avast! antivirus
Home Edition **4**.8

User Guide

INDICE

Introduzione

Benvenuti ad avast! antivirus Home Edition versione 4.8.

avast! antivirus rappresenta l'insieme di diverse premiate tecnologie che funzionano in perfetta sinergia, con un obiettivo comune: proteggere il vostro sistema ed i vostri preziosi dati dai virus informatici. Rappresenta la migliore soluzione per computer con piattaforma Windows.

avast! antivirus incorpora la tecnologia anti-spyware, certificata da West Coast Lab's Checkmark, anti-rootkit ed elevata capacità di protezione per i vostri dati e programmi.

A proposito di ALWIL Software a.s.

Dal 1988, ALWIL Software progetta i prodotti antivirus avast!, tra i più importanti e collaudati sul mercato e vincitore di numerosi premi.

Con sede a Praga, nella Repubblica Ceca, ALWIL Software sviluppa e commercializza i prodotti antivirus avast! per la protezione di tutti i principali sistemi operativi e dispositivi. Per ulteriori informazioni sull'azienda e i suoi prodotti vi preghiamo di visitare la nostra pagina www.avast.com

Ulteriore aiuto

Se doveste incontrare difficoltà con il programma antivirus avast!, che non riuscite a risolvere con la lettura di questo manuale, è possibile trovare la risposta nel Centro di supporto tecnico del nostro sito web:
http://support.avast.com

- Nella sezione **Knowledgebase** potete velocemente trovare le risposte alle domande più frequenti
- In alternative potete utilizzare i Forum di aiuto di avast! Qui è possibile interagire con altri utenti di avast! che hanno già trovato una soluzione al problema. Per accedere al forum occorre registrarsi, ma questo è un processo molto semplice e rapido. Per registrarsi per utilizzare il forum: **http://forum.avast.com/**

Se non ancora riuscite a risolvere il problema, è possibile "**Submit a ticket**" (inviare un messaggio) al nostro team di assistenza tecnica. Anche in questo caso è necessario registrarsi. Quando scrivete vi preghiamo di inserire quante più informazioni possibili.

Minacce per il vostro computer

Virus, spyware, rootkit e tutte le altre forme di software dannosi sono collettivamente noti come malware (abbreviazione di software dannoso); malware è anche talvolta indicato come "badware".

Cos'è un virus?

Un virus è una sorta di software, di solito "maligno", che viene utilizzato per diffondere se stesso o altri software dannosi da un computer all'altro. I virus possono causare danni del sistema, perdita di dati preziosi, e possono essere utilizzati per installare spyware, rootkit e altri malware su un sistema vulnerabile.

Un elemento chiave per prevenire l'infezione, è quello di installare un antivirus aggiornato su tutti i computer in rete. Gli utenti dovrebbero essere sicuri della fonte internet dalla quale si sta scaricando il software, perchè molti tipi di malware vengono installati insieme a software che in apparenza sembrano sicuri.

Cos'è uno spyware?

Lo spyware è un software installato su un computer e progettato per raccogliere informazioni sugli utenti, spesso senza il loro consenso. Queste informazioni possono generare i cosiddetti furti di identità, o il furto di informazioni preziose (bancarie, carte di credito) o di dati aziendali.

In questi giorni, gran parte degli spyware è sviluppata dalla criminalità organizzata, piuttosto che da singoli individui e viene installata da un virus o da un'altra forma di malware.

Cosa sono i rootkit?

I rootkit sono programmi che si installano nel vostro sistema, che mantenengono nascosti i loro processi, servizi e chiavi di Registro del sistema, in modo da rimanere invisibili all'utente. Essi rappresentano un notevole rischio per la sicurezza domestica e delle reti aziendali e sono notoriamente difficili da trovare e rimuovere.

I rootkit sono in genere installati attraverso altri malware (un cavallo di troia, ad esempio), ed è quindi molto importante che gli utenti abbiano sul loro PC un sistema antivirus / anti-spyware installato ed aggiornato. Uno di questi sistemi è avast! antivirus 4.8.

Caratteristiche principali di avast! antivirus

avast! è la multi-premiata linea di prodotti antivirus di ALWIL Software, certificata da ICSA Labs, e da Checkmark (per entrambi sia antivirus che anti-malware). avast! Antivirus riceve regolarmente sia il premio Virus Bulletin 100% per la rilevazione del 100% dei virus "in-the-wild" , sia il premio SC Awards. avast! Antivirus è in uso in 60 milioni di case ed uffici in tutto il mondo. E' specificamente progettato per avere bassi requisiti di sistema e per avere aggiornamenti automaticamenti ed incrementali, sia per il programma che per le definizioni dei virus.

avast! antivirus garantisce la massima sicurezza contro tutte le forme di malware. Qui di seguito potrete leggere le caratteristiche principali e le differenze tra avast! antivirus Home e Professional Edition.

Caratteristiche principali	Home Edition	Professional Edition
Motore antivirus ad elevate prestazioni	**Sì**	**Sì**
Protezione residente robusta	**Sì**	**Sì**
Anti-spyware integrato	**Sì**	**Sì**
Rilevazione rootkit integrato	**Sì**	**Sì**
Robusta auto-protezione	**Sì**	**Sì**
Aggiornamenti incrementali automatici	**Sì**	**Sì**
Cestino virus Virus per la raccolta dei files sospetti	**Sì**	**Sì**
Integrazione di Sistema	**Sì**	**Sì**
Virus cleaner integrato	**Sì**	**Sì**
Command line scanner	**No**	**Sì**
Bloccaggio Script	**No**	**Sì**
Aggiornamenti “PUSH”	**No**	**Sì**
Interfaccia utente avanzata e possibilità di programmare le operazioni	**No**	**Sì**

Kernel Antivirus

Il kernel antivirus è il nucleo del programma. L'ultima versione del kernel antivirus avast! possiede elevate capacità di rilevamento e prestazioni. Potete aspettarvi il 100% di rilevazione dei virus "in-the-wild" (virus già diffuso tra gli utenti) e dei cavalli di Troia.

Il kernel è certificato da **ICSA Labs**; prende frequentemente parte ai test del Virus Bulletin magazine, e spesso riceve il premio VB100.

Protezione Residente (o protezione "all'avvio")

La protezione residente (protezione in tempo reale del sistema), è una delle caratteristiche più importanti di un programma antivirus moderno. La protezione residente di avast! è una combinazione di varie parti o " moduli residenti", in grado di rilevare un virus prima che possa infettare il vostro computer.

Tecnologia anti-spyware inclusa

avast! antivirus include la tecnologia anti-spyware, certificate da West Coast Labs Checkmark ed offre maggiore protezione ai preziosi vostri dati e programmi.

Tecnologia anti-rootkit inclusa

Anche la tecnologia anti-Rootkit GMER è incorporata nel programma standard. Se un rootkit è scoperto, è inizialmente disabilitato e poi, se può essere rimosso in modo sicuro e senza compromettere le prestazioni del computer, è rimosso. avast! antivirus include una banca dati virus che può essere automaticamente aggiornato per fornire protezione continua contro i rootkit.

Protezione residente robusta

Alcuni virus tentano di disattivare il software antivirus del computer. Per proteggere il computer anche contro questi virus, avast! possiede un'auto-protezione molto robusta. Questa si basa sulla multi-premiata tecnologia avast! e fornisce un ulteriore livello di sicurezza, al fine di garantire la protezione dei vostri dati e programmi.

Aggiornamenti automatici

Gli aggiornamenti automatici rappresentano un altro punto chiave nella protezione anti-virus. Sia la banca dati virus che il programma stesso, possono essere aggiornati automaticamente. Gli aggiornamenti sono incrementali: solo i nuovi dati vengono scaricati, riducendo di gran lunga il tempo di trasferimento. Le dimensioni tipiche di un aggiornamento della banca dati virus sono di alcune decine di KB, mentre gli aggiornamenti del programma sono in genere non più di un centinaio di KB.

Se la connessione a Internet è continua (come nella connessione a banda larga), gli aggiornamenti sono completamente automatici ed eseguiti ad intervalli di tempo definiti. Se ci si collega a Internet solo occasionalmente, avast! controlla la connessione ed effettua l'aggiornamento quando si è online. Questa funzione è ulteriormente descritto a **pagina 43**.

Cestino Virus

Il Cestino Virus può essere considerato come una cartella dell'hard drive, con caratteristiche speciali che lo rendono un luogo isolato e sicuro per archiviare i file potenzialmente dannosi. È possibile lavorare con i file del cestino, ma con alcune restrizioni di sicurezza.

Il cestino virus rappresenta un isolamento completo dal resto del sistema operativo. Attraverso nessun processo (ad esempio un virus), è possibile accedere ai file contenuti all'interno del cestino, quindi non vi è alcun pericolo. Per ulteriori informazioni, vedere **pagina 57**.

Integrazione di sistema

avast! antivirus è completamente integrato nel vostro sistema. L'estensione Explorer consente l'avvio della scansione semplicemente cliccando con il tasto destro del mouse su una cartella o un file e selezionando un opzione dal sottomenu.

E' presente anche una speciale screen-saver, che, quando attivo, esegue la scansione antivirus. avast! antivirus funziona insieme ai vostri screen-saver favoriti, quindi non è necessario modificare le impostazioni personali per utilizzarlo. Per impostare lo screen saver di avast!, vedere **pagina 85**.

Nelle versioni 32-bit Windows NT/2000/XP/Vista, è anche possibile eseguire la scansione, mentre il sistema è in fase di avvio e prima che un virus possa essere attivato. Questa operazione è utile se si sospetta che il computer sia stato già infettato da un virus.

Virus Cleaner avast! integrato

avast! antivirus è progettato per proteggere il computer contro le infezioni virus e malware. La sua funzione principale è la prevenzione di un attacco virus. Include anche uno speciale "virus cleaner" in grado di rimuovere alcuni dei più comuni virus provenienti da computer infetti. Purtroppo, il numero di virus in circolazione è in costante aumento e nel caso in cui il computer venga infettato da un virus che non può essere rimosso dal "virus cleaner", potrebbe essere necessario l'intervento di un esperto.

Per ulteriori informazioni sul"virus cleaner", vedere **www.avast.com**

Command-line scanner (solo professional edition)

Per gli utenti esperti, avast! Professional Edition possiede il command-line scanner. Il programma AshCmd utilizza lo stesso kernel della scansione di avast! ed i risultati sono esattamente gli stessi. La scansione "command-line" viene effettuata utilizzando una serie di parametri ed opzioni, ed è disponibile anche uno speciale modulo STDIN/STDOUT . Questo modulo è destinato ad essere utilizzato in programmi BATCH ed il suo rendimento è uguale a quello dell' Interfaccia Utente Avanzata (compresa il file di resoconto).

Bloccaggio Script (solo professional edition)

Il bloccaggio script è un modulo che protegge il computer contro virus script nascosti all'interno di pagine web. Tali script sono normalmente innocui, come i programmi che li gestiscono e ne impediscono l'accesso ai file. Tuttavia, se il sistema di sicurezza in un browser ha delle falle il vostro computer potrebbe contrarre il virus. avast! controlla quindi gli script potenzialmente pericolosi delle pagine web che si visitano.

Aggiornamenti PUSH (solo professional edition)

Gli aggiornamenti PUSH sono un'altra caratteristica di avast! Professional Edition .
Si tratta di un importante cambiamento nella filosofia degli aggiornamenti. Ogni programma installato, controlla di tanto in tanto la disponibilità di nuove versioni. Gli aggiornamenti PUSH, invece, sono trasmessi dal nostro server, in modo che il computer possa rispondere rapidamente ed accettare gli aggiornamenti necessari. Il sistema si basa sul protocollo SMTP (come quello usato per le e-mail). L'aggiornamento è controllato dal "resident client" di posta elettronica avast! (*MS Outlook* and *Internet Mail*). L'intero sistema è protetto da algoritmi asimmetrici e protegge da un eventuale utilizzo non autorizzato.

Interfaccia utente avanzata (solo professional edition)

avast! Professional Edition include un' interfaccia utente avanzata dove è possibile gestire delle mansioni speciali, che possono essere programmate per in un determinato periodo di tempo, o ad intervalli regolari, ad esempio, giornalieri, settimanali o mensili. Ogni volta che una mansione viene eseguita, si crea nuova "sessione" nella quale vengono memorizzati e visualizzati i risultati della scansione. A differenza dell' interfaccia utente semplice, quando si lavora sull'interfaccia utente avanzata, è possibile determionare in anticipo azioni da svolgere in presenza dio un virus. Ad esempio è possibile programmare avast! per riparare eventuali file infetti. E 'anche possibile programmare un' azione alternativa, se la prima dovesse fallire. Ad esempio, se un file non può essere riparato, può essere automaticamente trasferito al cestino virus.

Requisiti di sistema

La configurazione hardware descritta qui di seguito rappresenta le caratteristiche **minime** consigliate per il sistema operativo.

Per un computer con Windows® 95/98/Me:
486 Processor, 32MB RAM e 100MB di spazio libero nell' hard disk.

Per un computer con Windows® NT® 4.0:
486 Processor, 24MB RAM, 100MB di spazio libero nell' hard disk e Service Pack 3 (o superiore) installato.

Per un computer con Windows® 2000/XP® Workstation (Non Server):
Processore Pentium class , 64MB RAM (consigliato 128MB) e 100MB di spazio libero nell' hard disk.

Per un computer con Windows® XP® edizione 64-bit:
AMD Athlon64, Opteron o Intel EM64T Pentium 4 / processore Xeon , 128MB RAM (consigliato 256MB) e 100MB di spazio libero nell' hard disk.

Per un computer con Windows® Vista:
processore Pentium 4 , 512MB RAM e 100MB di spazio libero nell' hard disk.

Il programma richiede circa 60MB di spazio nell' hard disk; il resto dello spazio è riservato alla banca dati virus ed il suo indice (VRDB, conosciuto anche come "integrity database" della versione precedente).

MS Internet Explorer 4 funzionale o superiore è necessario affinchè il programma possa funzionare.

Questo prodotto **non può essere installato sul server** (Windows Server NT/2000/2003).

Nota: possono sorgere dei problemi se si installano diversi prodotti antivirus contemporaneamente sullo stesso computer. Se è presente un altro software antivirus, si consiglia di disinstallarlo, prima di installare avast!

Come installare l'antivirus avast! Home Edition

In questa sezione viene descritto come scaricare ed installare avast! Home Edition sul vostro computer e come introdurre il codice di licenza del software una volta che il download e l'installazione sono state completate... Le schermate mostrate nelle pagine seguenti, sono come così come appaiono in Windows XP e possono variare leggermente in altre versioni di Windows.

E' possible scaricare avast! Home da **www.avast.com**.

Si consiglia di chiudere tutti gli altri programmi di Windows prima di iniziare il download.

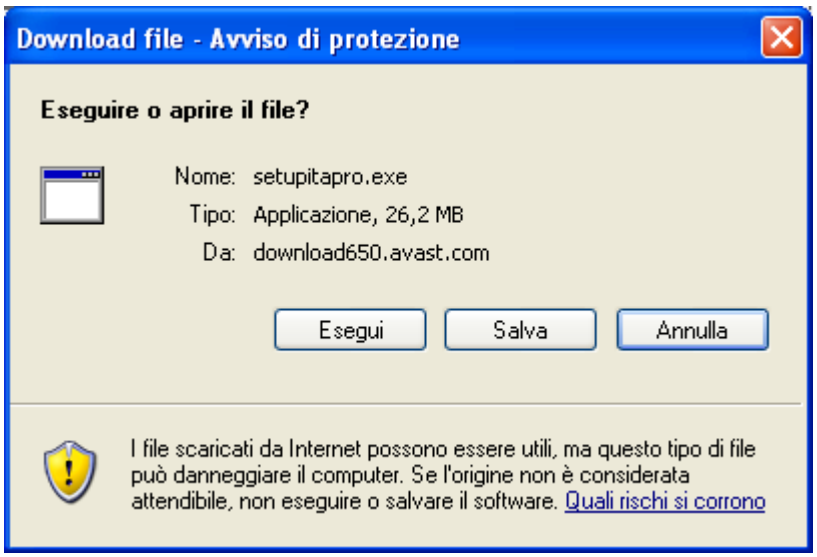
Cliccate su "Download" e poi "Download programmi" e quindi selezionate la versione da scaricare.

Dalla lista di lingue disponibili, selezionate la versione che desiderate – vedere qui sotto - e cliccare pulsante "Download".

