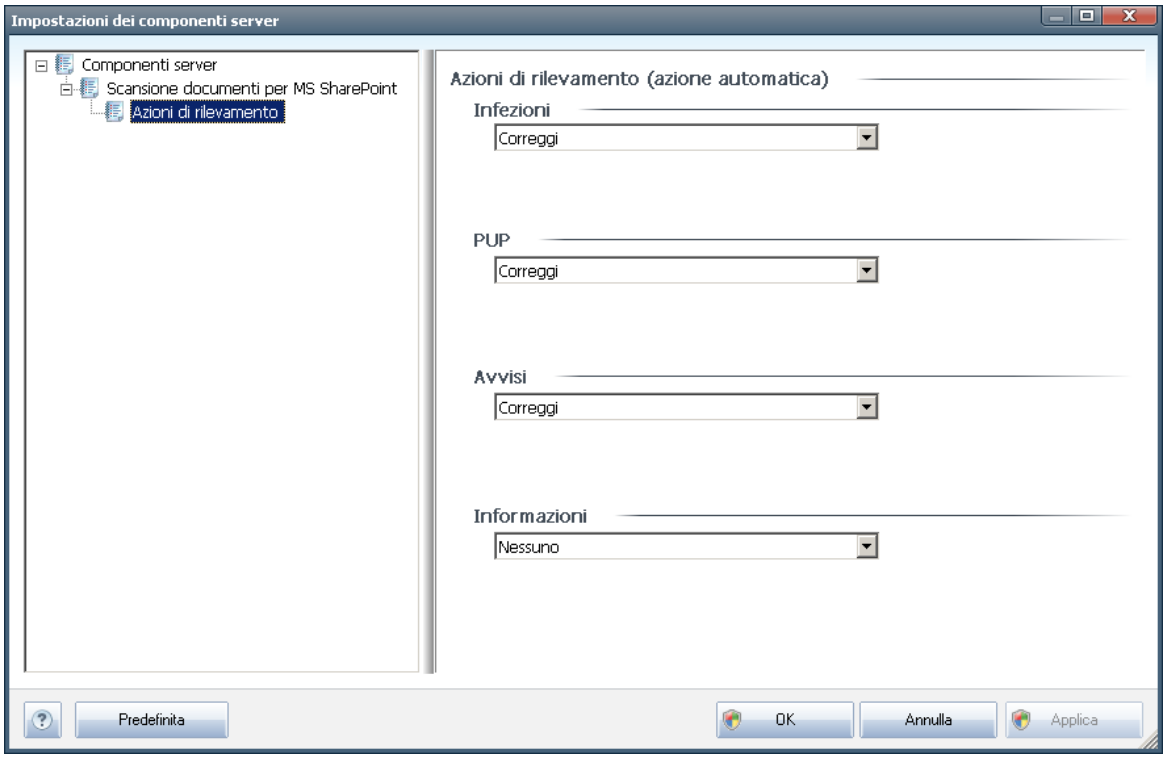
- ***Segnala archivi protetti da password***: gli archivi (ZIP, RAR e così via) protetti da password non possono essere sottoposti alla scansione antivirus. Selezionare la casella di controllo se si desidera che questi file vengano segnalati come potenzialmente pericolosi.

- ***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.

11.13.2. Azioni di rilevamento



In questa finestra di dialogo è possibile configurare il comportamento di ***Scansione documenti per MS SharePoint*** in caso di rilevamento di una minaccia. Le minacce sono suddivise in diverse categorie:

- ***Infezioni***: codice dannoso che viene copiato e diffuso automaticamente, spesso in modo nascosto fino al compimento del danno.
- ***Programmi potenzialmente indesiderati***: questi programmi in genere variano da veri positivi a semplici minacce potenziali per la privacy.
- ***Avvisi***: oggetti rilevati che non possono essere esaminati.
- ***Informazioni***: include tutte le minacce potenziali rilevate che non possono essere classificate in una delle suddette categorie.

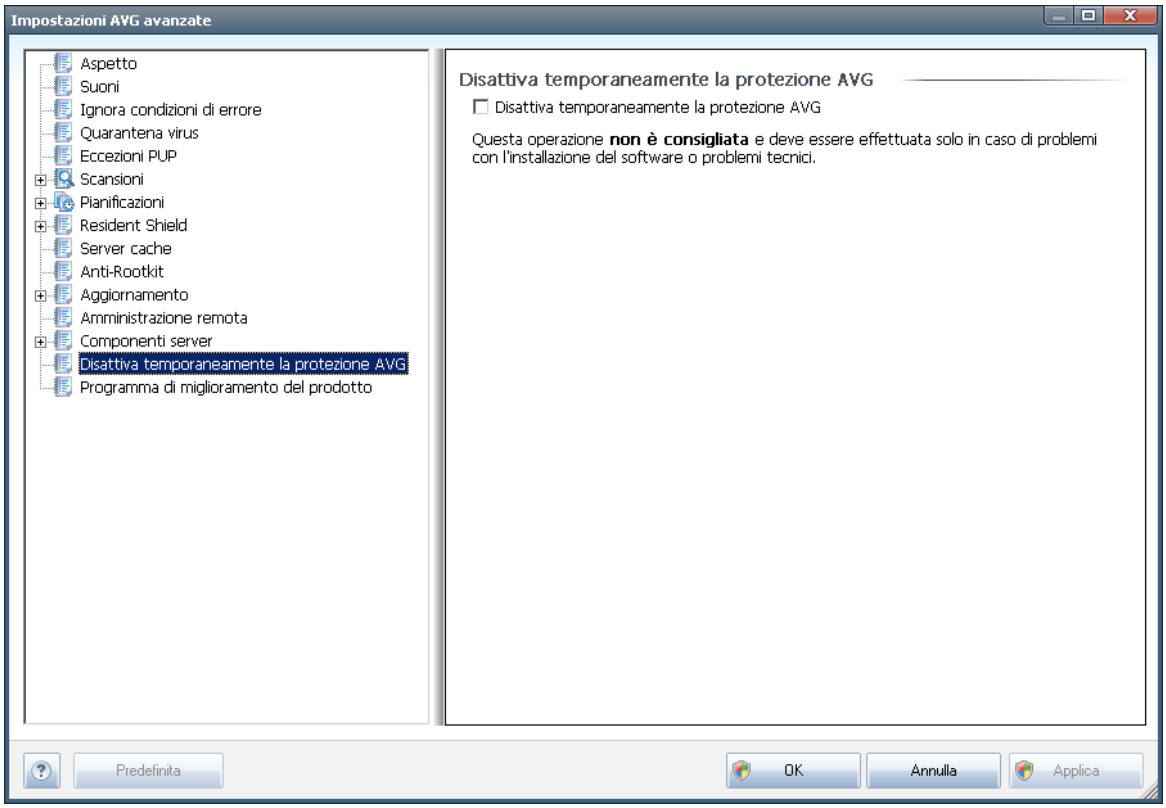
Utilizzare i menu a discesa per selezionare un'azione automatica per ogni categoria:

- ***Nessuna***: sul documento contenente tale minaccia non verrà eseguita alcuna azione.
- ***Correggi***: tenta di correggere il file/documento infetto.
- ***Sposta in quarantena***: ogni documento infetto verrà spostato in Quarantena

virus.

- ***Rimuovi***: il documento in cui è stato rilevato un virus verrà eliminato.

11.14. 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 File Server 2011**.

Non utilizzare questa opzione se non è assolutamente necessario.

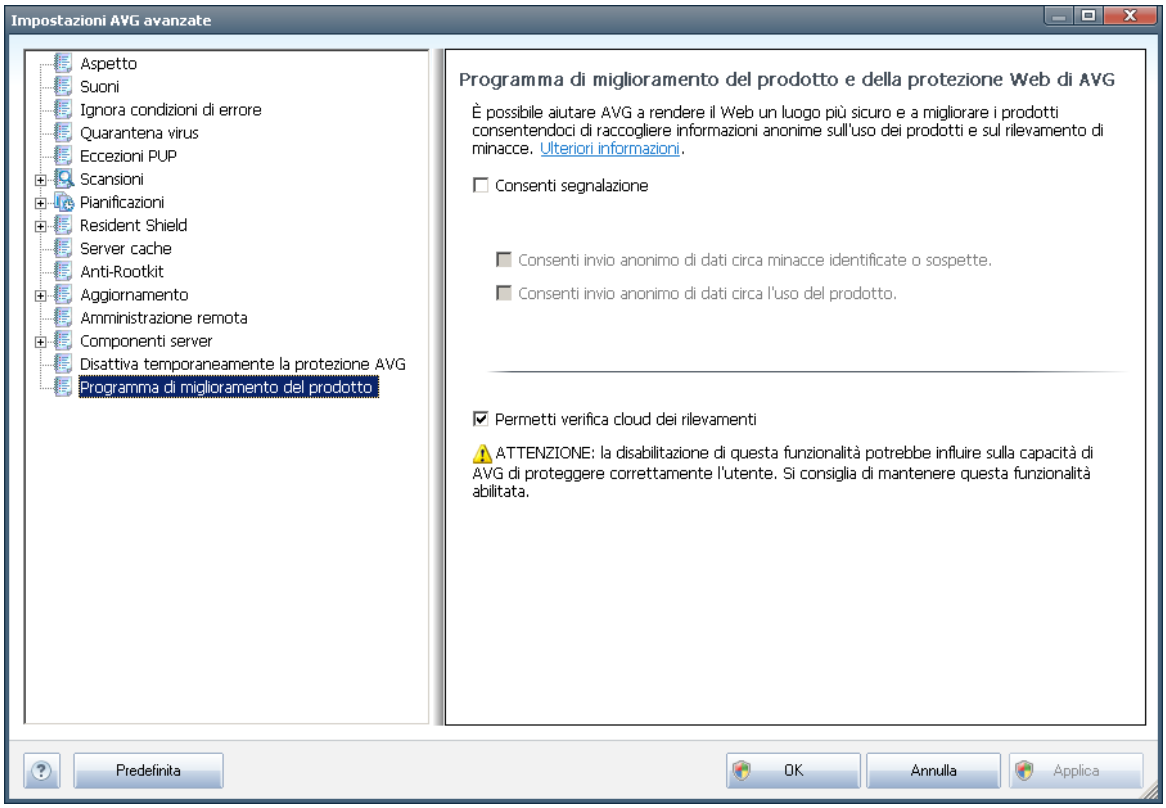
Nella gran parte dei casi, ***non è necessario*** disattivare AVG prima di installare nuovi software o driver, neppure se il programma di installazione o la procedura guidata suggeriscono di chiudere tutti i programmi e le applicazioni in esecuzione per accertarsi che non si verifichino interruzioni 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.

11.15. 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:

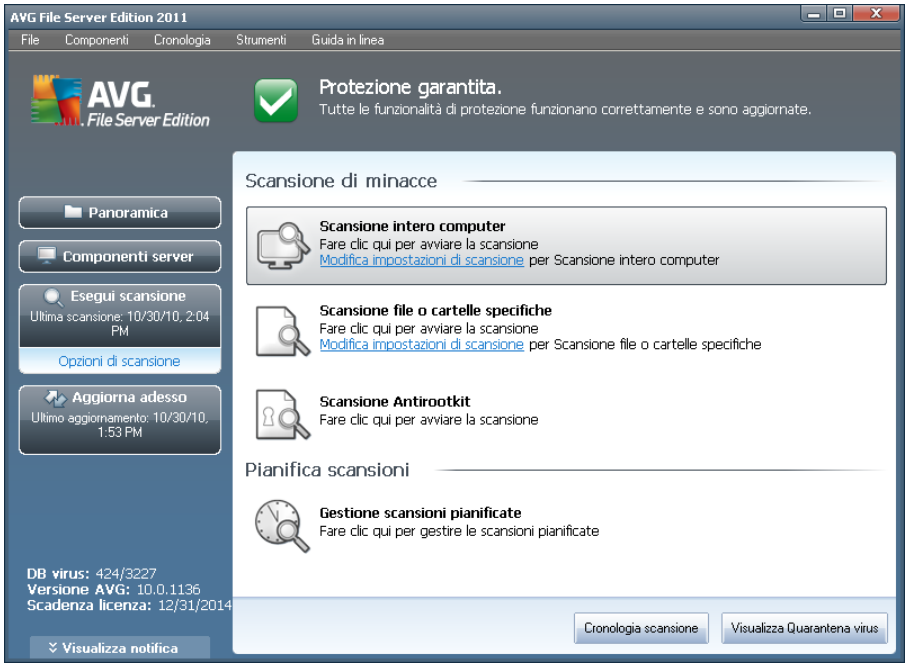
- ***Anti-Virus*** per proteggere il computer dai virus,

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

12. Scansione AVG

La scansione è una parte fondamentale della funzionalità di **AVG File Server 2011**. È possibile eseguire verifiche su richiesta o pianificarle affinché vengano eseguite su base giornaliera in un orario specifico.

12.1. Interfaccia di scansione



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

- panoramica delle scansioni predefinite: sono disponibili tre tipi di scansione definiti dal fornitore del software che possono essere utilizzati immediatamente su richiesta oppure pianificati:
  - ***Scansione intero computer***
  - ***Scansione file o cartelle specifiche***
  - ***Scansione 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

12.2. Scansioni predefinite

Una delle funzioni principali di **AVG File Server 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.

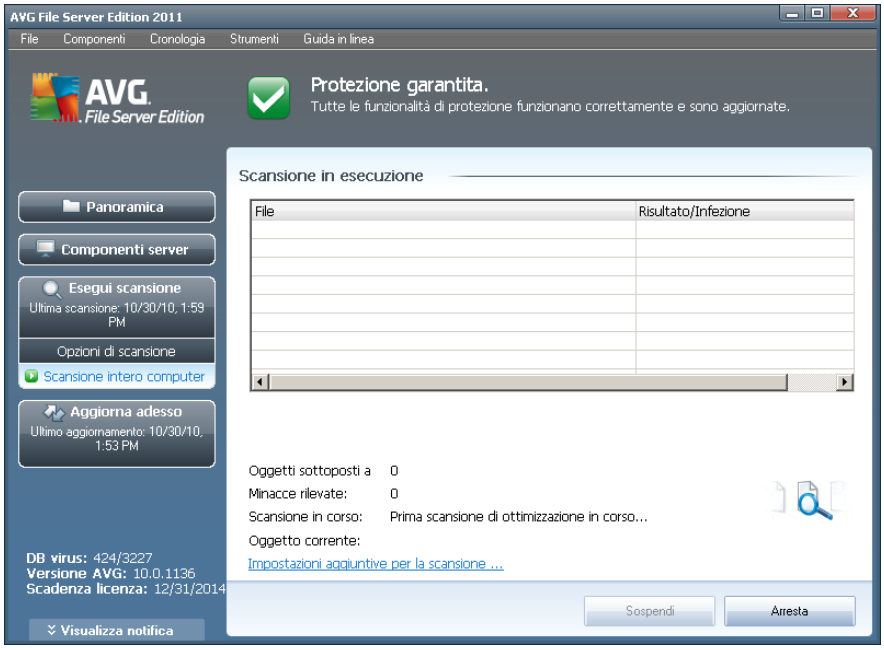
In **AVG File Server 2011** sono disponibili i seguenti tipi di scansione predefiniti dal fornitore del software:

12.2.1. 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.