Download di avast! 4 Home Edition

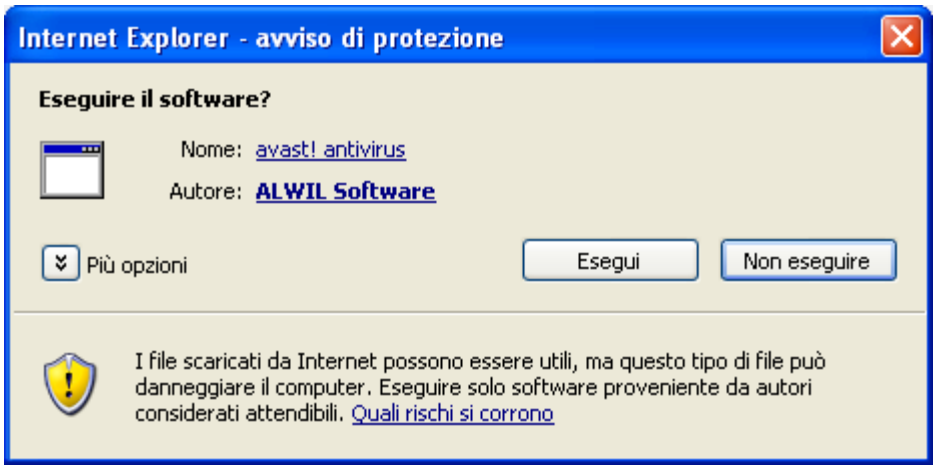
Download avast! 4 Home – versione **Inglese** (18.25 MB)
Download avast! 4 Home - versione **Araba** (18.05 MB)
Download avast! 4 Home - versione **Bulgara** (18.09 MB)
Download avast! 4 Home - versione **Catalana** (18.34 MB)

Se utilizzate Internet Explorer come web browser, visualizzerete la seguente schermata:



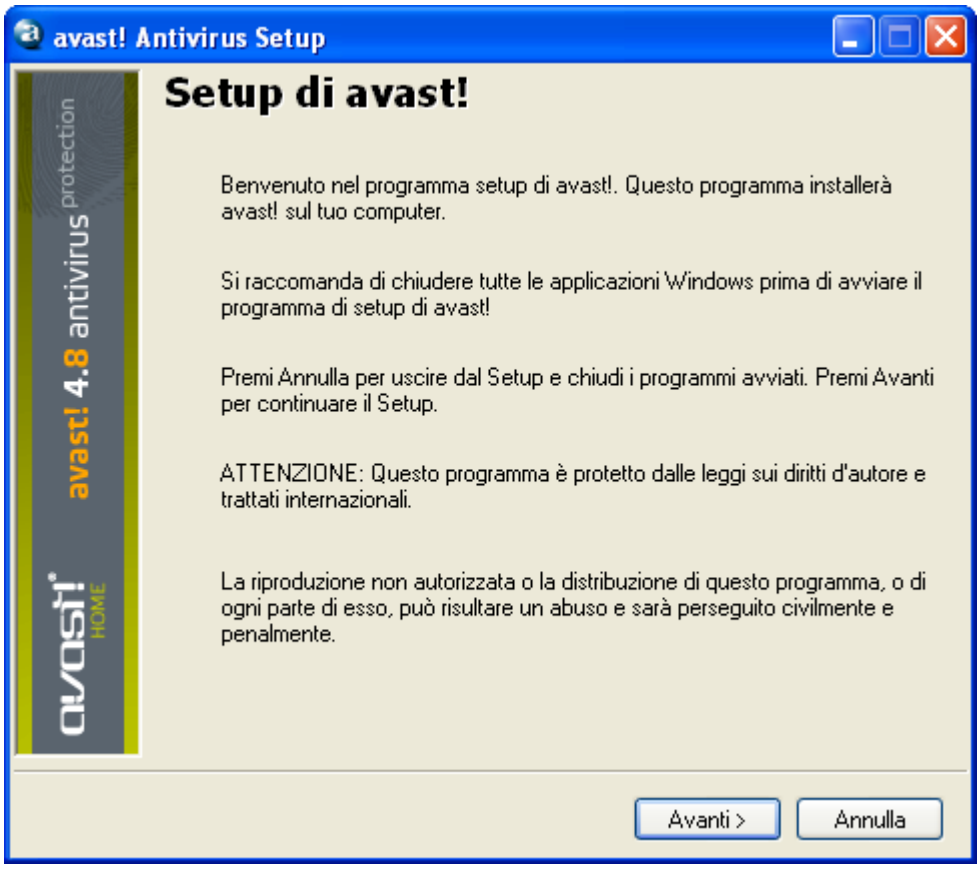
Cliccando su "Esegui" o "Salva" inizierà il download e l'installazione del file "Setupeng.exe" sul vostro computer.

Se si desidera installare avast! antivirus immediatamente, dopo il download del file, basta cliccare su "Esegui". La schermata è la seguente:



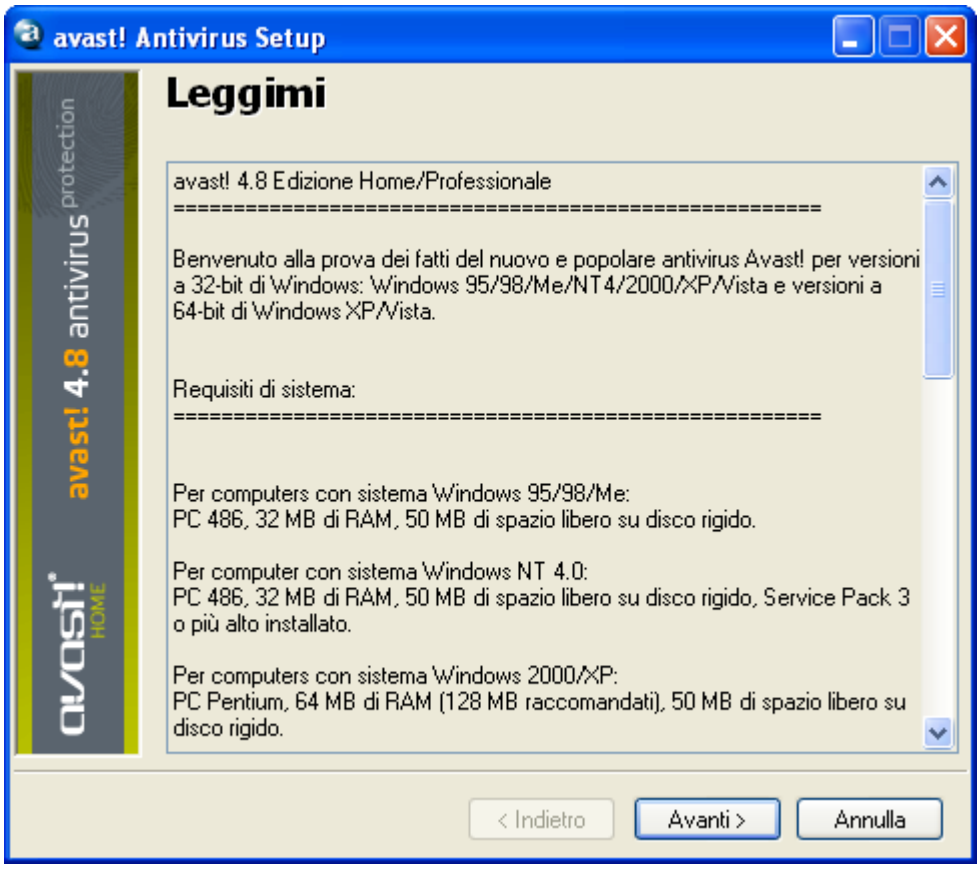
In altri browser web, si può avere solo l'opzione "Salva" il file. Facendo clic su "Salva" verrà scaricato il software per il computer ma non sarà installato in questo momento. Per completare il processo di installazione sarà necessario eseguire il "Setupeng.exe" file di installazione in modo ricordare dove è stato salvato! Fare doppio clic sul file per eseguirlo.

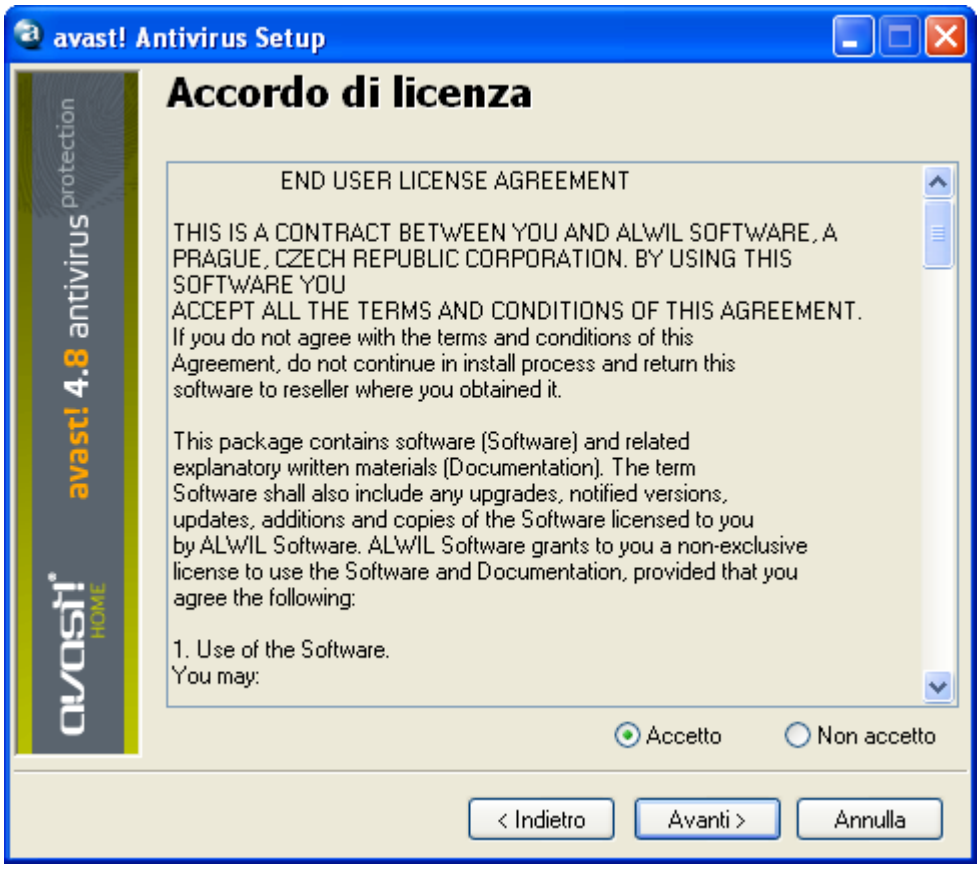
Cliccando su “Esegui” visualizzarete la schermata del Setup di avast!:



Clicando su “Avanti” sarete guidati nel processo di installazione.

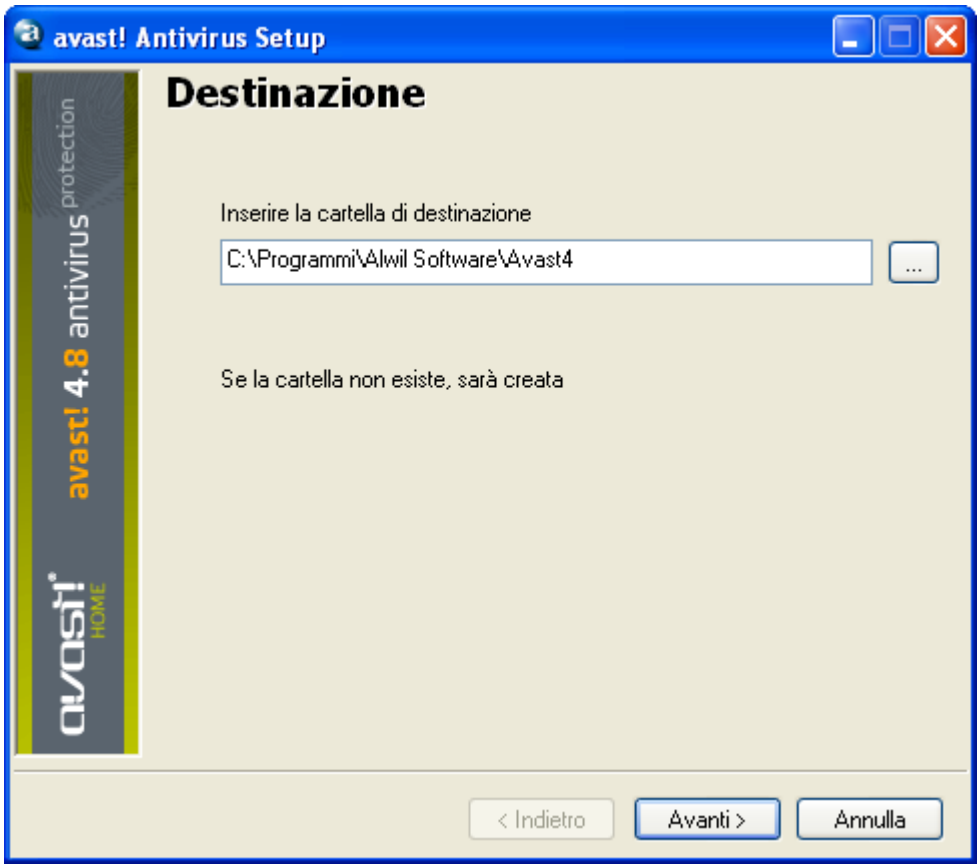
In primo luogo verrà chiesto di leggere i requisiti minimi di sistema e quindi di confermare che l'utente accetta le condizioni di licenza – come nelle schermate di seguito.


avast! Antivirus Setup
Leggimi
avast! 4.8 antivirus protection
avast! 4.8 Edizione Home/Professionale
==========
Benvenuto alla prova dei fatti del nuovo e popolare antivirus Avast! per versioni a 32-bit di Windows: Windows 95/98/Me/NT4/2000/XP/Vista e versioni a 64-bit di Windows XP/Vista.
Requisiti di sistema:
==========
Per computers con sistema Windows 95/98/Me:
PC 486, 32 MB di RAM, 50 MB di spazio libero su disco rigido.
Per computer con sistema Windows NT 4.0:
PC 486, 32 MB di RAM, 50 MB di spazio libero su disco rigido, Service Pack 3 o più alto installato.
Per computers con sistema Windows 2000/XP:
PC Pentium, 64 MB di RAM (128 MB raccomandati), 50 MB di spazio libero su disco rigido.
< Indietro
Avanti >
Annulla



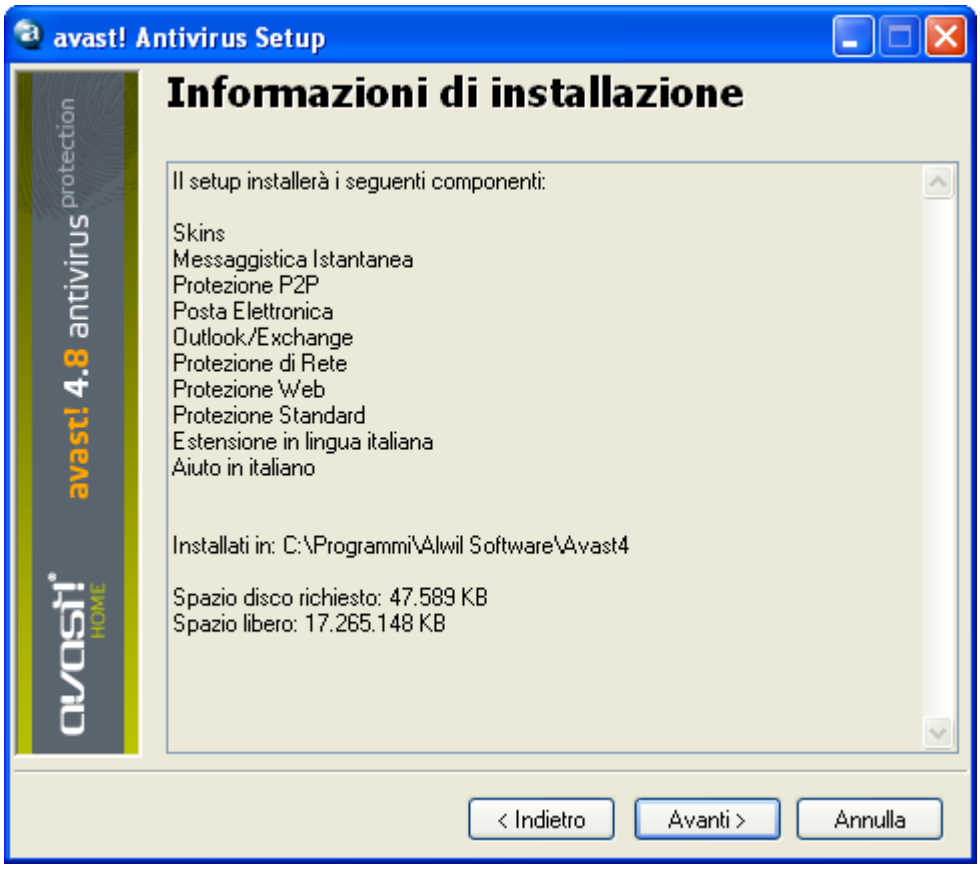
Per continuare, dovete cliccare su “Accetto” e poi “Avanti”.

Vi verrà chiesto di confermare la cartella di destinazione, ovvero dove il file di programma verrà salvato. Il programma selezionerà la cartella automaticamente, o ne creerà una nuova se ancora non esiste. Si consiglia di accettare la cartella di destinazione preimpostata. Per continuare cliccare su "Avanti".



Nella schermata successiva, vi verrà chiesto di confermare la configurazione. Le opzioni adatte alla maggior parte degli utenti vengono selezionate automaticamente. A meno che non si desideri modificare le impostazioni predefinite, ad esempio, la selezione della lingua, basta cliccare su "Avanti" e continuare.