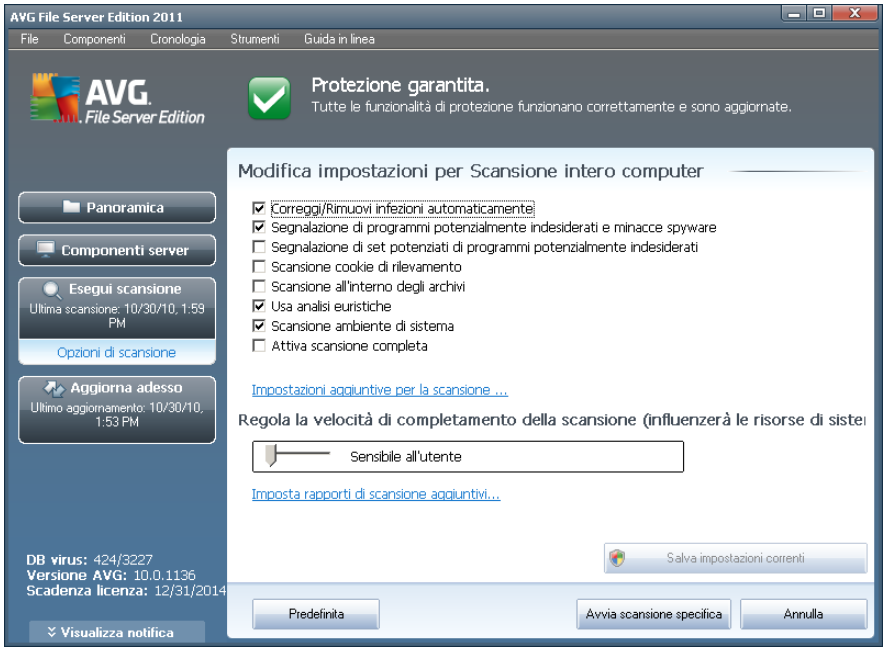
Avvio della scansione

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.

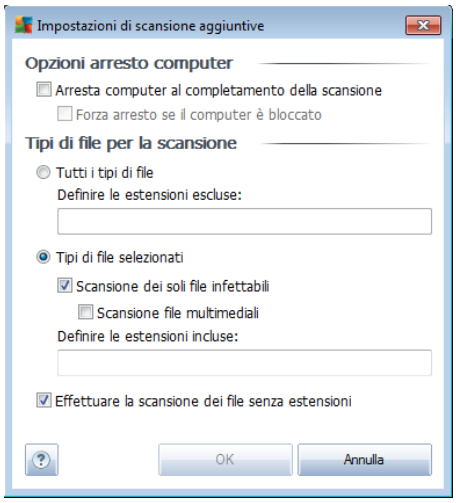
    - ***Segnalazione di set potenziati di programmi potenzialmente indesiderati*** (*disattivata per impostazione predefinita*): selezionare questa casella di controllo per rilevare pacchetti estesi di spyware, programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, 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:

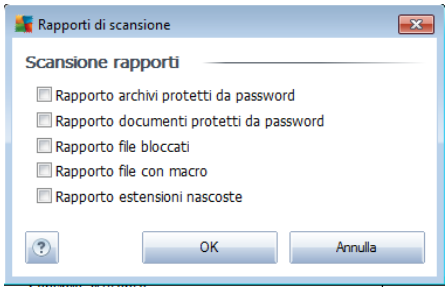


- ***Opzioni arresto computer***: consente di decidere se il computer deve essere arrestato automaticamente al termine del processo di scansione. Dopo aver confermato questa opzione (***Arresta computer al completamento della scansione***), viene attivata una nuova opzione che consente l'arresto del 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, la priorità è impostata sul livello *Sensibile all'utente* per ottimizzare la velocità del processo di scansione e l'utilizzo delle risorse di sistema. In alternativa, è possibile eseguire il processo di scansione più lentamente così da ridurre al minimo il carico sulle risorse di sistema (*utile quando è necessario lavorare al computer ma la durata della scansione non influisce*) o più velocemente con requisiti di risorse di sistema più elevati (*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.*

12.2.2. Scansione file o cartelle specifiche

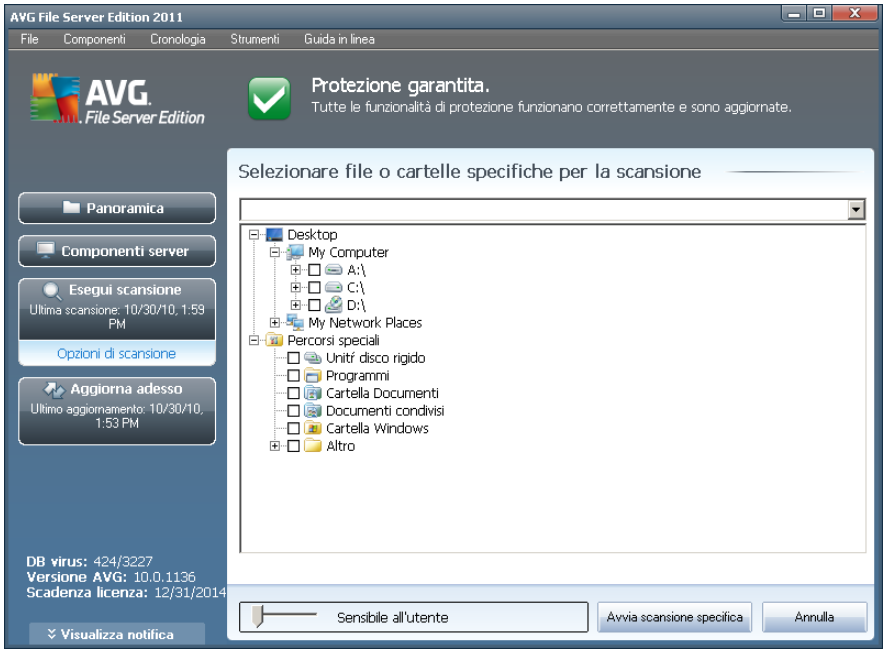
Scansione file o cartelle specifiche: consente di eseguire la scansione delle sole aree del computer selezionate per la scansione (*cartelle, dischi rigidi, dischi floppy, CD selezionati e così via*). L'avanzamento della scansione nel caso di rilevamento di virus e relativo trattamento è uguale a quello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

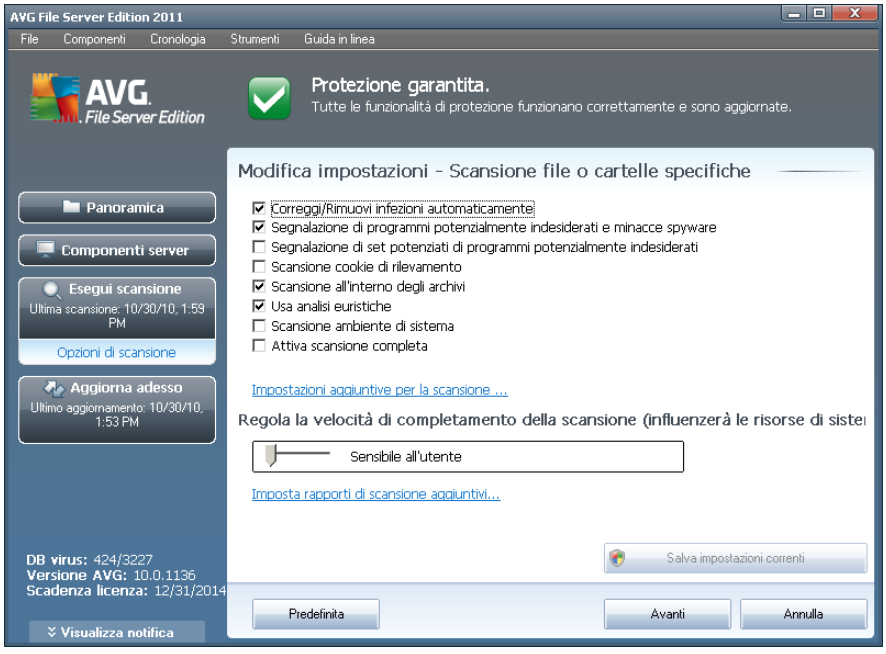
È possibile sottoporre a scansione una specifica cartella escludendo tutte le sottocartelle relative; a questo scopo scrivere un segno meno "**-**" davanti al percorso generato automaticamente (*vedere la schermata*). Per escludere l'intera cartella dalla scansione, utilizzare il parametro "!".