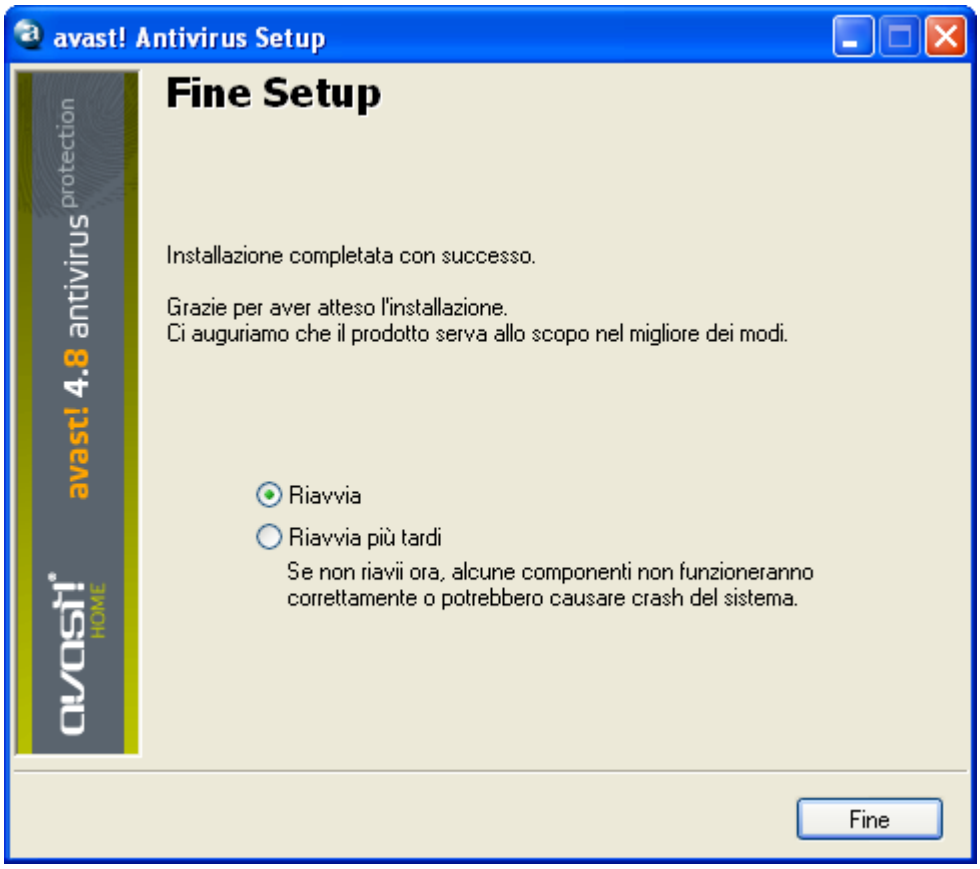
Il programma confermerà ciò che sta per essere installato e dove, e lo spazio che sarà occupato sul disco. Cliccare su "Avanti" per continuare.



Vi sarà chiesto se desiderate effettuare un controllo antivirus degli hard disk al riavvio del sistema – vedere **pagina 44**.

L'ultima schermata dovrebbe confermare che l'installazione è stata completata con successo, tuttavia, per completare il processo sarà necessario riavviare il computer.

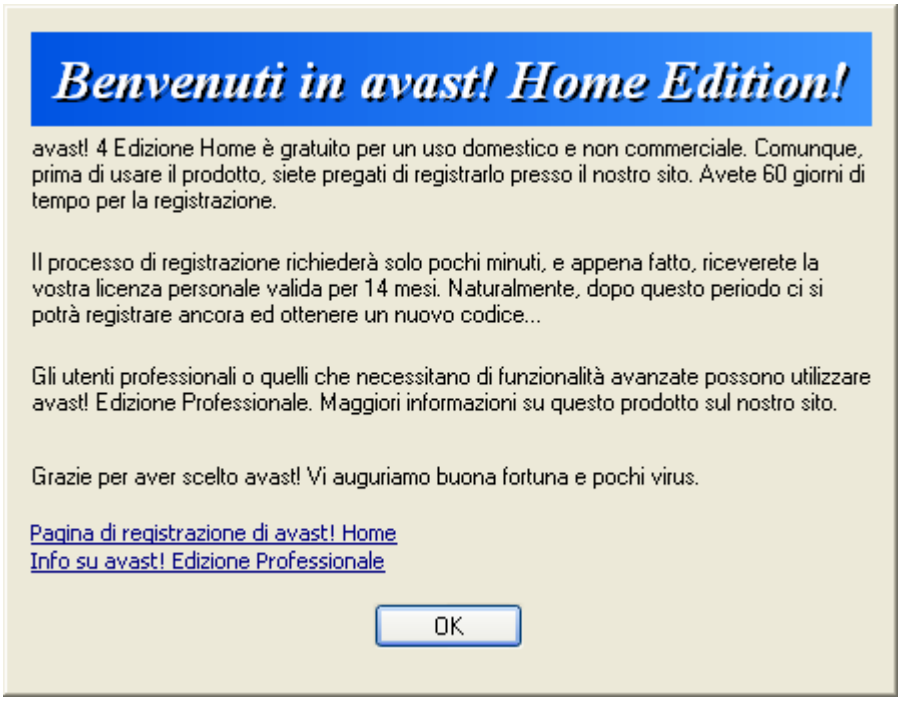
Con "Riavvia", e poi "Fine" il computer viene automaticamente riavviato.



L' installazione è ora completa.

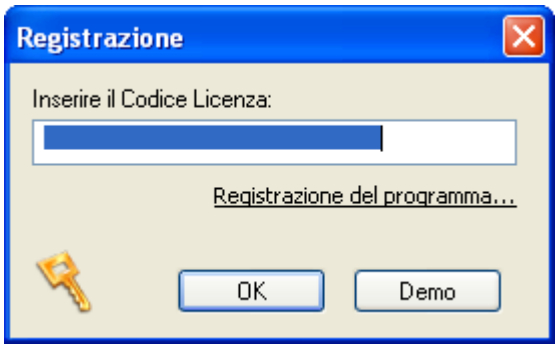
Come iniziare

Dopo l'avvio del computer, sullo schermo,appare la seguente schermata, in basso a destra, si dovrebbe vedere l'icona blu di avast!



avast! antivirus Home Edition è un programma gratuito per uso domestico e non-commerciale. Se si desidera utilizzarlo dopo i 60 giorni il periodo di prova, sarà necessario registrarsi per ricevere una chiave di licenza (gratuita), da inserire nel programma .

Pertanto, la prima volta che si esegue il programma, verrà visualizzata la schermata:



Non è necessario inserire una chiave di licenza subito. Se si desidera utilizzare il programma per 60 giorni, senza l'introduzione di una chiave di licenza, è sufficiente cliccare su "Demo". Tuttavia, è possibile richiedere una chiave di licenza cliccando su "acquista ora" e seguendo la procedura descritta nella sezione successiva.

Una volta che avete selezionato la versione demo, questa casella non verrà più visualizzata all'utilizzo del programma. E' possibile richiedere una chiave di licenza in qualsiasi momento – vedere la pagina seguente: "Come fare per registrare una

chiave di licenza"

Dopo 60 giorni, se non inserite una chiave di licenza apparirà nell'angolo in basso a destra dello schermo del computer il seguente avviso:

Informazioni avast! Il periodo di prova del programma è terminato. avast! non è più in grado di proteggervi. Per ulteriori informazioni cliccare qui....

Il seguente messaggio apparirà ad ogni avvio del programma:

avast!: Licenza scaduta. Inserire una nuova chiave di licenza.

Cliccando su “OK” apparirà di nuovo la finestra di registrazione:

Protezione Password

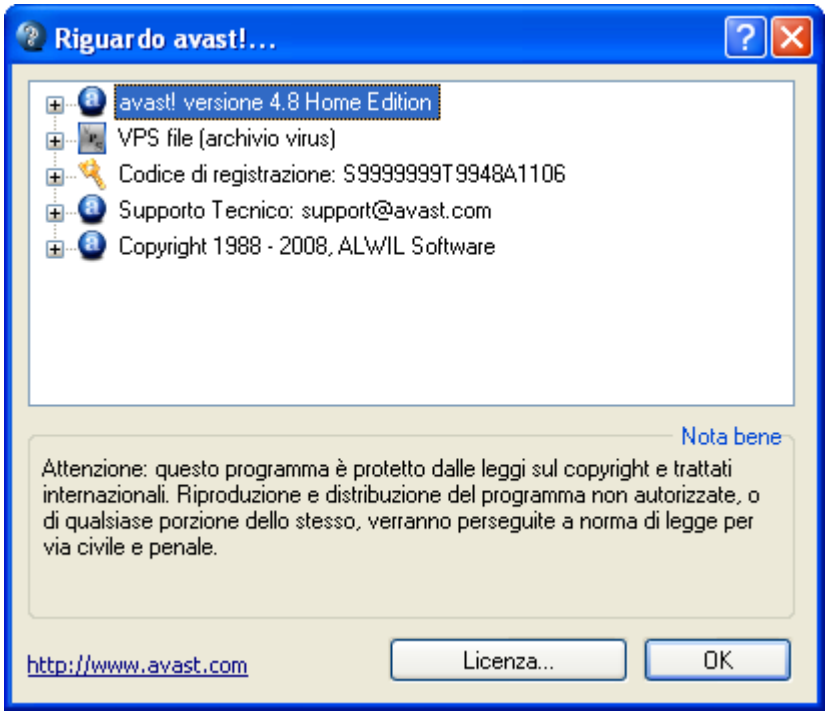
Cliccando con il tasto destro del mouse sull’icona blu di avast! in basso a destra dello schermo e selezionando "Imposta/Cambia password" è possibile creare una password per proteggere il vostro programma antivirus da eventuali modifiche non autorizzate.

Come registrare la chiave di licenza

Entro 60 giorni gli utenti di avast! Home Edition dovranno registrarsi ed inserire una chiave di licenza valida nel programma.

Per ricevere una chiave di licenza, basta andare su **www.avast.com** selezionare la lingua Italiana e cliccare su "Supporto" nella parte superiore dello schermo. Poi clicca su "Registrazione GRATUITA avast! Home". In alternativa, se avete già scaricato e installato il programma, cliccate con il tasto destro del mouse sull'icona blu di avast! in basso a destra dello schermo. Dal menu che appare, selezionare "Riguardo avast! ... "

Cliccare su " licenza" e apparirà la casella di registrazione:



Apparirà la schermata per la registrazione. Cliccare su "registrazione del programma".

Nella pagina successiva, potete completare l'iscrizione on-line. Quindi, cliccare su "Registra". Una chiave di licenza verrà inviata al vostro indirizzo e-mail entro 24 ore.

Inserimento chiave di licenza

Il codice di licenza, (ricevuto via e-mail all'indirizzo indicato durante il processo di acquisto), deve essere inserito nel programma. Ciò consentirà al programma di essere aggiornato automaticamente.

Nota – il programma avast! deve essere scaricato e installato prima di inserire la chiave di licenza.

Per vedere il video informativo che mostra come inserire il codice di licenza senza avviare il programma, cliccate **qui** o visitate **www.avast.com** e cliccate su "Supporto" nella parte superiore dello schermo. Dal menu di seguito, cliccare su "Supporto Tecnico". Poi cercare la voce "Istruzioni video" nell'angolo in basso a sinistra dello schermo e cliccare su "Come inserire la chiave di attivazione".

In alternativa, potete seguire le seguenti istruzioni:

1) Copiate il numero di licenza ricevuto via e-mail.

2) Sulla barra delle applicazioni, in basso a destra, vicino all' orologio, è presente l' icona avast! (una piccola sfera blu) con una "a" nel centro.

3) Cliccate con il tasto destro del mouse sull' icona, e dal MENU selezionare "Riguardo avast!"

4) Premete il tasto "Licenza"

5) Inserite la chiave di licenza nell' apposito spazio (è consigliato copiare ed incollare il codice).

6) Premete OK. Il programma può ora continuare ad essere utilizzato per 12 mesi alla fine dei 60 giorni di prova. Alla fine di quel tempo, sarà necessario semplicemente effettuare la registrazione ed inserire una nuova chiave di licenza.

Utilizzo dell' antivirus avast!

avast! antivirus fornisce protezione contro tutti i tipi di malware e contiene una robusta potente "protezione residente", anche denominata protezione “all’avvio” perchè la scansione dei file avviene al momento in cui vi si accede.

Normalmente, la protezione residente assicura che il computer non venga infettato da un virus. Una volta scaricato il programma, la protezione residente funziona di continuo in sottofondo, e monitora tutte le attività del computer. Tuttavia, se la protezione residente è disattivata per qualsiasi motivo, o se è rimasta inattiva per un certo periodo di tempo, è possibile eseguire una scansione manuale (nota come scansione "su richiesta") di tutti i file sul computer.

avast! antivirus include anche uno speciale screen saver che controlla costantemente il computer acceso ma non in uso.

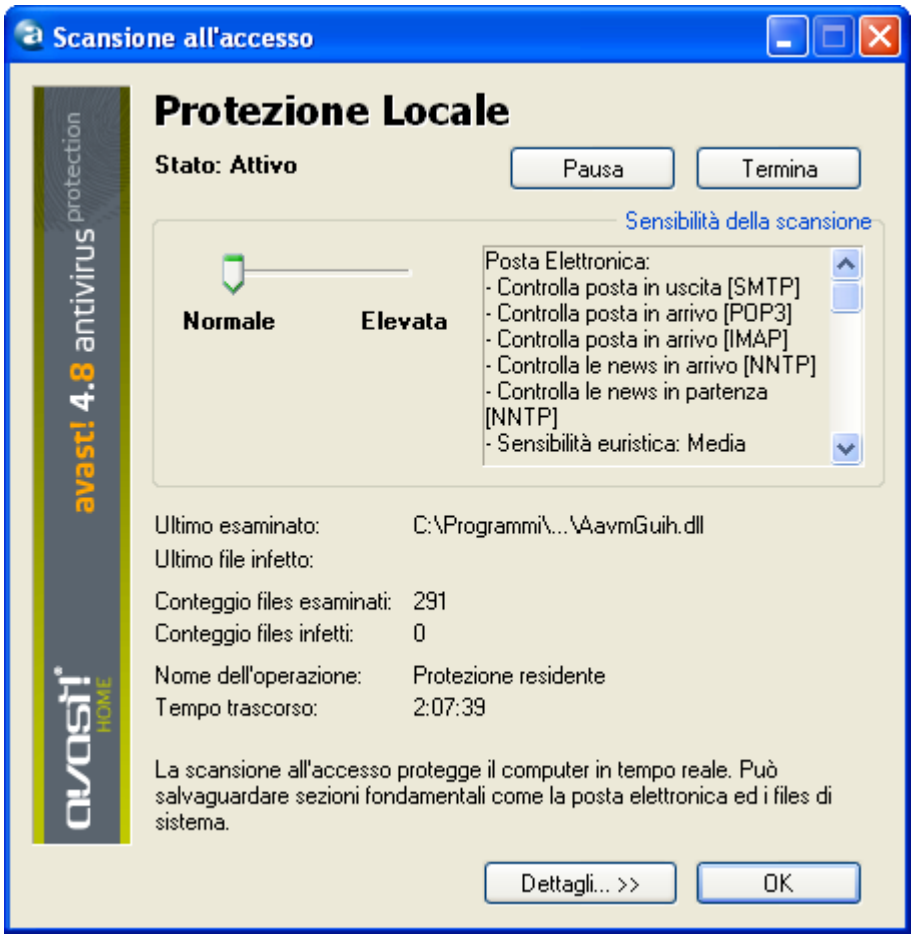
Protezione Locale “all’avvio”

Questa parte del programma controlla continuamente l'intero computer e tutti i programmi in esecuzione, per rilevare eventuali attività sospette (ad esempio un virus), in modo da prevenire eventuali danni ai file del vostro computer. E’ completamente indipendente (si attiva automaticamente quando si avvia il computer) e se tutto è OK, non vi accorgerete neanche che è in esecuzione.

L' icona blu sullo schermo del computer in basso a destra, accanto a l'orologio, mostra lo stato attuale della protezione locale. Normalmente la presenza dell’icona indica che la protezione locale è installata e protegge il computer. Se l' icona presenta un cerchietto rosso, la protezione è al momento inattiva e il computer non è protetto. Se è di colore grigio, significa che la protezione è in pausa - vedere pagina successiva.

Le impostazioni della protezione locale sono accessibili cliccando sull’icona di avast! con il tasto destro del mouse e selezionando "controllo di protezione all’ avvio".

Visualizzate la seguente schermata:



Sulla schermata è possibile sospendere temporaneamente la protezione locale cliccando su "Pausa", o "Termina". In questo caso, entrambe le opzioni hanno lo stesso effetto. Tuttavia, la protezione locale verrà automaticamente riattivata la prossima volta il computer viene riavviato. Questo è un sistema di sicurezza per garantire che il computer non sia accidentalmente lasciato senza protezione.

È inoltre possibile regolare la sensibilità della protezione locale, cliccando e muovendo cursore su "Normale" o "Elevata". La protezione locale comprende diversi moduli o "providers", ognuno dei quali progettato per proteggere una sezione diversa del computer – vedere pagina successiva. Tutte le modifiche apportate su questa schermata si riflettono su tutti i moduli di protezione locale.

La protezione locale comprende I seguenti moduli o "providers":

Messaggistica istantanea

controlla i file scaricati da messaggi istantanei o programmi di "chat" come ICQ, MSN Messenger e molti altri. Mentre i messaggi istantanei non comportano gravi rischi per la sicurezza a causa dei virus, le applicazioni di messaggistica istantanea moderne non sono solo strumenti per la chat: la maggior parte di essi consentono la condivisione di file - che può facilmente portare a infezioni virus, se non controllate adeguatamente.

Posta elettronica

controlla in entrata e in uscita i messaggi e-mail provenienti da clienti diversi da quelli di MS Outlook e MS Exchange, come ad esempio Outlook Express, Eudora ecc.

Protezione di Rete

fornisce protezione da worms di Internet, come Blaster, Sasser ecc. Questa funzione è disponibile solo su sistemi NT (Windows NT/2000/XP/Vista).

Outlook/Exchange

controlla in entrata e in uscita i messaggi e-mail provenienti da MS Outlook o MS Exchange e impedisce la che i messaggi contenenti un potenziale virus vengano accettati o inviati.

Protezione P2P

controlla i file scaricati dai comuni programmi P2P (file sharing) come Kazaa ecc.

Bloccaggio Script (solo avast! professional)

controlla gli script, qualsiasi pagina web si visiti, per evitare infezioni a causate dalla vulnerabilità nel vostro browser

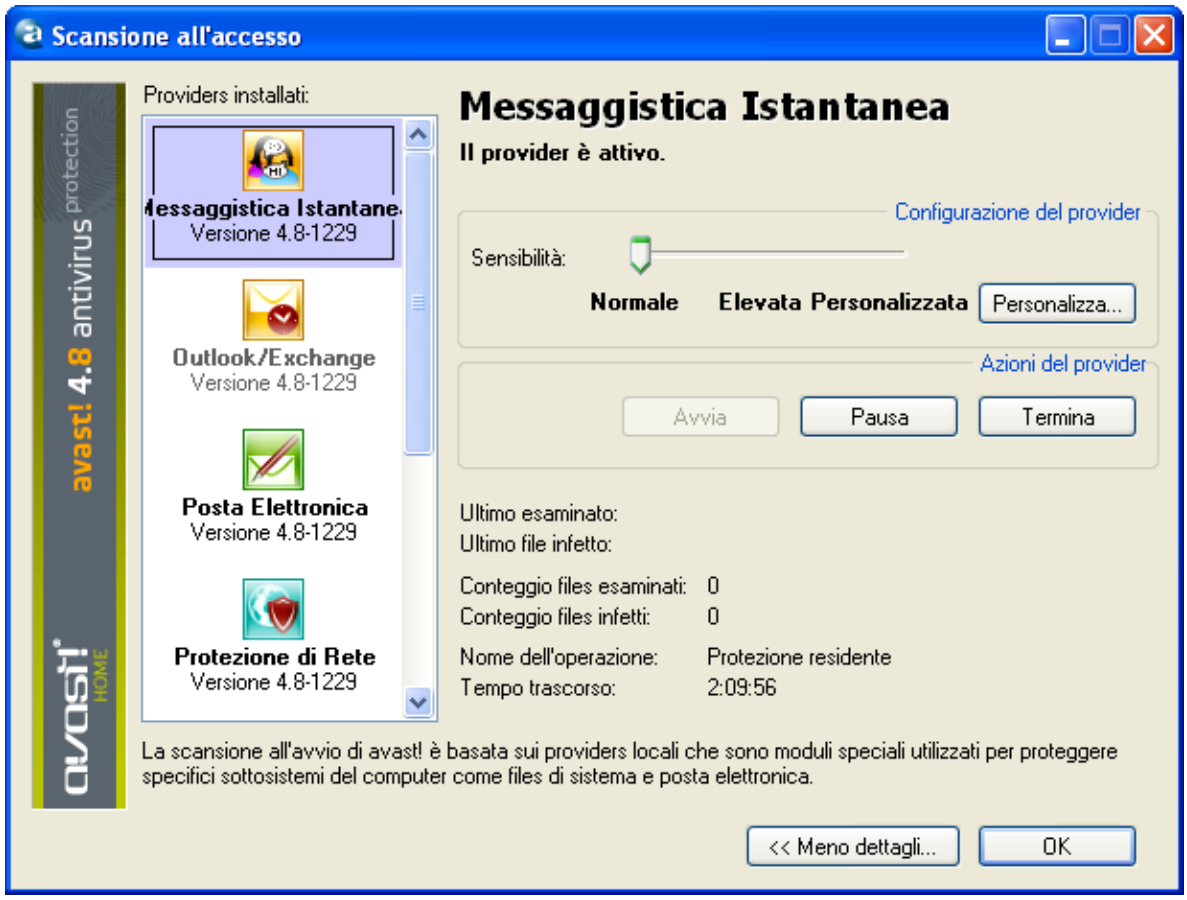
Protezione Standard

controlla i programmi in esecuzione ed documenti che vengono aperti. Funziona per evitare di eseguire un programma che include un virus o aprire un documento infetto, che potrebbero causare dei danni.

Protezione Web

protegge il computer dai virus durante l'utilizzo di Internet (navigazione, download dei file, ecc.) e può anche bloccare l'accesso a determinate pagine web. Se si scarica un file infetto, la protezione Standard impedisce che venga avviato e che causi dei danni. Tuttavia, la protezione Web rileverà il virus ancora prima che questo avvenga - durante il download del file, garantendo così una maggiore protezione. La protezione Web è compatibile con tutti i principali browser Web, tra i quali Microsoft Internet Explorer, Firefox, Mozilla e Opera. Grazie alla tecnologia chiamata "Intelligent Stream Scanning", il file è scaricato e sottoposto a scansione quasi in tempo reale, e l' impatto sulla velocità di navigazione è trascurabile.

E 'possibile regolare la sensibilità di ogni modulo separatamente. Per impostare la sensibilità individuale per ciascun modulo, o per mettere in pausa o interrompere un modulo specifico, basta cliccare su "Dettagli ...". Si visualizzerà quanto segue:



Come potete vedere qui sopra, i singoli moduli sono riportati sul pannello di sinistra. La sensibilità di ogni modulo può essere impostata cliccando sul relativo modulo sul lato sinistro, e muovendo il cursore. In questo riquadro è anche possibile sospendere le singole parti della protezione residente,

temporaneamente o definitivamente: basta cliccare su "Pausa" o "Termina". Se si clicca su "Pausa", il relativo modulo sarà automaticamente riattivato la prossima volta che si riavvia il computer. Se si seleziona "Termina", il programma vi chiederà se desiderate che modulo in questione si disattivi a tempo indeterminato, o se deve essere riattivato con il prossimo riavvio del computer - vedere page 89. Se si clicca su "Sì", quel particolare modulo verrà disattivato, anche dopo il riavvio del computer, fino a quando non si decida di riattivarlo manualmente.

Ci sono una serie di opzioni aggiuntive che possono essere selezionate per ogni modulo; per esempio, è possibile specificare i tipi di file da controllare. Queste opzioni sono accessibili cliccando su "Personalizza" e sono descritte a **pagina 62**- impostazioni protezione locale.

Come effettuare manualmente una scansione – Interfaccia semplice

La prima volta che si avvia il programma, si visualizza una console color grigio/argento simile a un CD player, che contiene tutti i controlli per la definizione, l'esecuzione e la trasformazione dei risultati di una scansione anti-virus - vedi sotto. Questo è l'aspetto preimpostato o la "skin" del programma (l'aspetto può essere cambiato selezionando altre "skin" - vedi **pagina 35**).

Inizialmente, il player appare dietro una scatola contenente il "5 punti chiave per iniziare".Cliccate su "Maggiori informazioni" per saperne di più, quindi "Home page per tornare alla schermata principale. Le informazioni importanti, sono sintetizzata nelle pagine successive. E' possibile tornare di nuovo a questi punti chiave in qualsiasi momento accedendo al **menu delle opzioni** (vedi pagina successiva) e selezionando "Guida introduttiva".

Al centro della console sono mostrate le seguenti informazioni:

- ***Attuale versione archivio virus*** – la banca dati virus (archivio) contiene i dettagli di tutti i virus attualmente conosciuti ed è utilizzato dal programma per individuare eventuali file sospetti.
- ***Protezione locale*** – qui potete vedere l'attuale livello di sensibilità.

- ***Data ultima scansioneDate of last scan*** – indica la data dell'ultima scansione manuale.

- ***Archivio recupero virus*** – contiene i dettagli dei file installati sul computer e viene utilizzato per la riparazione nel caso in cui siano danneggiati da un virus. La data indica data quando l'archivio recupero virus è stato aggiornato.

- ***Aggiornamenti automatici*** – mostra lo stato dell'aggiornamento dell'archivio virus e del programma stesso - per modificare lo stato dell' aggiornamento, cliccare sul lato destro della finestra - vedere **pagina 43**.

Su entrambi i lati della console sono presenti tre pulsanti:

- **In alto a sinistra** - il pulsante apre il **Cestino Virus**. Per ulteriori informazioni su come operare con i files del cestino virus, vedere **pagina 57**.

- **Al centro a sinistra** – cliccando su questo pulsante si visualizza una barra con un cursore che può essere utilizzato per modificare la sensibilità della protezione locale. Cliccando sul cursore e spostandolo verso sinistra o verso destra, si diminuisce o aumenta la sensibilità. Nota – modificando qui il livello di sensibilità,si influenzeranno tutti i moduli di protezione locale. Per regolare i moduli singolarmente, vedere **pagina 26**

- **In basso a sinistra** –

cliccando su questo pulsante o cliccando sulla situazione attuale nella finestra, si aggiorna l'archivio virus.

L'archivio Virus può essere aggiornato anche cliccando con il tasto destroy del mouse sull'icona blu di avast! sulla barra delle applicazioni, e selezionando GENERA VRDB adesso.

I tre pulsanti a destra sono utilizzati per definire le aree da sottoporre a scansione - hard disk locali, supporti rimovibili (floppy disk, CD, ecc..) e le cartelle selezionate – vedere pagina successiva.

- pulsante **AVVIO** – cliccate su questo pulsante per iniziare o riprendere la scansione delle aree selezionat. Dopo, questo pulsante diventa **PAUSA**.

- pulsante **PAUSA** – cliccate su questo pulsante per arrestare la scansione.

- Pulsante **STOP** – cliccate su questo pulsante per terminare la scansione

  Menu – cliccate sulla freccetta in alto a sinistra per visualizzare **MENU delle OPZIONI**. Le opzioni del menu sono accessibili anche cliccando con il tasto destro del mouse con il cursore posizionato ovunque sulla console.

  Quando si usa il programma senza una "skin" (vedere **pagina 35**), le opzioni del menu sono accessibili cliccando su "Strumenti" o "Impostazioni" nella parte superiore dello schermo.

  si può accedere ad alcune opzioni del menu senza avviare il programma, ma cliccandocon il tasto destro delmouse sull'icona blu di avast! in basso a destra dello schermo del computer.

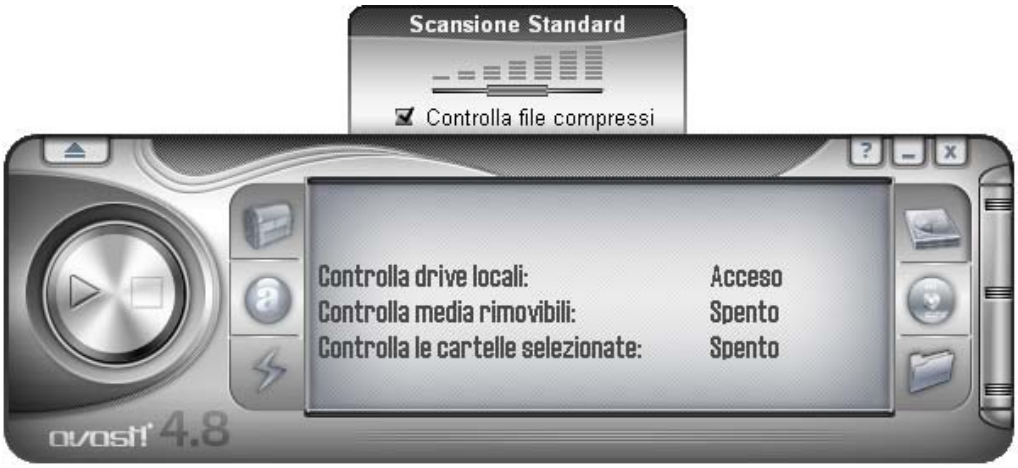
  Tutte le opzioni del menu sono descritte approfonditamente nel presente manuale d'uso.

Selezionare le aree per la scansione manuale

Prima di avviare la scansione, dovete scegliere i file che si desidera controllare.

- ***Controlla i drive locali***

Se si desidera effettuare la scansione di tutto il computer (tutti i file su tutti gli hard disk), basta cliccare sul pulsante in alto a destra. La schermata con le Informazioni sullo stato attuale è ora sostituita da una nuova figura - vedere sotto. Per tornare indietro, cliccate con il tasto destro del mouse sulla console e selezionate "Informazioni di stato".



Sulla console, verrà visualizzata la scritta "Controlla drive locali" e lo stato è cambiato da "Spento" ad "Acceso".

Potrete vedere un'altra finestra sulla console. Questa finestra può essere usata per impostare la sensibilità della scansione. Cliccando sul dispositivo di scorrimento e tenendo premuto il tasto del mouse, è possibile spostare il cursore verso sinistra per ridurre la sensibilità, o verso destra, per aumenterla. Nella finestra, è anche possibile decidere se controllare o meno i files compressi. Queste opzioni sono descritte approfonditamente nella sezione successiva.

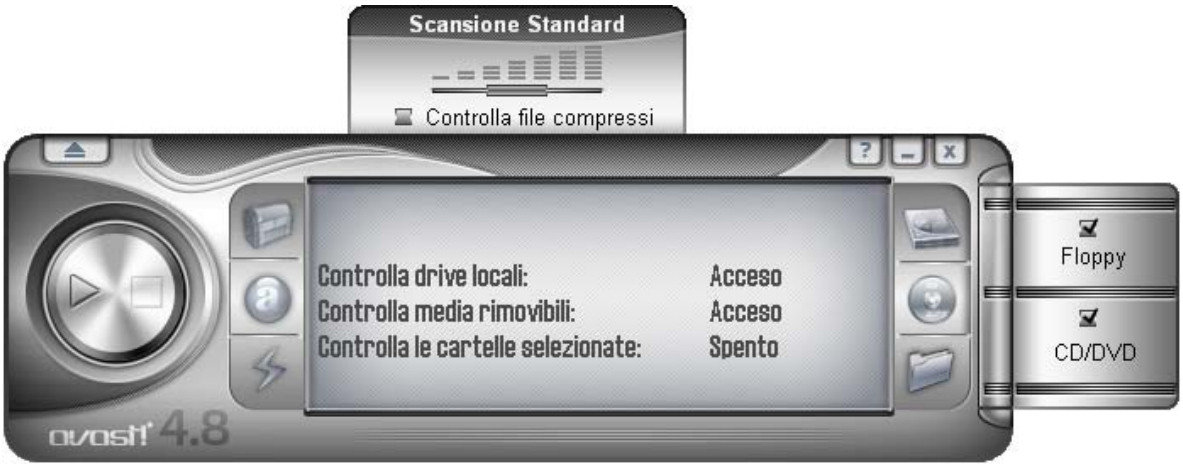
- ***Controlla media rimovibili***

Se si desidera eseguire la scansione del contenuto delle periferiche rimovibili, ad esempio, floppy disk o CD / DVD, cliccare sul pulsante al centro verso destra.

Facendo clic su questo pulsante cambierà lo stato di "Controlla media rimovibili" da "Spento" ad "Acceso".

Due finestrelle appariranno sulla destra della console per scegliere quale tipo di periferica rimovibile deve essere controllata (altri media magnetici e ottico-magnetici, come i dischi ZIP, sono considerati dischetti).

Anche in questo caso la finestra che appare sopra può essere usata per impostare la sensibilità della scansione e per decidere se controllare o meno i files compressi.



- ***Controlla le cartelle selezionate***

L'ultima opzione è il pulsante in basso a destra. Si clicca su questo pulsante se si desidera scegliere di controllare solo alcune cartelle. Apparirà un elenco di tutte le cartelle sul vostro computer e sarà possibile scegliere quelle da controllare. Questa impostazione,offre maggiore flessibilità, ma richiede all'utente di impostare esattamente ciò che deve essere sottoposto a scansione.

Anche in questo caso la finestra che appare sopra può essere usata per impostare la sensibilità della scansione e per decidere se controllare o meno i files compressi.

E 'possibile combinare più di un tipo di scansione, ad esempio, cliccando su entrambi i pulsanti relativi ai drive locali e ai media rimovibili.

Impostare la sensibilità della scansione ed iniziare il controllo

Nel definire l'area da sottoporre al controllo, è possibile impostare la sensibilità della scansione e se eseguire la scansione del contenuto del file compressi, ovvero i file con estensione. zip,.rar, ace,.acj ecc.. Per includere questi file, è necessario innanzitutto scegliere le zone che si desidera controllare (vedere sopra), e quindi selezionare la casella nella sezione "controlla file compressi". La sensibilità della scansione determina quanto approfondita sarà la scansione. La sensibilità è impostata spostando il cursore verso sinistra o verso destra. È possibile scegliere tre livelli di sensibilità.

- **Scansione Rapida**. Questa scansione, come indica il nome, è abbastanza veloce, in quanto i file sono esaminati in base ai loro nomi, e solo quelli considerati potenzialmente pericolosi, sono controllati. Questo tipo di scansione può talvolta portare a tralasciare alcuni file che contengono virus, però di solito non succede.

- **Scansione Standard**. In questo tipo di scansione, i file vengono analizzati in base al loro contenuto (non i loro nomi, come avviene nella scansione rapida). Tuttavia, solo le parti "pericolose" del file sono controllate, non l'intero file. Anche questo tipo di scansione (pur essendo più efficiente di quella rapida) può talvolta portare a tralasciare alcuni file che contengono virus.

- **Scansione Approfondita**. In questo tipo di scansione i file sono controllati completamente, secondo le infezioni elencate nella banca dati. Questo tipo di scansione è quella con la più alta affidabilità, ma richiede molto più tempo rispetto a quella rapida o standard.

Dopo aver selezionato le opzioni di scansione, tutto ciò che dovete fare è avviare il controllo. Per effettuare questa operazione, cliccate sul pulsante Play (freccia rivolta verso destra) sul lato sinistro della console.

Metodo alternativo

È inoltre possibile definire l'area da sottoporre a scansione, aprendo il **menu delle opzioni** e cliccando sul pulsante "Inizio scansione" e poi "Selezionare l'area da controllare". Dopo aver selezionato l'area da sottoporre al controllo, è possibile specificare se controllare i files compressi o meno.