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

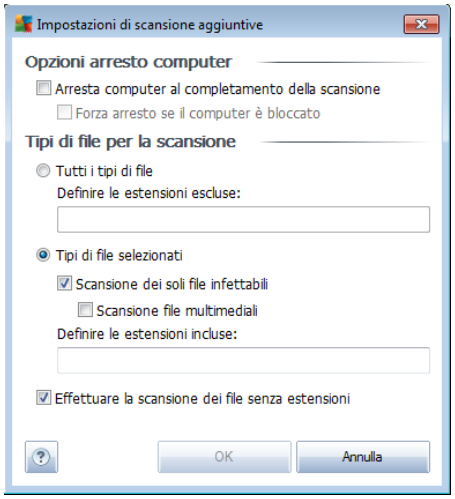
  - ***Usa analisi euristiche*** (*disattivata per impostazione predefinita*): l'analisi euristica (*emulazione dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale*) sarà uno dei metodi utilizzati per il rilevamento di virus durante la scansione.

  - ***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;

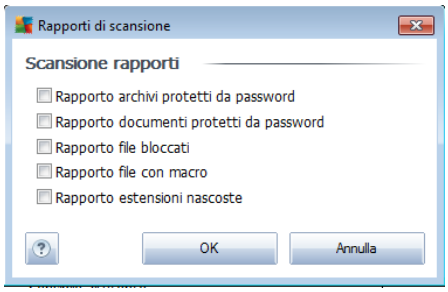
    - ***Tipi di file selezionati***: è possibile specificare che si desidera sottoporre a scansione solo file potenzialmente infettabili (*i file che non possono essere infettati non verranno sottoposti a scansione, ad esempio alcuni file di testo normale o altri file non eseguibili*), inclusi i file multimediali (*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, la priorità è impostata sul livello *Sensibile all'utente* per ottimizzare la velocità del processo di scansione e l'utilizzo delle risorse di sistema. In alternativa, è possibile eseguire il processo di scansione più lentamente così da ridurre al minimo il carico sulle risorse di sistema (*utile quando è necessario lavorare al computer ma la durata della scansione non influisce*) o più velocemente con requisiti di risorse di sistema più elevati (*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).*

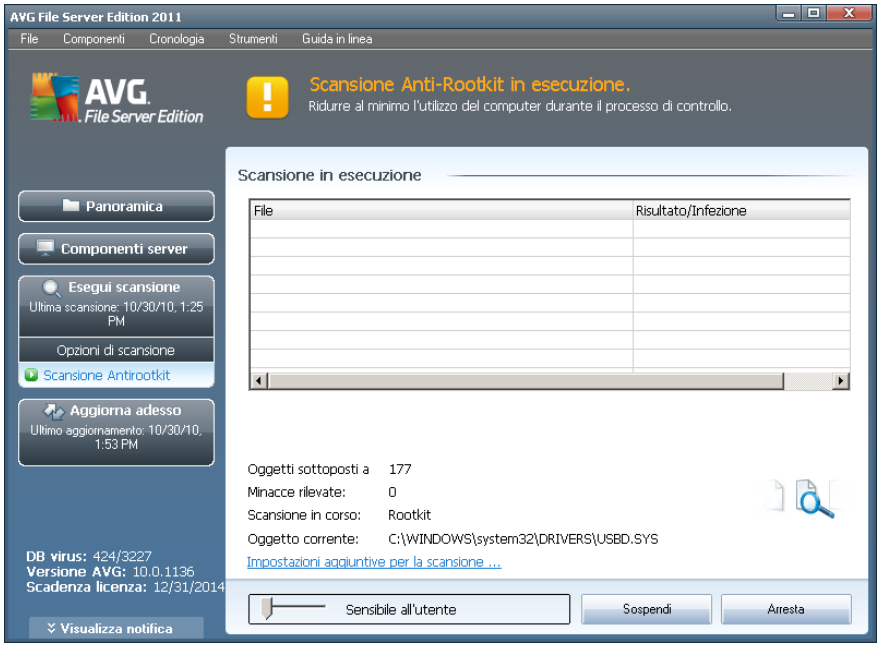
12.2.3. Scansione Anti-Rootkit

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.

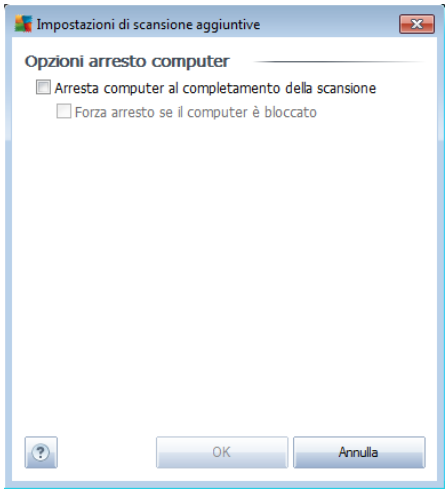


Modifica della configurazione della scansione

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:

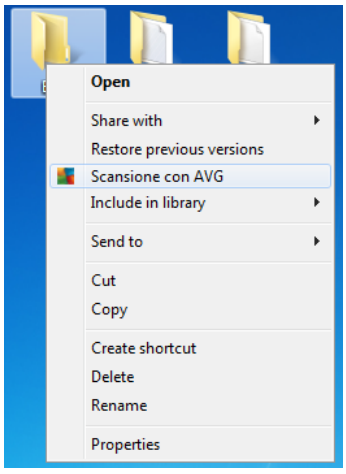
- ***Scansione automatica***: è possibile utilizzare il dispositivo di scorrimento per modificare la priorità del processo di scansione. Per impostazione predefinita, la priorità è impostata sul livello medio (*Scansione automatica*) per ottimizzare la velocità del processo di scansione e l'utilizzo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



12.3. Scansione in Esplora risorse

Oltre alle scansioni predefinite avviate per l'intero computer o per le aree selezionate, **AVG File Server 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

12.4. Scansione da riga di comando

In **AVG File Server 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.

12.4.1. 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

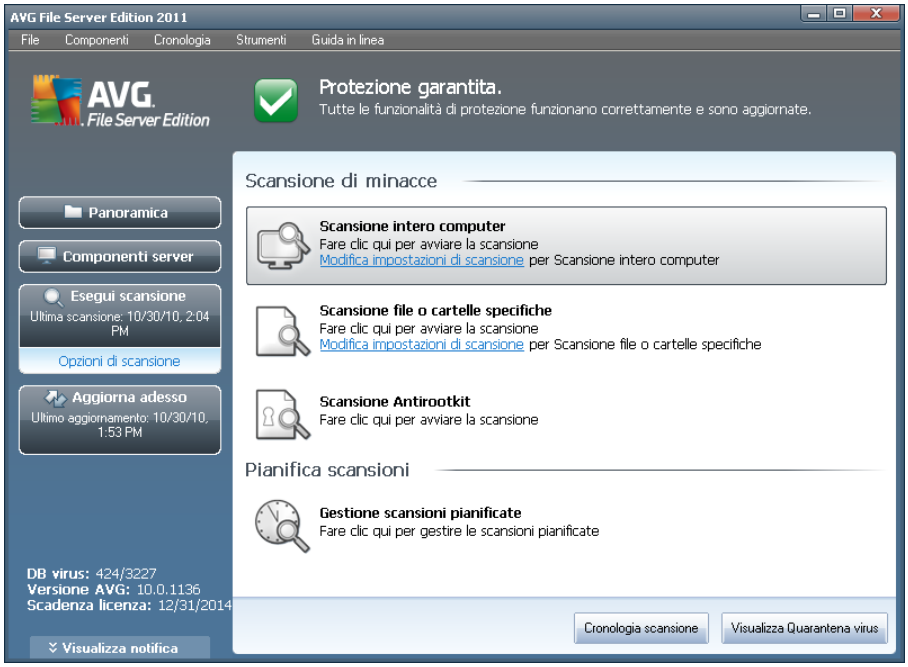
- ***/BOOT*** Abilita controllo MBR/BOOT
- ***/PROC*** Scansione dei processi attivi
- ***/PUP*** Segnala "Programmi potenzialmente indesiderati"
- ***/REG*** Scansione Registro di sistema
- ***/COO*** Esegui scansione dei cookie
- ***/?*** Visualizza la Guida sull'argomento
- ***/HELP*** Visualizza 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

12.5. Pianificazione di scansioni

AVG File Server 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.

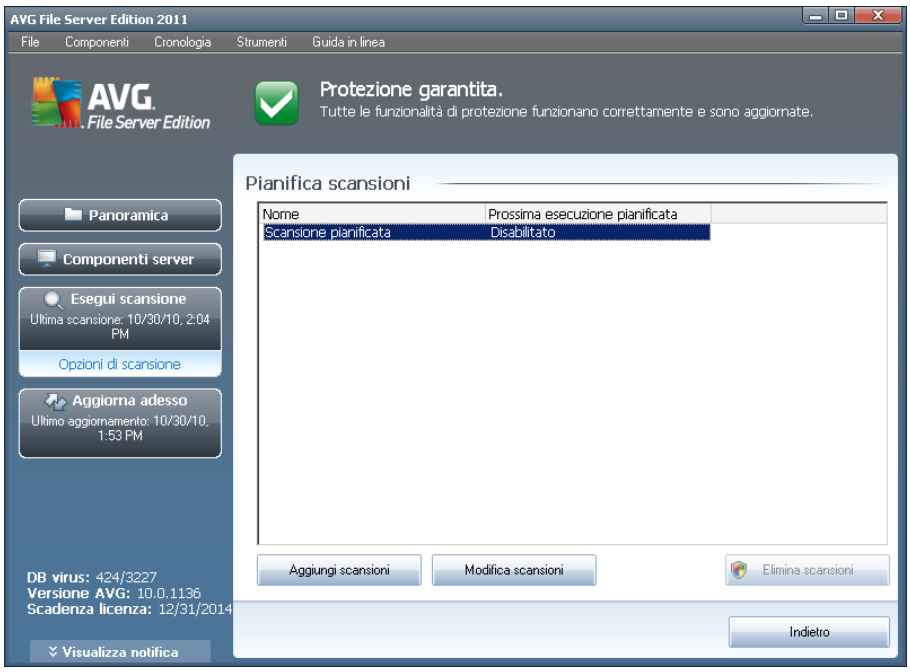
Scansione intero computer deve essere avviata regolarmente, almeno una volta alla settimana. Tuttavia, se possibile, avviare la scansione dell'intero computer ogni giorno, come impostato nella configurazione predefinita della pianificazione della scansione. Se il computer è sempre acceso, è possibile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

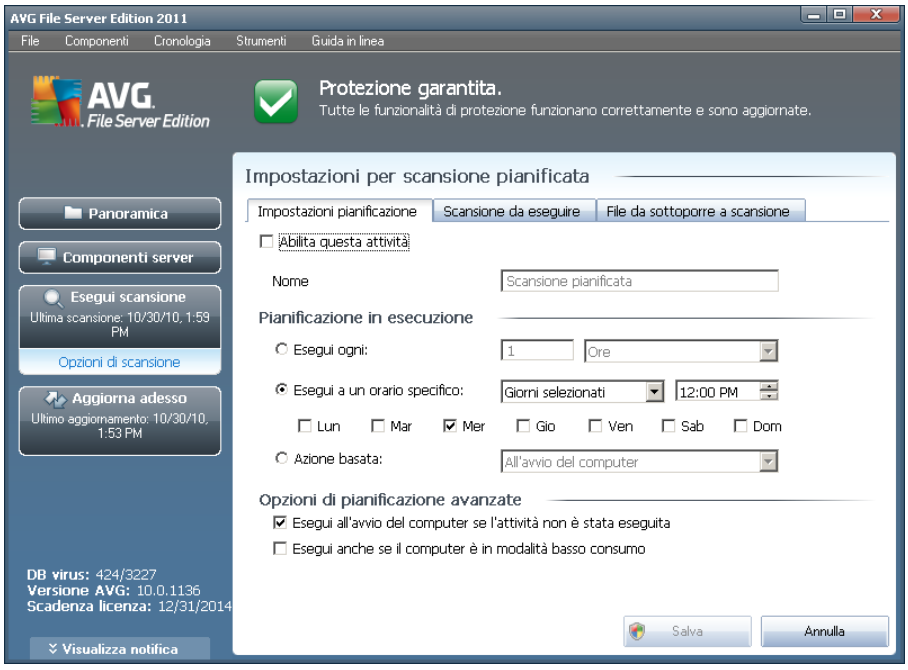
- ***Modifica pianificazione scansione***: il pulsante può essere utilizzato solo se è stato selezionato in precedenza un controllo esistente dall'elenco dei controlli pianificati. In tal caso il pulsante è visualizzato come attivo e, selezionandolo, si passa alla finestra di dialogo ***Impostazioni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

12.5.1. 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.

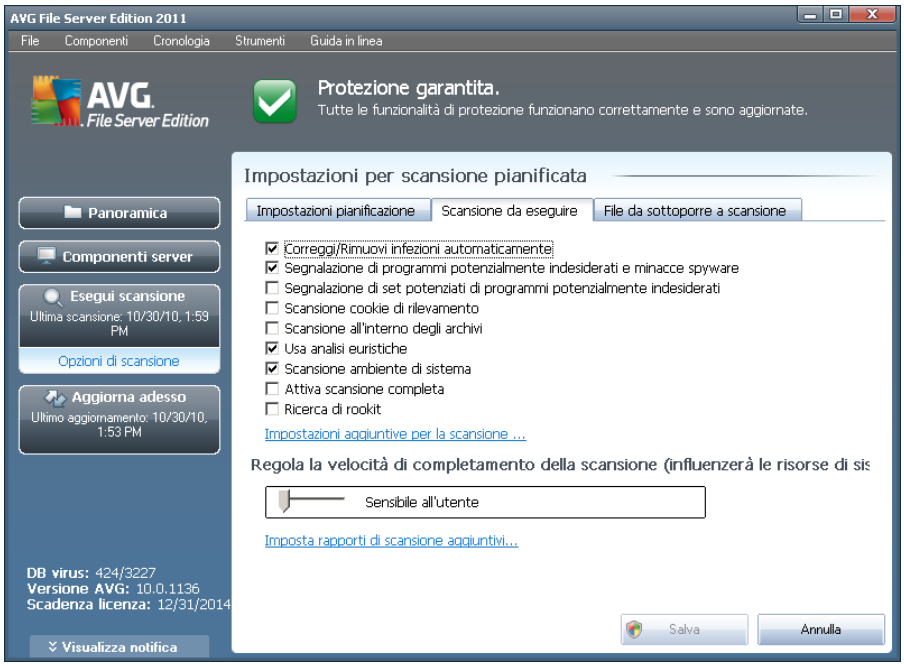
Pulsanti di controllo delle impostazioni per la finestra di dialogo della scansione pianificata

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.