Cliccando su "Seleziona il livello di controllo" è possibile inoltre determinare se la scansione deve essere rapida, standard o approfondita, come descritto sopra.

Eseguire la scansione ed elaborare i risultati

Dopo aver cliccato sul pulsante Play, o selezionando "Inizio scansione" nel **menu delle opzioni** il programma inizia a controllare le aree selezionate. Questo processo può richiedere molto tempo, a seconda del numero e le dimensioni dei file e alla velocità del vostro computer. Ricordate che, sebbene l'opzione di scansione approfondita richieda molto tempo, è sempre la più efficace.

Una volta avviato il programma, si può lavorare sul vostro computer con altri file o programmi, anche se la scansione è in corso. Per effettuare questa operazione, si raccomanda di ridurre a icona avast! in modo che sia in esecuzione in sottofondo. In caso contrario, è possibile che il computer diventi molto lento (la scansione di virus è piuttosto impegnativa). Per mettere la scansione sottofondo, è sufficiente fare clic sul pulsante minimizza (_) nell'angolo in alto a destra della console, mentre la scansione è in esecuzione. In questo modo scompare dallo schermo. Per riportarlo sullo schermo, è sufficiente cliccare sulla casella "avast!" che si trova nella barra orizzontale in basso allo schermo.

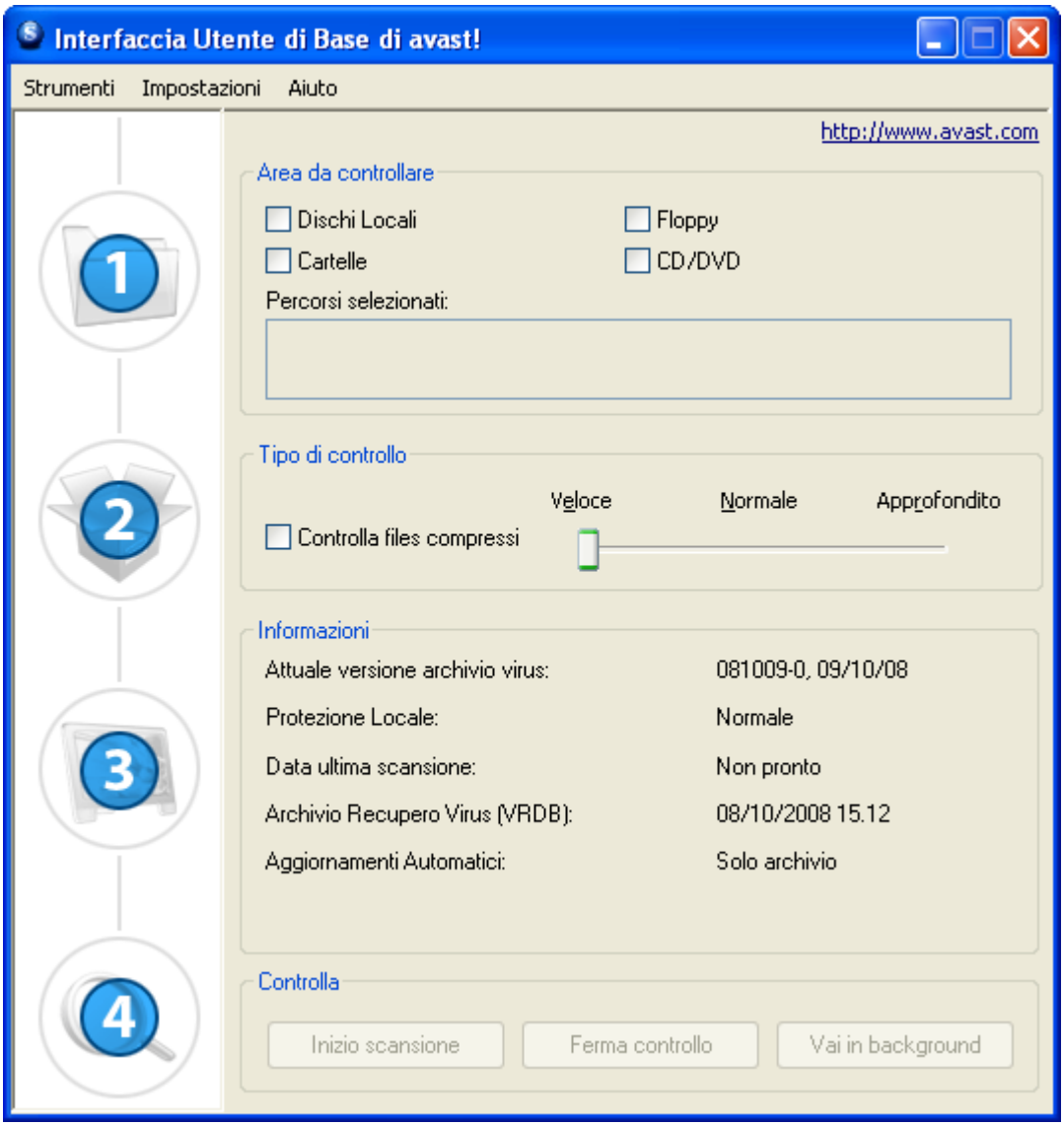
Quando la scansione è terminata, e se non sono stati rilevati virus durante la scansione, la console visualizza la finestra di scansione con le informazioni di base: numero di cartelle e file controllati, il tempo utilizzato ecc...

Se sono rilevati dei virus, il programma vi chiederà cosa fare con i file infetti. Ci sono alcune opzioni, ad esempio, spostare il file nel **Cestino Virus**, o eliminarlo, rinominarlo o spostarlo, o se è possibile, anche ripararlo. Potete anche semplicemente mantenere intatto il file, ma questa opzione può comportare la diffusione del virus e causare ulteriori danni. Queste opzioni sono descritte approfonditamente nella sezione "**Cosa fare se viene rilevato un virus**".

Cambiare l'aspetto dell'Interfaccia Utente semplice

Se si utilizza l'interfaccia utente semplice, è possibile selezionare diversi programmi skin. Sono presenti tre distinte skin (apparenze) standard e tante altre possono essere scaricate da Internet:- **menu delle opzioni**, cliccare su "Seleziona skin" e poi sul link "Scarica altre skin....". Se si desidera utilizzare il programma senza skin, basta selezionare "Impostazioni" dal menu delle opzioni, quindi disattivare la casella "Abilita le maschere per l'interfaccia utente semplice". La prossima volta che si avvia il programma, le opzioni verranno visualizzate nel loro formato di base. Per ripristinare la skin, basta attivare di nuovo la suddetta opzione. La skin sarà ripristinata la prossima volta che si avvia il programma.

Apparenza dell'interfaccia utente semplice senza alcuna skin:



L'area da controllare ed il tipo di scansione sono impostate selezionando le apposite caselle. Se si desidera effettuare la scansione solo di cartelle specifiche,

cliccando sulla casella "Cartelle" si aprirà una nuova finestra che elenca tutte le cartelle del computer. Per selezionare una cartella, è sufficiente selezionare la casella che verrà visualizzata nella sezione "percorsi selezionati".

È possibile regolare la sensibilità di scansione spostando il cursore verso la posizione richiesta ed includere nella scansione i files compressi (controlla files compressi).

Dopo aver attivato la scansione, è possibile continuare a usare il computer per altri compiti, cliccando sul pulsante "Vai in background".

È inoltre possibile regolare la sensibilità della protezione residente, cliccando su "Impostazioni" e poi su "protezione locale". È possibile utilizzare il dispositivo di scorrimento per modificare la sensibilità su "Normale" o "Elevata" o è possibile disattivare completamente la protezione locale (“Disabilitato”). Tuttavia, come descritto in precedenza, le modifiche apportate qui si estendono e tutti i moduli di protezione locale. Per regolare la sensibilità dei moduli singolarmente, vedere **pagina 26**.

È possibile accedere ad altre funzioni, come ad esempio il Cestino Virus e l’archivio Virus cliccando su "Strumenti" e selezionando l'opzione desiderata tra quelle disponibili. Queste, e tutte le altre caratteristiche, sono descritte in dettaglio più avanti in questo manuale.

Le informazioni sullo stato attuale del programma sono presentate nella parte inferiore della schermata, come descritto nella sezione precedente.

Cosa fare se viene rilevato un virus

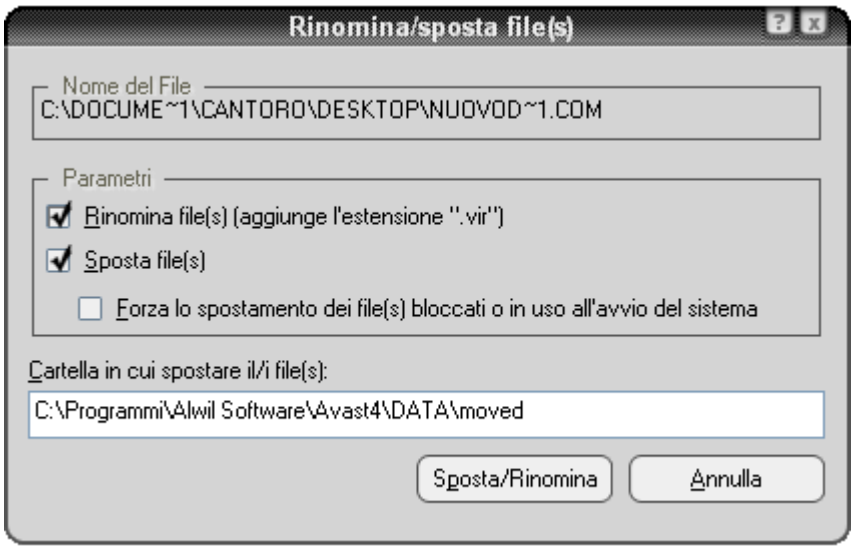
Se il programma rileva un file sospetto, la scansione verrà interrotta in quel punto ed apparirà la seguente schermata, con le opzioni su cosa fare:

Cliccando su "Continua" non si intraprendono azioni in relazione al file individuato e questo sarà visualizzato alla fine della scansione nella lista dei risultati - vedere a **pagina 42**. Cliccando su "Stop" si concluderà la scansione in quel punto.

Se un virus è stato rilevato da uno dei moduli di protezione locale ad esempio, cercando di aprire un file infetto, o dallo screensaver, la schermata sarà leggermente diversa - i pulsanti "Continua" e "Stop" saranno sostituiti da un unico pulsante "Nessuna azione". Cliccando su questo pulsante non si intraprende nessuna azione, il file infetto resterà dov' è, ma il virus non sarà attivato.

In alternativa, se si desidera intervenire subito, ci sono quattro possibili opzioni.

Opzione 1: Spostare il file interessato in un'altra cartella del vostro computer. Allo stesso tempo, si avrà l'opportunità di rinominarlo. Cliccando su "Rinomina/Sposta" verrà visualizzata la seguente schermata con la casella "Sposta file(s)" già selezionata.



Nella parte bianca della schermata, è possibile specificare dove si desidera spostare il file sospetto. Il programma seleziona automaticamente la cartella di destinazione, oppure è possibile sceglierne una distinta.

Se si seleziona la casella "Rinomina file(s)", si aggiungerà automaticamente l'estensione ". Vir" alla fine del nome del file, per identificarlo come file potenzialmente pericoloso, per non correre richsi ed infettare involontariamente il vostro computer.

Se non è possibile spostare il file, ad esempio, perché è utilizzato al momento da un altro programma, selezionando la casella "Forza lo spostamento dei file(s) bloccati o in uso all'avvio del sistema", il file verrà trasferito automaticamente alla destinazione selezionata, non appena si riavvia il computer.

Nota - nel caso in cui sia infetto un ***file di sistema***, cioè un file che viene utilizzato per l'esecuzione di un programma, spostare il file potrebbe visualizzare un errore la prossima volta che il computer tenta di aprire il programma. Tuttavia, se il file è stato spostato nel Cestino Virus, sarà protetto in una zona di quarantena dove non può causare danni agli altri file e dove potrà eventualmente essere riparato prima di essere trasferito nella sua posizione originale - vedere **pagina 8**

Opzione 2: Cancella file – cliccando su "Cancella" apparirà la seguente schermata:

A seconda della versione di Windows che si sta usando, ci sono due modi per cancellare il file.

- ***Cancella file(s) e portarli nel cestino***
  il file (s) viene spostato nel Cestino, ma non eliminato definitivamente. Lo stesso file può essere ripristinato in seguito. Questa opzione potrebbe non essere disponibile in alcune versioni di Windows.

- ***Cancella file(s) definitivamente***
  in tal modo il file (s) verrà rimosso dal computer permanententemente senza alcuna possibilità di ripristinarlo in un secondo momento. Tuttavia, questa operazione eliminerà solo il file infetto. Alcuni virus installano nuovi file sul computer e, se questi stessi file non contengono un virus, non saranno ritenuti sospetti. Nonostante questi file trovino spazio sul vostro computer, non dovrebbero essere pericolosi.

Se è stato rilevato un virus che può essere completamente rimosso dal virus cleaner incorporato, (rimozione dei nuovi file creati dal virus compresa) , verrà visualizzato un ulteriore pulsante - ***"rimuovere completamente il virus dal sistema"*** -. Se questa opzione è disponibile, si raccomanda di usarla.

Se momentaneamente non è possibile eliminare il file, ad esempio, perché è utilizzato da un altro programma, selezionando la casella "Se necessario, cancella file(s) al prossimo riavvio" il file verrà cancellato, non appena si riavvia il computer. Cliccare su "Elimina" nuovamente per confermare l'eliminazione.

Nota - nel caso in cui sia infetto un ***file di sistema***, cioè un file che viene utilizzato per l'esecuzione di un programma, cancellare il file potrebbe visualizzare un errore la prossima volta che il computer tenta di aprire il programma.
Prima di eliminare il file, assicuratevi che il file infetto non sia un file di sistema, o che sia possibile sostituirlo con un file pulito, per esempio con una copia di backup.
Se non si è sicuri, si consiglia di spostare il file nel Cestino Virus. Qui sarà protetto in una zona di quarantena dove non è in grado di causare danni agli altri file e dove potrà essere eventualmente riparato prima di essere ritrasferito nuovamente alla posizione originale - vedere **pagina 8**

Opzione 3: Ripara file.

cliccando su "Ripara" apparirà la seguente schermata:

Cliccando su "Ripara", il programma tenterà di ripristinare il file.

Per ripristinare un file, il programma farà riferimento al ***Virus Recovery Database***. Se non vi sono sufficienti informazioni sul programma nella banca dati, ci sono buone possibilità che possa essere riparato. Nota - solo i file che sono stati fisicamente cambiati da un virus possono essere riparati. Se sono stati creati dei nuovi file, questi rimarranno intatti a meno che non possano essere rimossi dal Virus Cleaner - vedere Opzione 2.

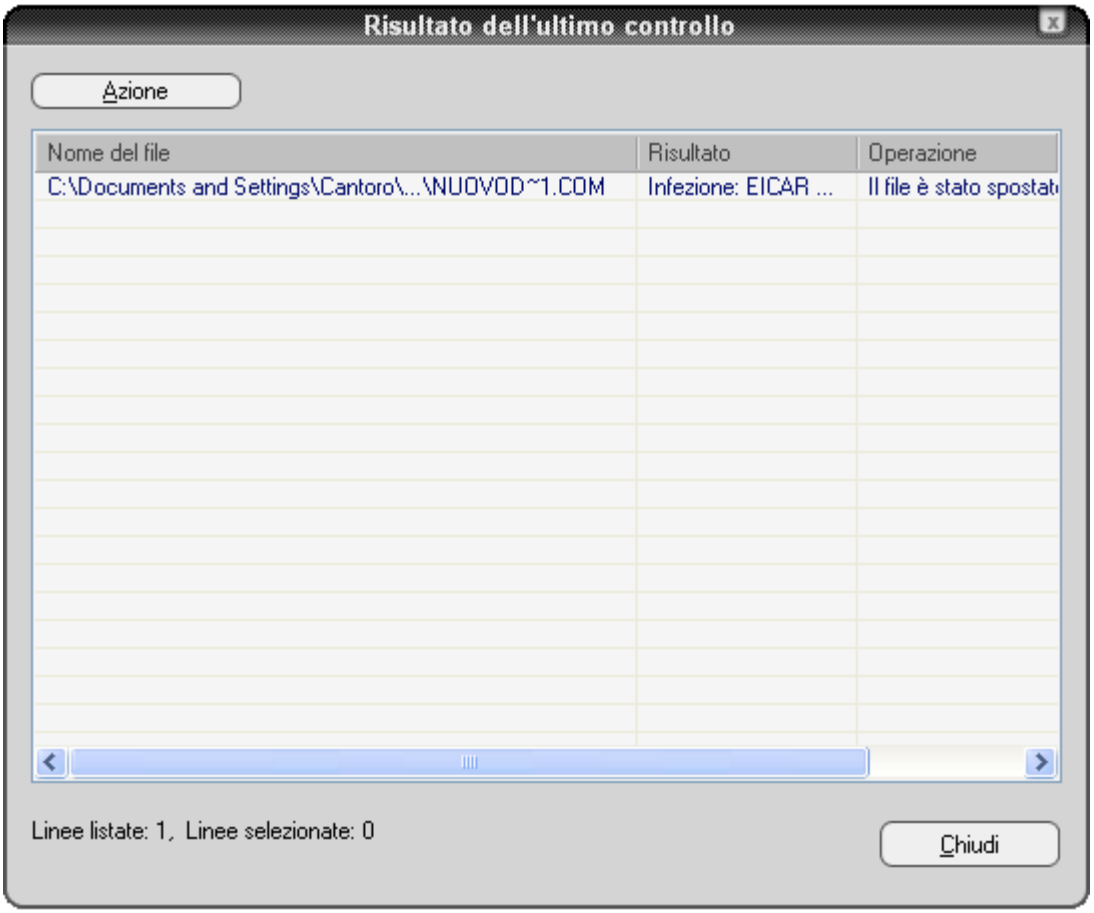
Se non vi è alcuna informazione nella banca dati, la riparazione può essere ancora possibile, ma il pieno recupero è improbabile. E 'quindi molto importante che la banca dati sia in continuo aggiornamento - per aggiornare il Virus Recovery Database, basta cliccare con il tasto destro del mouse sull'icona di avast!con la "i" nell'angolo in basso a destra dello schermo del computer e selezionare GENERA VRDB adesso. La banca dati verrà quindi aggiornata con l'indicazione di eventuali nuovi programmi installati sul vostro computer, subito dopo l'ultimo aggiornamento.

Opzione 4: L' **OPZIONE CONSIGLIATA** è quella di spostare spostare il file nel **Cestino Virus**.

Nota - nel caso in cui sia infetto un ***file di sistema***, cioè un file che viene utilizzato per l'esecuzione di un programma, cancellare il file potrebbe visualizzare un errore la prossima volta che il computer tenta di aprire il programma.
Tuttavia, se il file è spostato nel Cestino Virus, sarà protetto in una zona di quarantena dove non è in grado di causare danni agli altri file e dove potrà essere eventualmente riparato prima di essere ritrasferito nuovamente alla posizione originale - vedere **pagina 8**

Risultati dell'ultima scansione

Una volta che avete deciso l'azione da intraprendere con il file selezionato, la scansione riprende automaticamente. Se sono rilevati altri file sospetti, e l'opzione ELIMINA TUTTO non è stata selezionata, la scansione si arresta di nuovo e il processo viene ripetuto. Quando la scansione è completa, vengono visualizzati i risultati insieme con i dettagli sulle azioni intraprese nei confronti di ogni file sospetto - vedere sotto.



Se si è scelto di non intraprendere alcuna azione durante il processo di scansione, in merito ad un particolare file, questo file verrà elencato nei risultati di scansione, tuttavia la colonna "Operazione" risulterà vuoto.

Per operare con il file in questione, occorre cliccare sul nome del file nella tabella, quindi su "Azione" nell'angolo in alto a sinistra, e visualizzerete così l'elenco delle opzioni, come descritto nelle pagine precedenti. L'azione intrapresa sarà poi visualizzata nella sezione "Operazione".

Per abbandonare i risultati della scansione cliccare su "Chiudi". Per visualizzare i risultati di scansione, è sufficiente aprire il **menu delle opzioni** e selezionare

l'opzione "Risultati dell' ultima scansione".

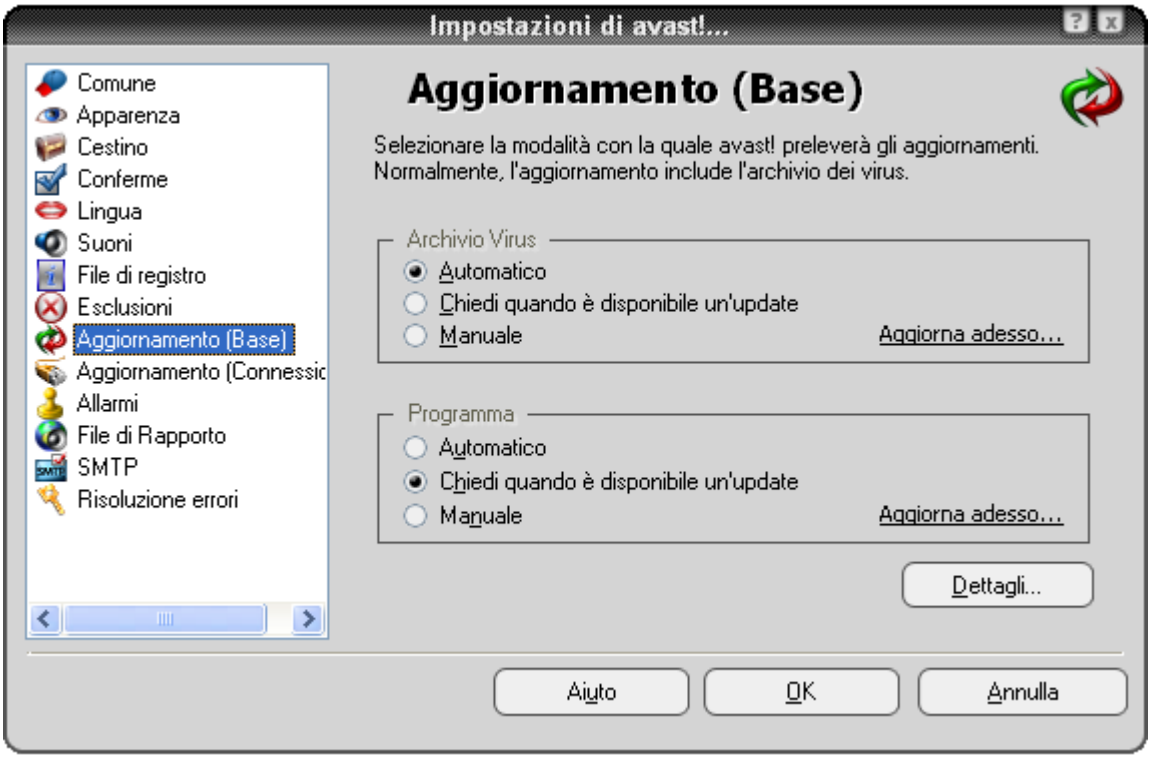
Nota: Se si chiude avast!, l'opzione "Risultati dell' ultima scansione". non sarà disponibile e non sarà in grado di visualizzare i risultati la prossima volta che si avvia il programma. Questa opzione sarà nuovamente disponibile solo se si esegue una nuova scansione. Tuttavia, le informazioni sulla presenza di eventuali virus o errori, vengono salvate e possono essere visualizzate aprendo il Log Viewer - vedere a **pagina 58**.

Funzioni avanzate

Impostazione aggiornamenti automatici

Qualsiasi programma antivirus è efficace solo se è il suo archivio virus funziona, per questo è importante aggiornare regolarmente sia il programma che l'archivio.

È possibile decidere se il programma e l'archivio virus devono essere aggiornati automaticamente o manualmente, o soltanto in presenza della notifica della disponibilità di un aggiornamento di avast! Per cambiare lo stato, basta cliccare sulla situazione attuale (ad esempio "Solo Archivio") nella schermata della console di avast!, o semplicemente aprire il **menu delle opzioni** (vedere **pagina 30**), selezionare "Impostazioni", quindi "Aggiorna (Base)". Qui è possibile cambiare le impostazioni per gli aggiornamenti.



Cliccare su "OK" e sulla console vera visualizzato quanto segue:

- **ACCESO** se si seleziona“Automatico” per il programma e per l’archivio virus
- **SOLO PROGRAMMA** se si seleziona“Automatico” solo per il programma
- **SOLO ARCHIVIO** se si seleziona“Automatico” solo per l’archivio virus
- **SPENTO** se NON si seleziona“Automatico” per il programma e per l’archivio virus

Per aggiornare **manualmente** sia il programma che l’archivio virus andare su **menu delle opzioni** (vedere **pagina 30**) e selezionare l’opzione “Aggiornamento”.

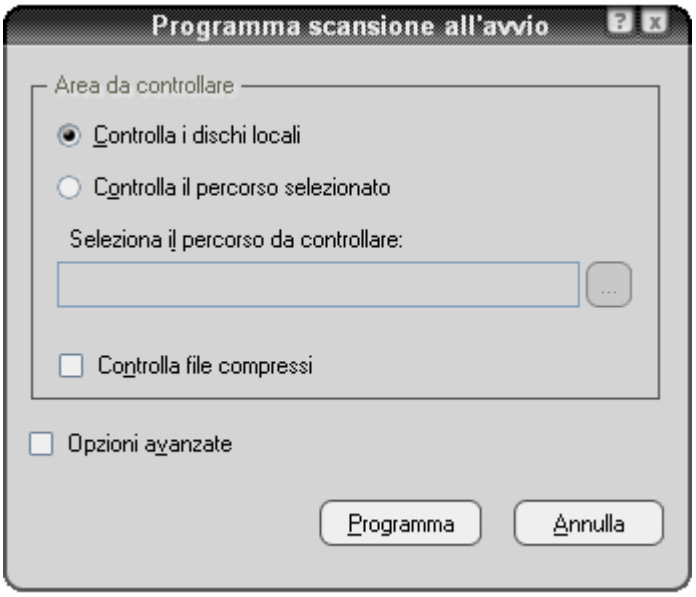
- Per aggiornare l’archivio virus selezionare **Aggiornamento iAVS**
- Per aggiornare il programma avast!, selezionare **Aggiornamento del Programma**

Come programmare la scansione all’avvio

(solo su versioni 32 bit di Windows NT/2000/XP/Vista)

E 'possibile programmare una scansione automatica quando il computer viene riavviato, vale a dire quando avviene il "boot-up" prima dell'avvio effettivo del sistema operativo. L’operazione è utile quando si sospetta che un virus possa essere entrato nel vostro computer, permettendone la rilevazione prima che sia attivato e prima di causare danni.

Per programmare la suddetta scansione, basta accedere al **menu delle opzioni** (vedere **pagina 30**) e cliccare su “Programma scansione all’avvio”. Apparirà la seguente schermata:



Da qui è possibile effettuare la scansione di tutti i dischi o solo di alcune aree selezionate. Per eseguire la scansione delle aree selezionate, cliccare su "Controlla il percorso selezionato" e digitare il nome del percorso, oppure selezionare la casella a destra per cercare l'area che si desidera sottoporre a scansione. Quando si trova l'area che si desidera controllare, cliccarci sopra ed il nome del percorso verrà copiato automaticamente.

Se si desidera controllare i file compressi, selezionate la casella "Controlla file compressi"

Selezionando "Opzioni avanzate" è possibile specificare come operare con eventuali file infetti. Le opzioni sono le seguenti:

- Cancella file infetto
- Sposta file infetto
- Sposta file infetto nel Cestino
- Ignora file infetto
- Ripara file infetto

Con "Sposta file infetto" i files vengono trasferiti nella cartella C:/Program Files\Alwil Software\Avast4\DATA\moved. L'estensione ".vir" sara aggiunta al nome del file per identificare il file come sospetto ed evitare di aprirlo accidentalmente e causare così danni al computer.

Se si sceglie una qualsiasi delle opzioni per Eliminare o Spostare i file infetti, vi verrà chiesto di confermare come volete agire con eventuali **files di sistema** infetti.

I files di sistema, vengono utilizzati dal computer per eseguire i programmi, e l'eliminazione o lo spostamento di questi files potrebbero avere gravi conseguenze. Vi sarà chiesto quindi, di confermare se si desidera:

- Permettere l'eliminazione o lo spostamento, o
- Ignorare l'eliminazione o lo spostamento dei files sistema

Selezionando " l'eliminazione o lo spostamento " si evitano eventuali problemi operativi, ma il computer sarà ancora a rischio di potenziali infezioni. L'azione consigliata è quindi quella di spostare tutti i file sospetti nel Cestino Virus, dove possono essere successivamente trattati in una zona protetta chiamata quarantena. Una volta spostato nel cestino virus, il file non può più causare danni ad altri file. È quindi possibile operare con i files interessati, come descritto a **pagina 57**, in modo da essere eliminati, se si è certi di non compromettere la funzionalità del pc, o essere spostati nella loro posizione originale, o semplicemente essere lasciati da parte fino a quando non si decide cosa fare.

Dopo aver confermato come maneggiare eventuali files infetti, cliccare su "Agenda". Apparirà il seguente messaggio:

Cliccare su "Sì" per riavviare il computer ed eseguire la scansione all'avvio, o cliccare su "No" per effettuare la scansione automaticamente la prossima volta che si riavvia il computer.

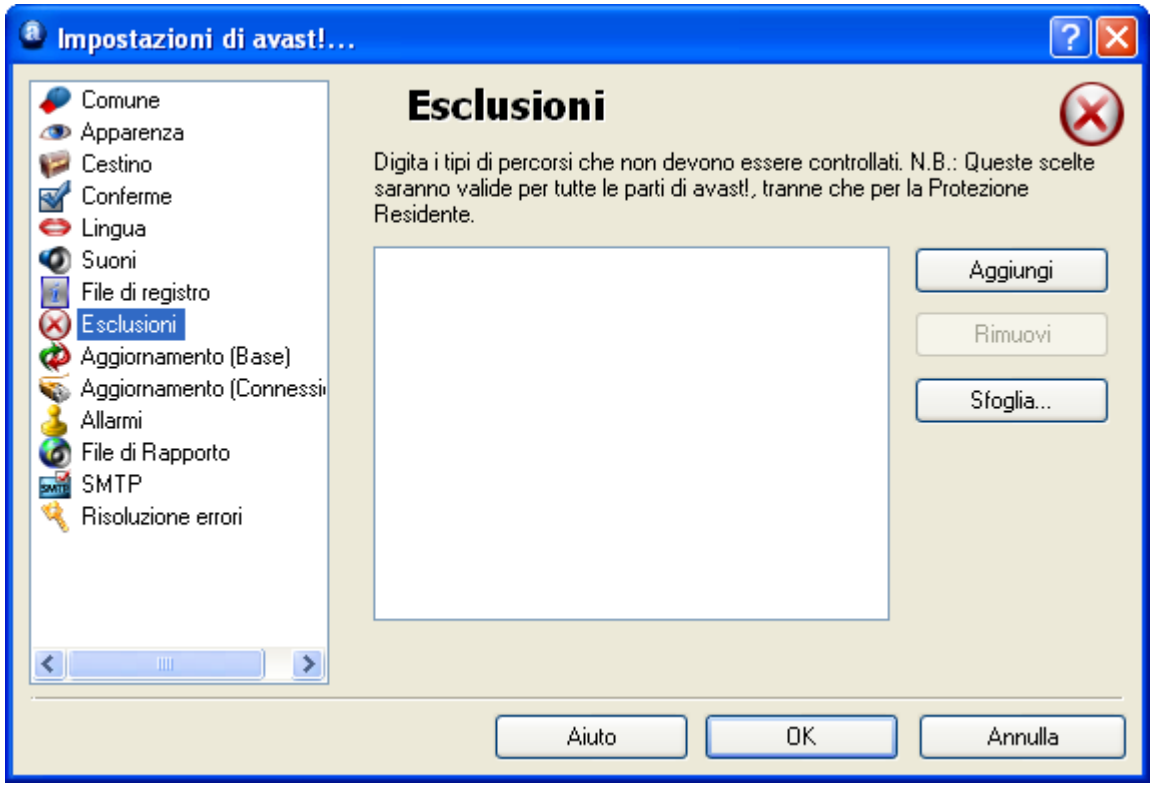
Esclusione files durante la scansione

E 'possibile evitare la scansione di alcune aree, o di un unico file, il che significa che non saranno controllati durante la scansione. Quest'operazione può essere utile in alcuni casi:

Evitare falsi allarmi. Se il programma rileva un virus in un file, ma si è sicuri che si tratta di un falso allarme, è possibile escludere il file dal controllo ed di evitare falsi allarmi. Si prega di informare il nostro team di Alwil Software della presenza di questi file, in modo da risolvere il problema in futuro.

Accellerare il processo di scansione. Se si dispone di una cartella sull'hard disk che contiene solo immagini, si può ad esempio escluderla dal controllo aggiungendola alla lista delle esclusioni, riducendo in questo modo il tempo la scansione.