12.5.2. 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.

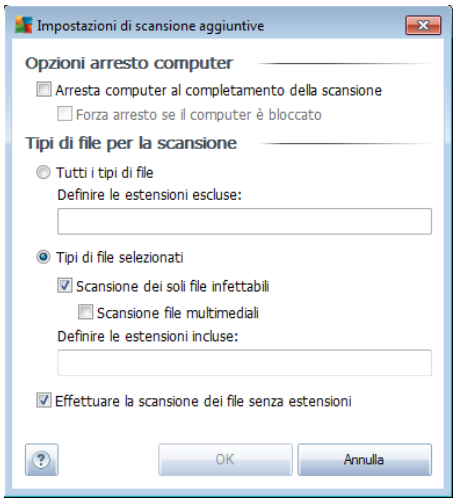
- ***Usa analisi euristiche*** (*attivata per impostazione predefinita*): l'analisi euristica (*emulazione dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale*) sarà uno dei metodi utilizzati per il rilevamento di virus durante la scansione.

- ***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:

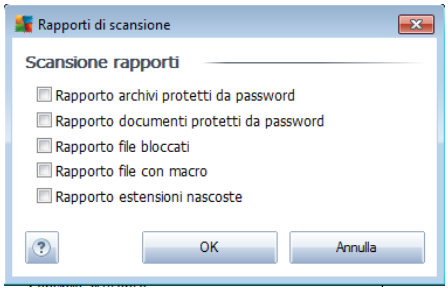
  - ***Tutti i tipi di file*** con la possibilità di definire le eccezioni fornendo un elenco di estensioni di file separate da virgola da non sottoporre a scansione;

  - ***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. Il livello medio ottimizza la velocità del processo di scansione e l'uso delle risorse di sistema. In alternativa, è possibile eseguire il processo di scansione più lentamente così 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 requisiti di risorse di sistema più elevati (*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****.*

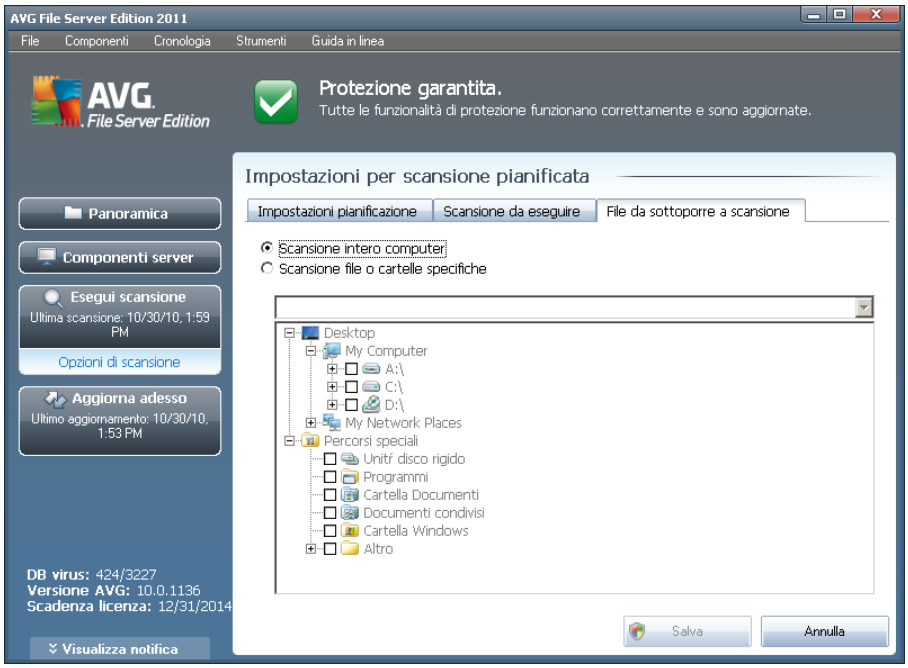
Pulsanti di controllo

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.

12.5.3. 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\

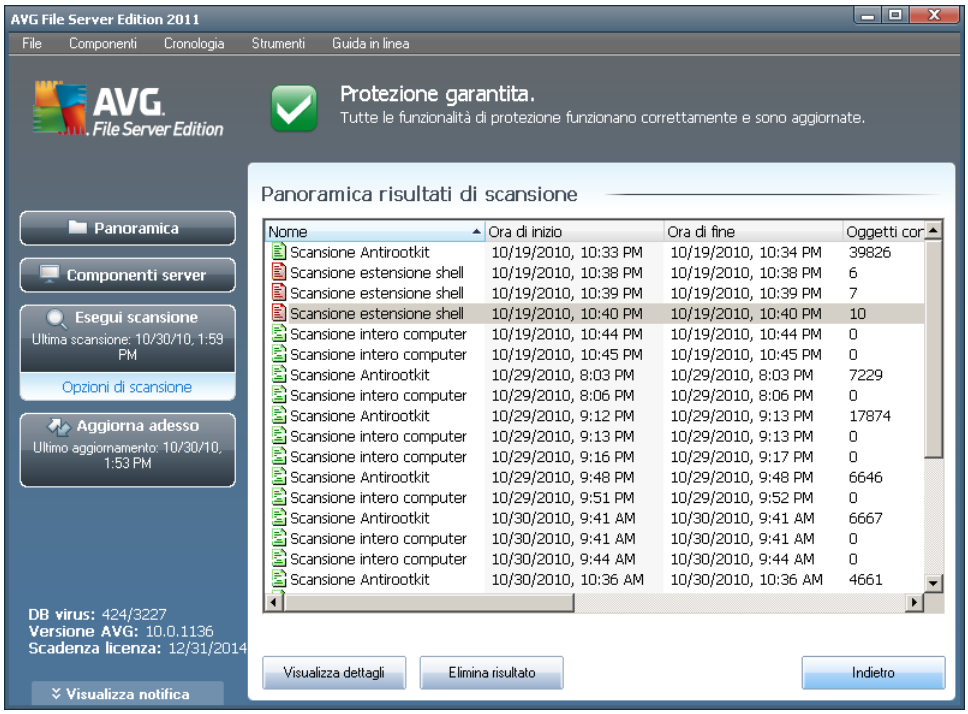
- ***Documenti condivisi***
  - *per Windows XP*: C:\Documents and Settings\All Users\Documenti condivisi\
  - *per Windows Vista/7*: C:\Users\Public\Documenti condivisi\
- ***Cartella Windows***: C:\Windows\
- ***Altro***
  - *Unità di sistema*: disco rigido su cui è installato il sistema operativo (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.