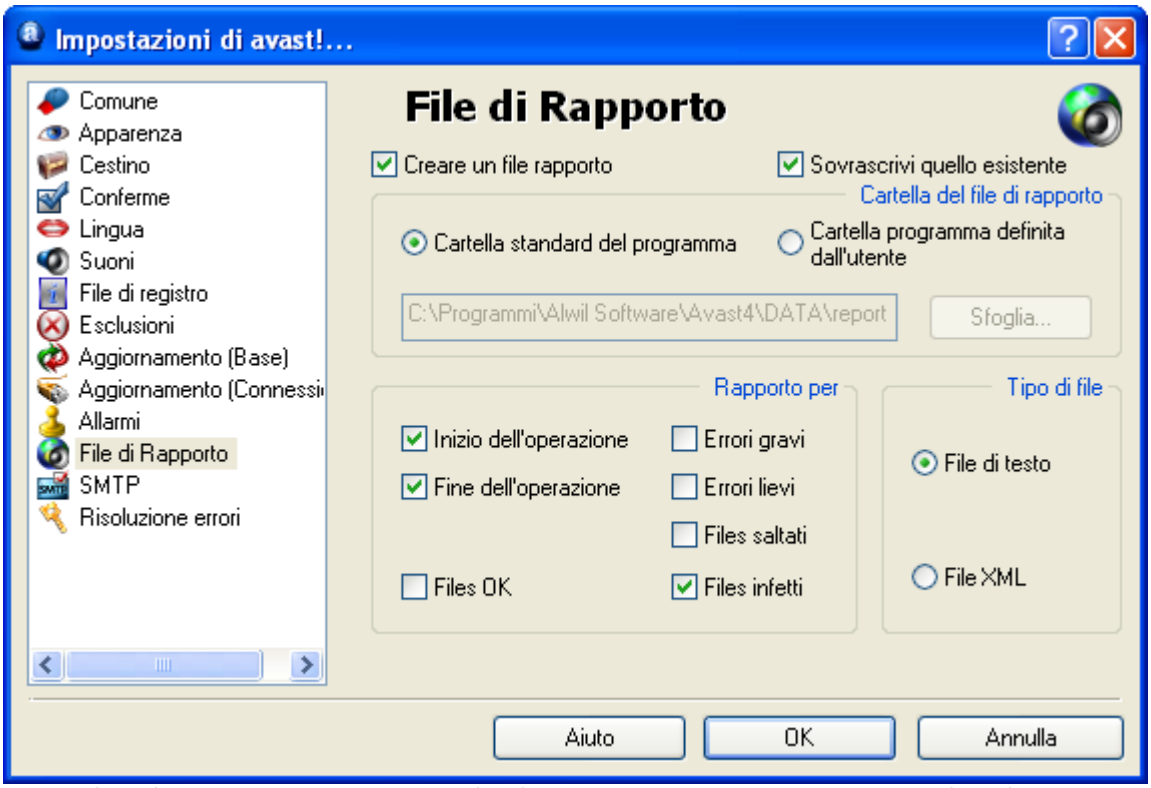
Tenete presente che queste esclusioni saranno valide per tutte le future scansioni, fatta eccezione per la protezione locale. Per escludere dal controllo determinati file o cartelleè sufficiente cliccare su "Impostazioni" e quindi su "Esclusioni" nel **menu delle opzioni** (vedere **pagina 30**):



Per escludere una cartella o un file, cliccare su Sfoglia e quindi selezionare la cartella o il file da escludere. In alternativa, cliccare su "Aggiungi" e digitare manualmente il percorso della cartella o del file. Se si vuole escludere una cartella, comprese tutte le relative sottocartelle, è necessario aggiungere "\ *" alla fine del nome della cartella ad esempio, C: \ Windows \ *. Per rimuovere una cartella o un file dalla lista delle esclusioni, bast cliccare sullo stesso file, ed una volta evidenziato, cliccare su "Rimuovi"

Come creare un file di rapporto con i risultati della scansione

È possibile registrare permanente i risultati di ciascuna scansione, mediante la creazione di una rapporto visionabile in qualsiasi momento. Per creare un rapporto, basta accedere alle **menu delle opzioni**, come descritto a **pagina 30** e selezionare "Impostazioni". Cliccare su "File di Rapporto" e nella schermata successiva, selezionare la casella "Creare file rapporto", come illustrato di seguito.



Se si desidera creare un nuovo file dopo ogni scansione e non si desidera tenere un registro con tutti i precedenti risultati di scansione, selezionare la casella "Sovrascrivi quello esistente". Se questa casella non è selezionata, i risultati di ogni scansione verranno aggiunti a quelli della precedente relazione.

È inoltre possibile scegliere se si desidera salvare la relazione – nella cartella standard programma, che il programma crea automaticamente, o in un altro luogo che è possibile specificare cliccando su "Cartella programma definita dall'utente" e inserendo il percorso della cartella.

Quindi, è possibile specificare quali informazioni includere nel file di rapporto:

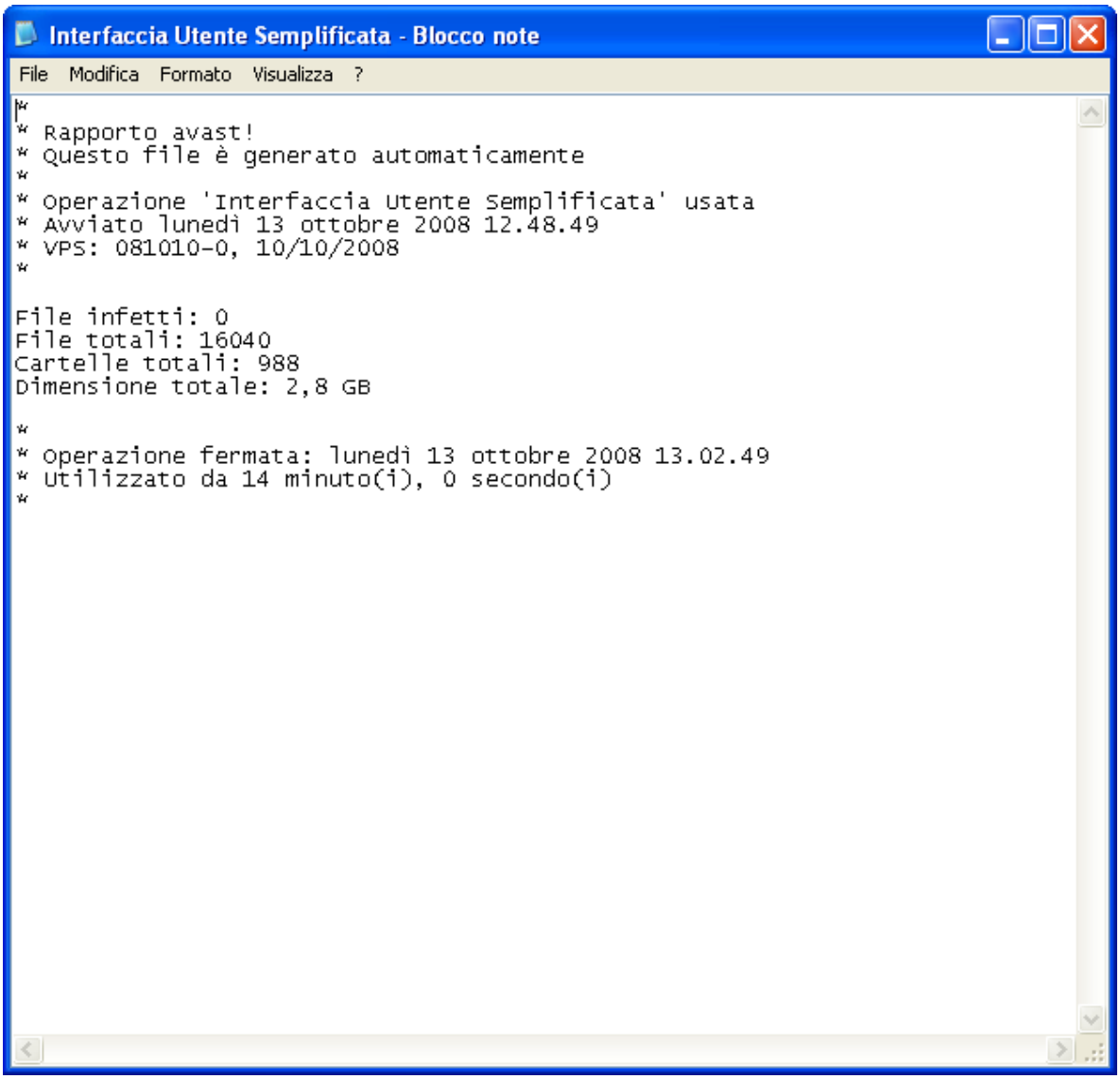
- Inizio dell'operazione – data e ora d'inizio della scansione
- Fine dell'operazione – data e ora della fine della scansione

- Files OK – file che sono stati controllati senza rilevare nulla di sospetto. Se tutte le unità locali fossero controllate, questa casella produrrebbe una lunga relazione, di diverse migliaia di righe. Si consiglia pertanto di selezionare questa casella solo se si ha intenzione di effettuare una scansione limitata e se si desidera che tutti i file puliti siano riportati insieme ad i files sospetti.
- Errori gravi quando il programma rileva qualcosa di inaspettato. Questi errori di norma richiedono un ulteriore approfondimento.
- Errori lievi, sono errori meno gravi relative a files che non sono potuti essere controllati perchè utilizzati da alter applicazioni.
- Files saltati, ovvero non controllati in base alle impostazioni di scansione. Per esempio, nella scansione rapida, i files sono controllati in base alla loro estensione. I files con estensione non considerata pericolosa, non sono controllati. Anche i files escusi dal controllo saranno riportati come “saltati”.
- Files infetti – files che potenzialmente contengono un virus.

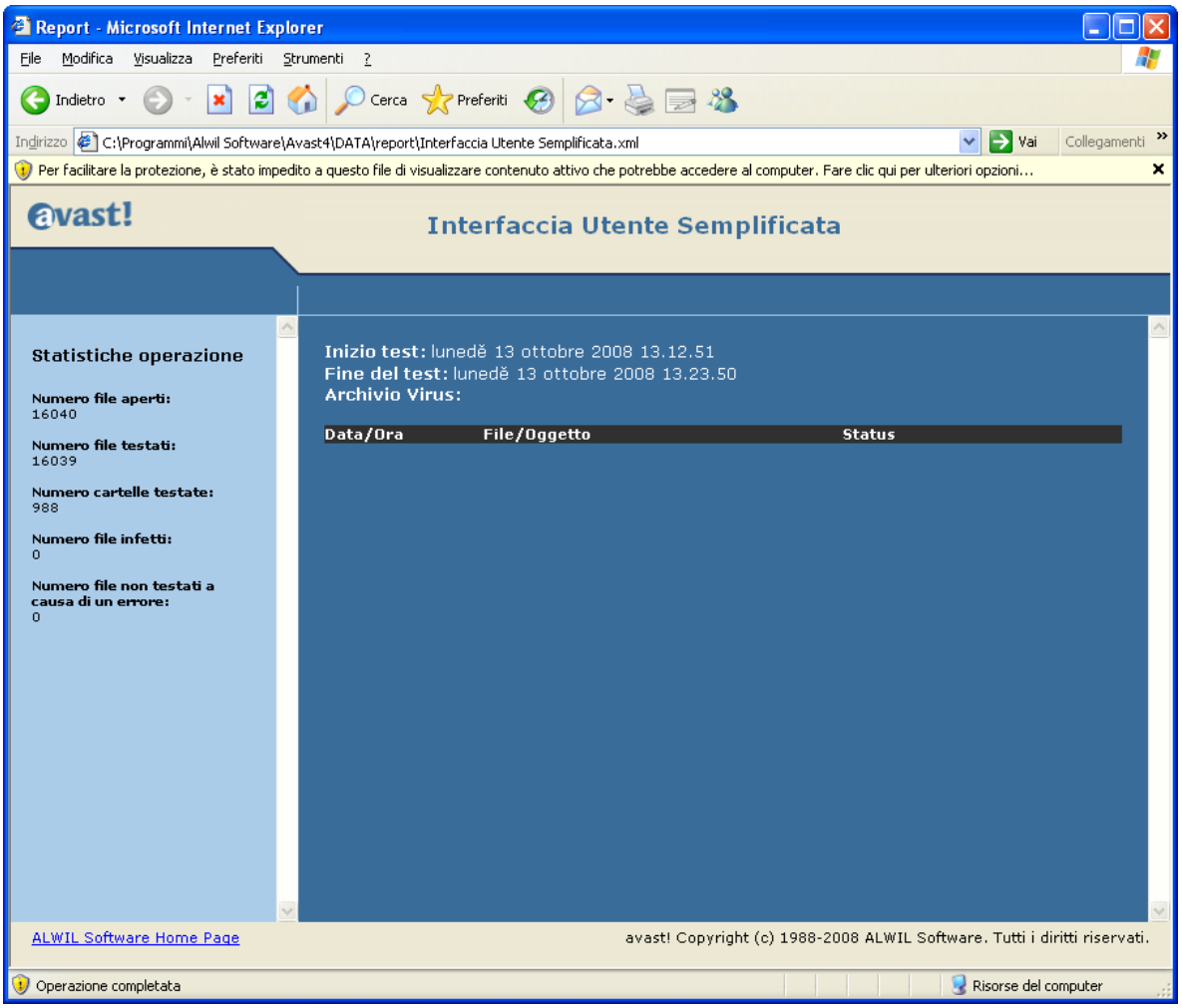
Infine è possibile specificare se la relazione deve essere sotto forma di file di testo o di file XML. Dopo aver eseguito la scansione, vi sarà una nuova riga nella finestra informativa della console - "Vedi il rapporto l'ultima scansione" come illustrato di seguito.

Cliccando su "Vedi il rapporto l'ultima scansione" verrà visualizzato nel formato specificato. In alternativa, aprire il **menu delle opzioni** (vedere **pagina 30**) e cliccare su "Vedi rapporti di scansione".

Rapporto in file di testo:



Rapporto in file XML:



Le relazioni delle scansioni precedenti sono memorizzate nella cartella standard del programma o nella cartella scelta per la relazione - vedi pagina precedente.

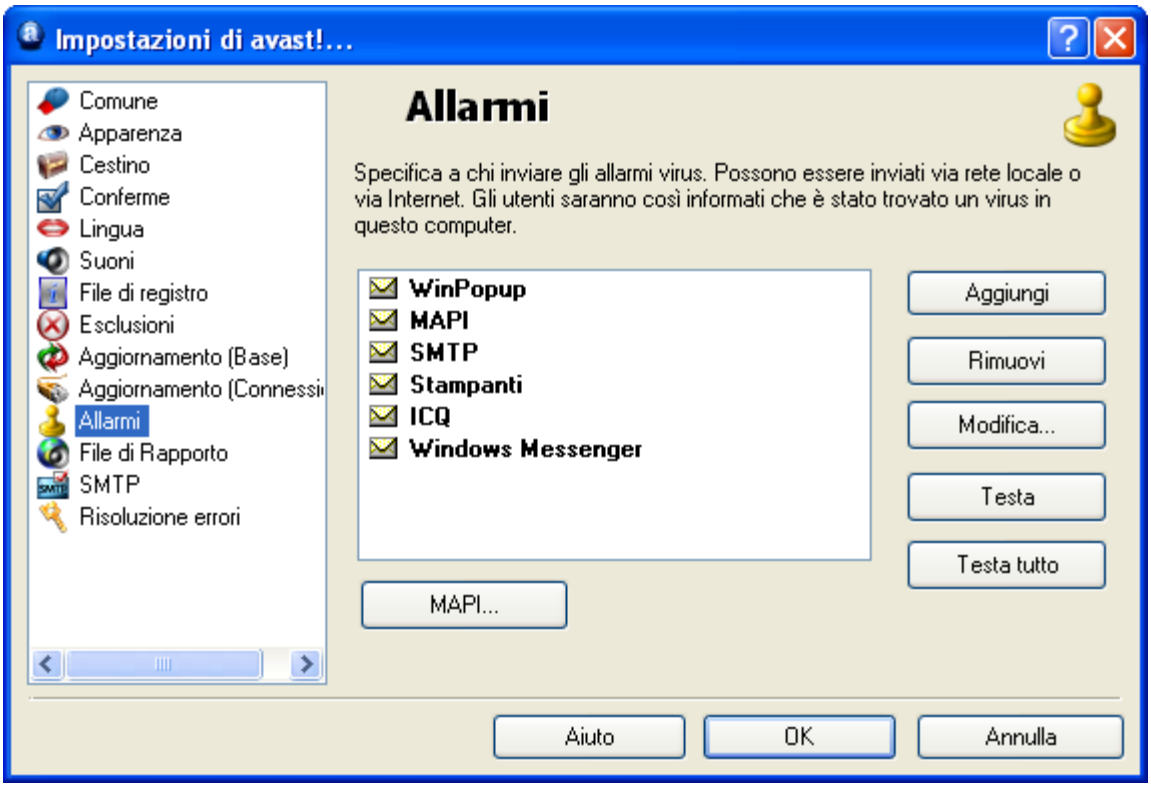
Se avete scelto il file di testo e non la casella "Sovrascrivi quello esistente" non è stata contrassegnata, sarà possibile vedere le precedenti relazioni ogni volta che si visualizza il rapporto in seguito ad una nuova scansione.

Se non si desiderano ulteriori relazioni, è sufficiente accedere alle "Impostazioni" quindi "File di rapporto" nel **menu delle opzioni** (vedere **pagina 30**) e deselezionare la casella di controllo "Creare un file di rapporto".

Allarmi

avast! è in grado di inviare un messaggio di allarme in presenza di un virus. Nel **menu delle opzioni**, selezionare "Impostazioni" e poi "Allarmi". Questa funzione è

utile per gli amministratori di rete che riceveranno notifica circa la presenza di un virus su uno qualsiasi dei computer di rete, in modo da poter reagire rapidamente.



L' allarme può essere inviato nelle seguenti forme:

- **WinPopup.** Cliccare su on "Aggiungi" e selezionare WinPopup. Inserire quindi l'indirizzo IP o il nome di rete del computer per inviare l'avviso, o cliccare su "Sfoglia" e selezionare l'indirizzo dalla lista delle opzioni disponibili.

- **MAPI.** L'avviso sarà inviato via e-mail, utilizzando il protocollo MAPI. Inserire l'indirizzo per inviare la posta elettronica, quindi cliccare sul pulsante MAPI nella parte inferiore dello schermo e inserire il nome del profilo MAPI e la password corrispondente.

- **SMTP.** L'avviso sarà inviato via e-mail, utilizzando il protocollo SMTP. Per creare una nuova segnalazione, cliccare su "Aggiungi" e quindi su SMTP. Nella casella che appare, inserire l'indirizzo e-mail della persona alla quale inviare la segnalazione. È inoltre necessario specificare alcune ulteriori impostazioni - vedere la sezione successiva "SMTP".

- **Stampanti.** La segnalazione verrà inviata alla stampante selezionata. Cliccare su "Aggiungi" e poi "stampante", quindi su "Sfoglia" e selezionare la stampante da una delle opzioni disponibili.

- **ICQ.** L'avviso sarà inviato con un messaggio su ICQ. Basta inserire il numero ICQ della persona alla quale inviare l'avviso.