12.6. 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

12.7. Dettagli di Risultati scansione

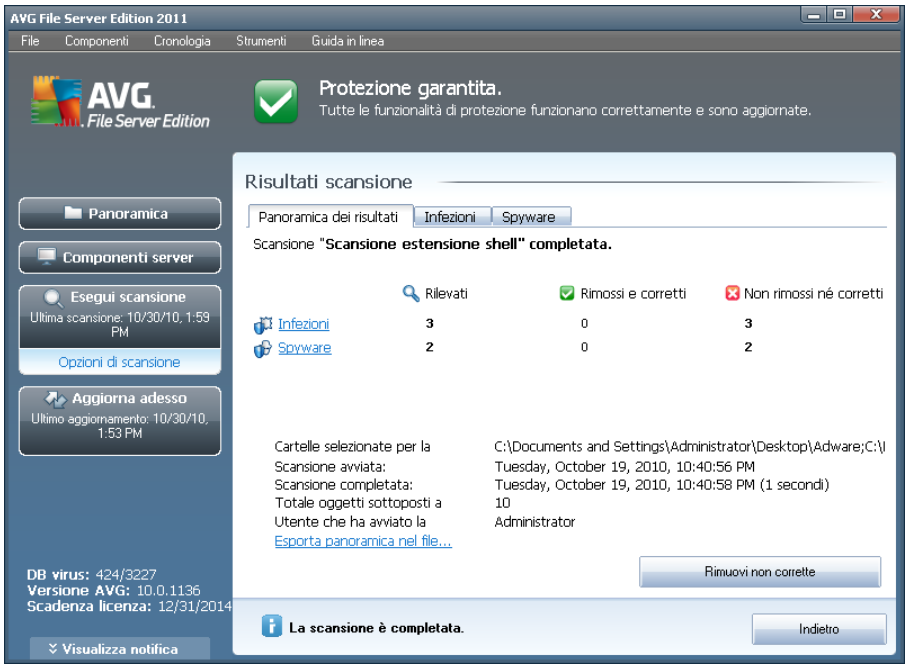
Se nella finestra di dialogo ***Panoramica risultati di scansione*** è selezionata una scansione specifica, è possibile fare clic sul pulsante ***Visualizza dettagli*** per passare alla finestra di dialogo ***Risultati scansione*** che contiene i dati dettagliati sul corso e sui risultati della scansione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

12.7.1. Scheda Panoramica dei risultati



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

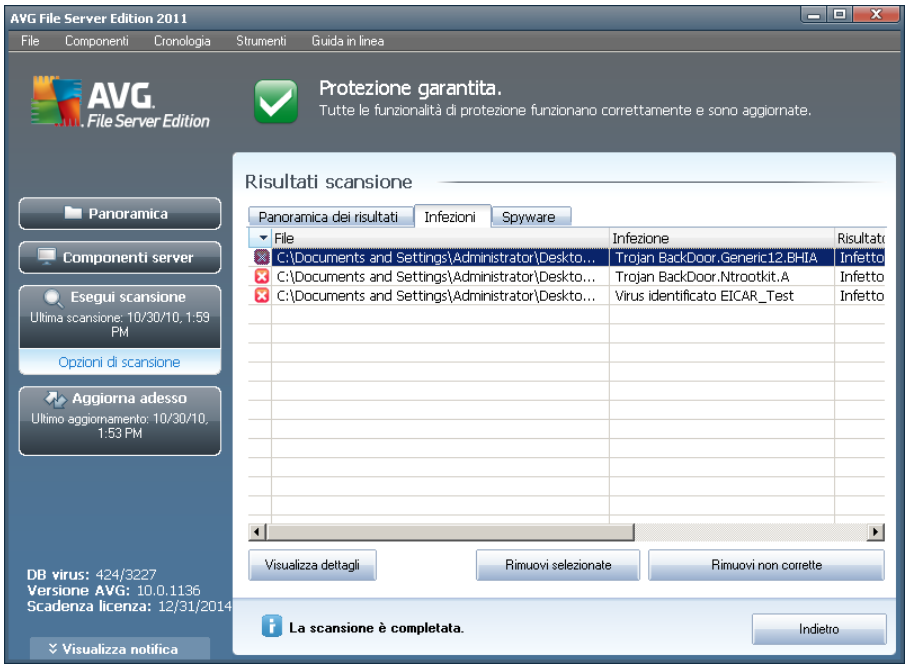
- infezioni da virus / spyware rilevate
- infezioni da virus / spyware rimosse
- numero di infezioni da virus / spyware che non è possibile rimuovere o correggere

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***.

12.7.2. 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:

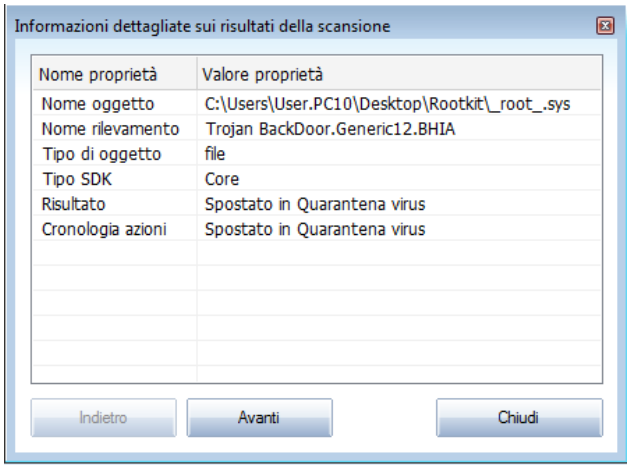
- ***File***: percorso completo della posizione originale dell'oggetto infetto
- ***Infezioni***: nome del virus rilevato (*per informazioni dettagliate su virus specifici, consultare l'Enciclopedia dei virus in linea*)
- ***Risultato***: definisce lo stato corrente dell'oggetto infetto rilevato durante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

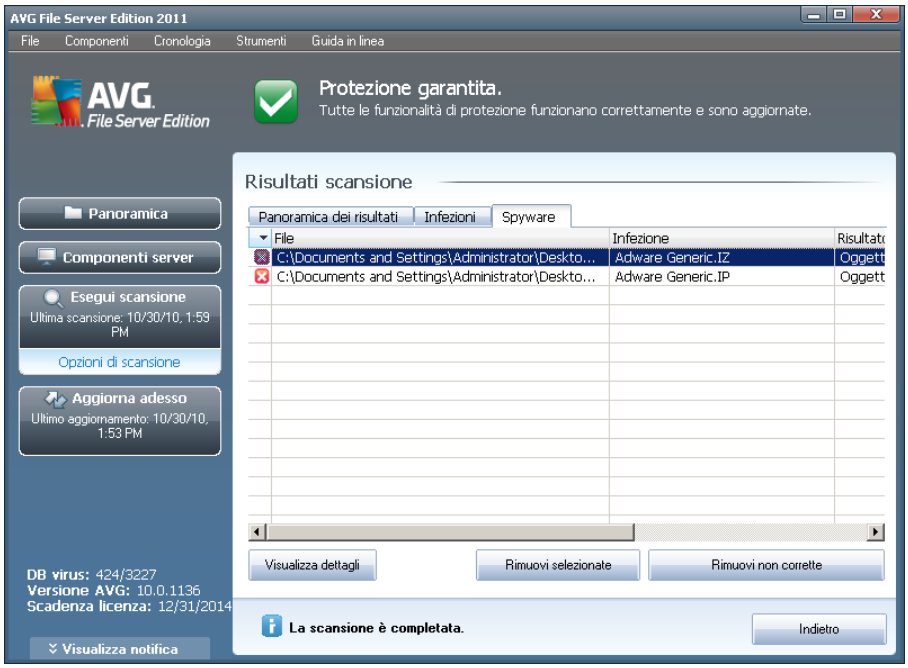


  In questa finestra di dialogo sono disponibili informazioni dettagliate sull'oggetto infetto rilevato (*ad esempio nome e posizione dell'oggetto infetto, tipo di oggetto, tipo di SDK, risultato del rilevamento e cronologia delle azioni correlate all'oggetto rilevato*). I pulsanti ***Indietro*** / ***Avanti*** 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***

12.7.3. 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:

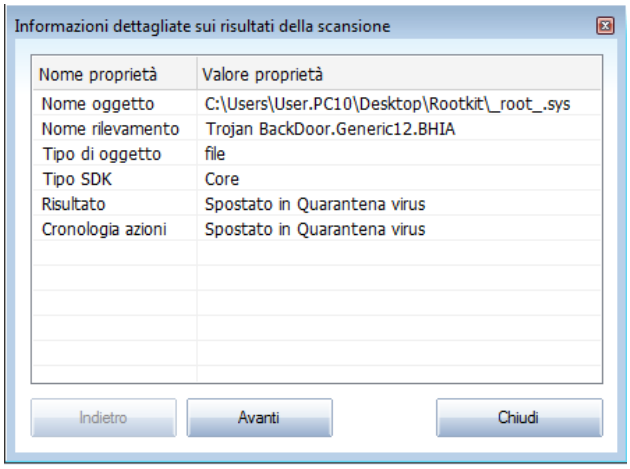
- ***File***: percorso completo della posizione originale dell'oggetto infetto
- ***Infezioni***: nome dello spyware rilevato (*per informazioni dettagliate su virus specifici, consultare l'**Enciclopedia dei virus** in linea*)
- ***Risultato***: definisce lo stato corrente dell'oggetto rilevato durante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

12.7.4. 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.

12.7.5. 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***.

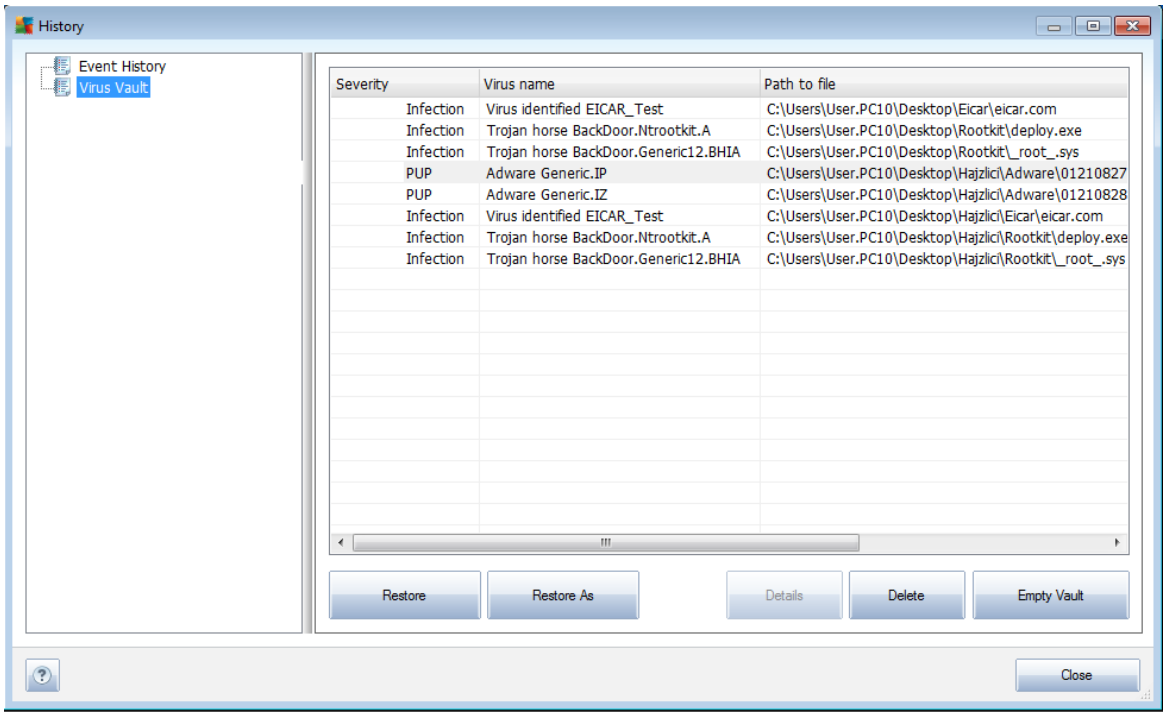
12.7.6. Scheda Informazioni

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*).

12.8. 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***: specifica il tipo di infezione (*in base al livello di infezione; tutti gli oggetti elencati possono essere certamente 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***: se si decide di spostare un oggetto infetto rilevato da ***Quarantena virus*** in una cartella selezionata, utilizzare questo pulsante. L'oggetto sospetto rilevato verrà salvato con il nome originale. Se il nome originale è sconosciuto, verrà utilizzato il nome standard.
- ***Elimina***: consente di rimuovere definitivamente il file infetto da ***Quarantena virus***
- ***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*).

13. 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 File Server 2011** venga mantenuto aggiornato anche durante la giornata.

13.1. Livelli di aggiornamento

AVG fornisce due livelli di aggiornamento selezionabili:

- ***Aggiornamento definizioni*** contiene le modifiche necessarie per una protezione antivirus affidabile. In genere, non sono incluse eventuali modifiche del codice e viene aggiornato 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.*

13.2. 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.

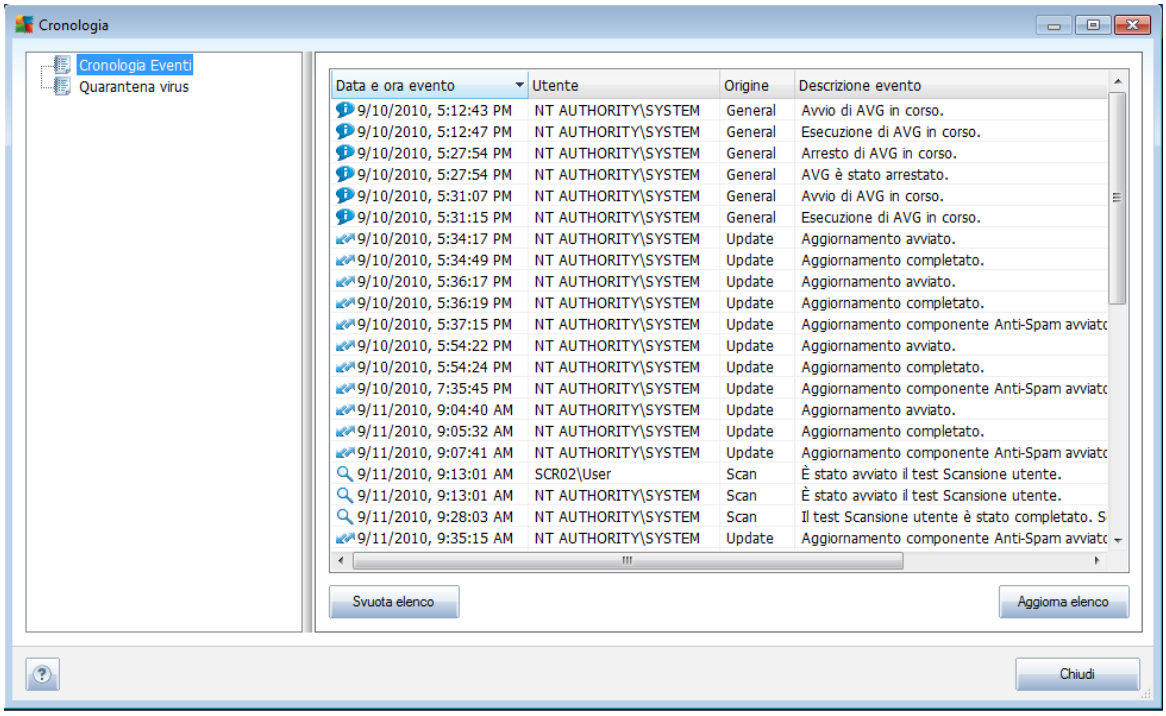
13.3. Processo di aggiornamento

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.*

14. 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 File Server 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

15. 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***.