- **Windows Messenger.** Basta inserire l'indirizzo e-mail che il destinatario dell'avviso utilizza per accedere al servizio Windows Messenger.

Per creare un nuovo allarme, cliccare su "Aggiungi" e selezionare il tipo di allarme richiesto, quindi inserire le informazioni richieste, come descritto sopra. Una volta creato un allarme, ogni volta che viene rilevato un file sospetto destinatario scelto riceverà un avviso.

Per modificare o eliminare un allarme creato, basta selezionarlo, quindi cliccare su "Modifica" o "Rimuovi".

Cliccando su "Testa" un messaggio di prova verrà inviato all'indirizzo selezionato, mentre cliccando su "Testa tutto" verrà inviato un messaggio di prova a tutti i destinatari dell' avviso presenti nella lista.

SMTP

Cliccando su SMTP nella lista a sinistra dello schermo, è possibile specificare i parametri server SMTP. avast! utilizza queste impostazioni per l'invio di e-mail, in particolare quando:

- Invia messaggi di allarme se viene rilevato un virus
- Invia files dal Cestino virus ad ALWIL Software.
- avast! invia "crash reports" ad ALWIL Software.

Vi preghiamo inserire le seguenti informazioni:

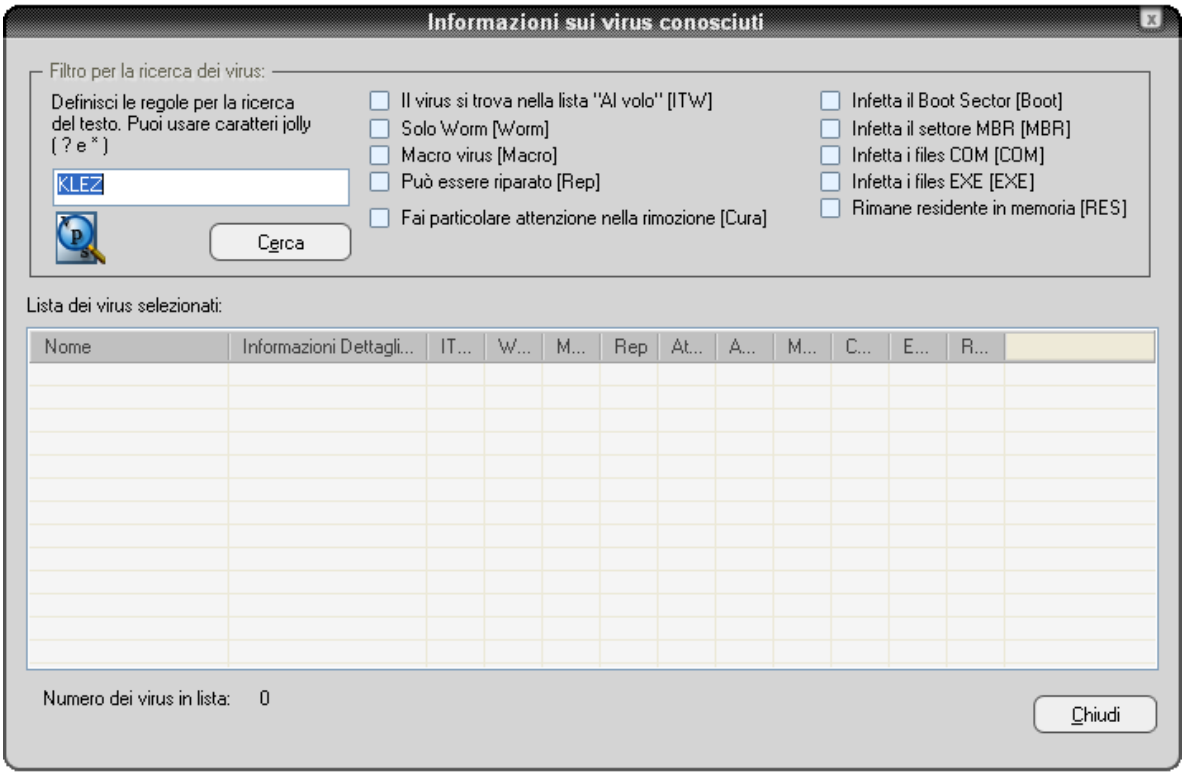
- Indirizzo Server – indirizzo server e-mail in uscita (per esempio smtp.server.com o 192.168.1.25).
- Porta – numero di porta (il numero predefinito è 25).
- Dall'indirizzo - indirizzo del mittente ("Da").

Se il server SMTP richiede l'autenticazione all'accesso, si dovrebbe anche selezionare la casella ed inserire il nome utente e la password.

Ricerca nell'archivio virus

L'archivio dei virus contiene informazioni dettagliate su tutti i virus conosciuti, e viene utilizzato dal programma per individuare eventuali infezioni.

Per accedere all' archivio virus, aprire il **menu delle opzioni** (vedere **pagina 30**) e cliccare su "Archivio Virus ". Verrà visualizzata la seguente schermata:



I virus nella lista possono essere cercati in base molti parametri. Se si conosce il nome del virus, basta digitare il nome nella casella e cliccare sul Cerca. Se si conosce solo una parte del nome, è possibile digitare "?" Al posto di uno carattere sconosciuto (lettera o numero) o "*" al posto di più caratteri sconosciuti.

Esempio: Supponiamo di essere alla ricerca del virus "Klez". Il suo nome effettivo nell'archivio è Win32: Klez-H [Wrm]. Si dovrebbe dunque digitare: * Klez *. Saranno trovati tutti i virus che contengono la parola "Klez".

Per restringere la ricerca, è anche possibile utilizzare le caselle di controllo accanto a ciascuna caratteristica del virus. Per effettuare una ricerca su una particolare caratteristica, basta selezionare la casella cliccando due volte. Facendo clic su qualsiasi casella una volta, la casella diventa grigia e significa che il virus non presenta tale caratteristica. Se una casella è deselezionata, ma a sinistra presenta il colore blu/verde, significa che non importa che il virus abbia la suddetta caratteristica o meno.

Caratteristiche di ricerca del virus:

- ***Il Virus si trova nella lista "Al volo" (ITW…)***
  Il virus è sulla lista dei virus diffusi tra gli utenti di tutto il mondo.

- ***Solo Worm (Worm)***
  Questo è un particolare tipo di virus che non infetta i file direttamente, ma esegue altre azioni, come diffondersi via e-mail, rubare password ecc.

- ***Macro virus (Macro)***
  Questo tipo di virus usa il linguaggio macro, soprattutto dei prodotti Microsoft (per esempio Word, Excel).

- ***Può essere riparato (Rep)***
  I files infettati da questi virus può essere riparatik da avast! e riportati al loro stato originale prima dell' infezione.

- ***Fai particolare attenzione nella rimozione (Cura)***
  Per questi virus, è necessario seguire dei passaggi speciali durante la loro rimozione (altrimenti si potrebbero causare dei danni perfino maggiori di quelli causati dal virus stesso!).

- ***Infetta il Boot sector (Boot)***
  Questo tipo di virus infetta il settore di avvio dell'hard disk o di un dischetto.

- ***Infetta il settore MBR (MBR)***
  Questo tipo di virus infetta il master boot sector dell' hard disk.

- ***Infetta i files COM (COM)***
  Questo tipo di virus infetta i files eseguibili con estensione".com".

- ***Infetta i files EXE (EXE)***
  Questo tipo di virus infetta i files eseguibili con estensione ".exe".

- ***Rimane residente in memoria (RES)***
  Questi virus rimangono nella memoria RAM del computer e infettano i file non appena vengono avviati.

Lavorare con i file nel Cestino Virus

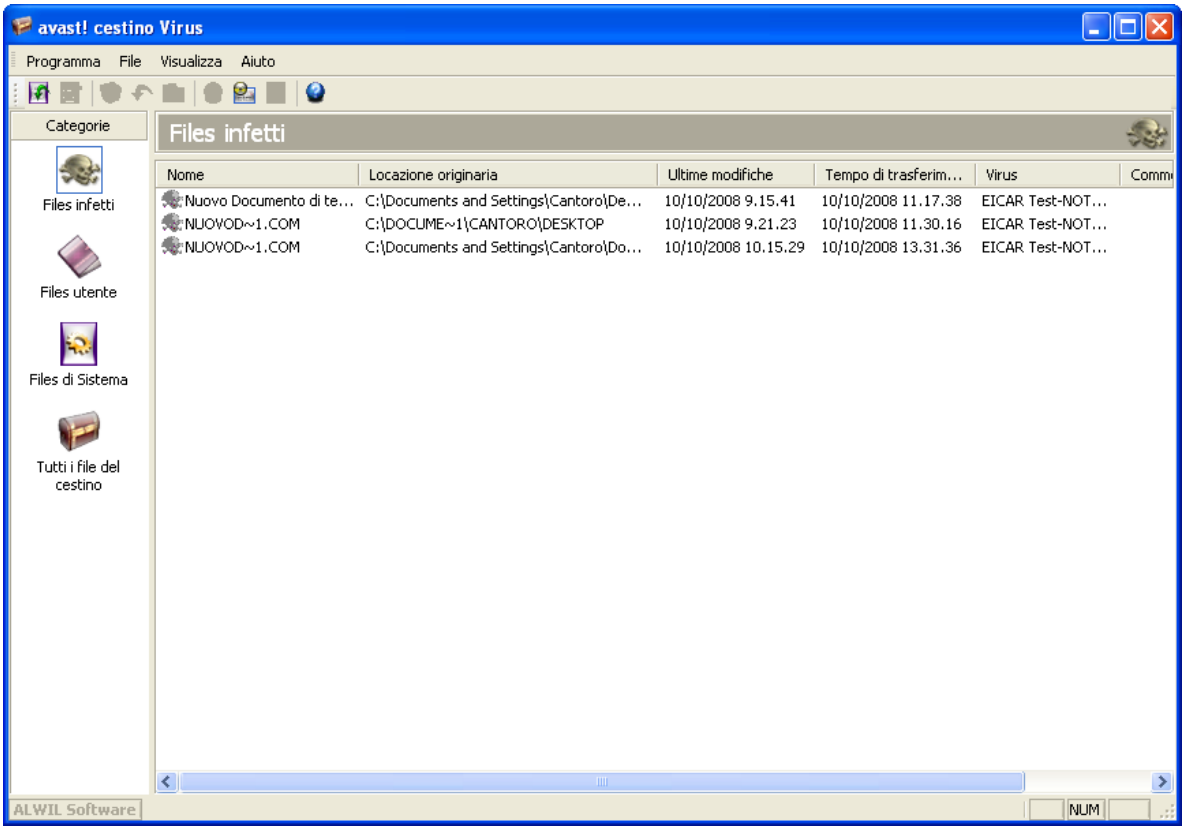
E' possibile accedere al Cestino Virus direttamente dal **menu delle opzioni**. Grazie alle sue proprietà uniche, il cestino virus è una vera e propria "quarantena", che può essere utilizzata per le seguenti finalità:

- ***Archiviazione virus.***
  Se avast! trova un virus e si decide di non cancellarlo, vi verrà data la possibilità di spostarlo nel cestino. Con il virus nel cestino, si può essere sicuri che non sarà avviato per sbaglio.

- ***Archiviazione files sospetti.***
  Il cestino è utile per l'archiviazione e le successive analisi dei files sospetti.

- ***Backup dei files di sistema.***

Durante l'installazione, copie di alcuni importanti files di sistema sono memorizzati nel cestino, nella categoria "files di sistema" (vedere sotto). Se i principali files di sistema sono infettati da un virus, le copie possono essere ripristinate dal cestino alla loro posizione originale.



Cliccando con il tasto destro del mouse su qualsiasi file si visualizzano le seguenti opzioni. In alternativa, si può cliccare con il tasto sinistro su un file, quindi sulla corrispondente icona nella parte superiore dello schermo oppure su "File" e selezionare l'opzione desiderata *(Nota: **Se si clicca due volte** su un file, non sarà possibile eseguirlo - verranno visualizzate le proprie caratteristiche. Si tratta di una misura di sicurezza per proteggere ulteriormente da infezioni accidentali all'interno del cestino):*

- ***Aggiorna tutti i files***
  Selezionate questa opzione se si desidera visualizzare la lista completa dei file. Il programma aggiorna automaticamente l'elenco, ma è possibile utilizzare questa opzione se non volete attendere.

- ***Aggiungi file.***
  Potete aggiungere files solo alla categoria "Files Utente" .

- ***Cancella file.***
  Se si seleziona questa opzione, il file verrà eliminato irreversibile, ovvero i files non sono semplicemente spostato nel cestino! Prima di eliminare qualsiasi file, assicuratevi che non si tratti di un file di sistema. L' eliminazione di un file di sistema potrebbe avere conseguenze molto gravi.

- ***Ripristina file.***
  Il file verrà ripristinato alla sua posizione originaria e, al tempo stesso rimosso dal cestino.

- ***Estrai file.***
  Il file verrà copiato nella cartella selezionata.

- ***Controlla file.***
  Il file vera controllato.

- ***Proprietà.***
  Si visualizzano le proprietà del file; è possibile aggiungere un commento al file.

- ***Manda un'Email ad ALWIL Software.***
  Il file selezionato verrà inviato (via e-mail) ad ALWIL Software. È opportuno utilizzare questa opzione solo in casi particolari - ad esempio se si sospetta che il programma abbia erroneamente individuato un file come virus. Non dimenticate di includere tutte le informazioni possibili - ad esempio il motivo per il quale si invia il file, la versione del vostro archivio virus, ecc.. in modo da aiutarci a migliorare il servizio che vi offriamo.

Cliccando su “Programma” e "Impostazioni del programma" e poi su "Cestino" è possibile regolare la dimensione massima consentita del Cestino ovvero la massima quantità di spazio da occupa sul vostro computer. È inoltre possibile specificare la dimensione massima di ogni singolo file da inviare al cestino.

Visualizzatore registro

Dopo ogni scansione, avast! antivirus crea diversi file di registro nei quali sono archiviate le informazioni su eventuali errori o file sospetti. Qui si trovano inoltre informazioni su installazioni e aggiornamenti del programma e sull’archivio virus. Per visualizzare questi registri, è sufficiente selezionare " Visualizzatore registro"dal **menu delle opzioni** (vedere **pagina 30**).

Le informazioni memorizzate nei files di registro sono suddivise nelle seguenti categorie:

Info	Solo information, tutto OK.
Nota bene	Informazioni importanti, tutto OK. Include informazioni sul programma e sugli aggiornamenti della banca dati.
Attenzione	Si è verificato un errore o è stato identificato un virus, ma il programma è in grado di funzionare o risolvere il problema.
Errore	Si è verificato un errore, il programma non può funzionare.
Critico	Errore critico, il programma sarà chiuso.
Allarme	Possibile rischio per l'intero computer.
Emergenza	Pericolo per l'intero computer (sicurezza, eliminazione file di sistema).

Cliccando su "Impostazioni del programma" e poi su "File di registro", è possibile regolare il limite di dimensione del file di registro.

Visualizzatore registro, è possibile effettuare la ricerca di documenti specifici, filtrare i registri in base a criteri specifici, o di trasferirli in un'altra posizione.

Cercare un registro

1. premere “CTRL” ed “F” insieme, o
2. cliccare su “Modifica”nell’angolo in alto a sinistra dello schermo e poi su“Trova”, o
3. cliccare sulla lente d’ingrandimento nell’angolo in alto a sinistra dello schermo, o

4. click con il tasto destro del mouse sulla lista dei registri e quindi cliccare su“Trova” nel menu.

Verrà visualizzata una casella in cui è possibile digitare tutto o parte del nome del registro che si desidera trovare. Se si conosce il nome esatto, basta selezionare la casella "Solo parole intere". Allo stesso modo, se si desidera solo cercare i registri utilizzando lettere maiuscole o minuscole, selezionare la casella "Maiuscole/minuscole ". Cliccando su "Su" o "Giù" si determina l’elenco registri in ordine crescente o decrescente.

Quindi, cliccare su "Trova successivo". Sarà visualizzato Il primo registro. Qualsiasi altro registro che corrisponda al nome inserito, può essere trovato cliccando su "Trova successivo".

Filtro elenco registri. per restringere la ricerca dei registri ad un breve elenco che soddisfa determinati criteri, ad esempio, una specifica parola chiave o la parte di una parola.

1. premere "CTRL" e "R" insieme, o
2. cliccare su "Modifica" nell'angolo in alto a sinistra dello schermo e poi su "Filtro", o
3. cliccare sull’imbuto giallo nell'angolo in alto a sinistra dello schermo, o
4. cliccate con il tasto destro sulla lista dei registri e poi su "Filtra" nel menu

Apparirà la casella per definire il filtro secondo i seguenti criteri:

Includi
Inserisci una parola chiave o parte di una parola inclusa nei registri da visualizzare. È possibile utilizzare caratteri “jolly” per esempio, si può digitare * al posto di lettere che non si conoscono. Più parole chiave devono essere separate da un punto e virgola (;).

Escludi
Inserisci una parola chiave o parte di una parola inclusa nei registri da non visualizzare.

Intervallo di tempo
Qui è possibile definire l'inizio e la fine del periodo per il quale si desidera ricevere i registri da visualizzare.

Seleziona le linee definite
Selezionando questa opzione, i registri corrispondenti ai criteri definiti saranno evidenziati nella lista.

Mostra solo le linee definite (nascondi il resto)
Selezionando questa opzione, i registri corrispondenti ai criteri definiti saranno evidenziati nella lista.Gli altri registri non saranno visualizzati. Questo è utile se l'elenco originale è molto lungo.

Ordina registri
Cliccando su una qualsiasi delle colonne sarà possibile ordinare i record in ordine crescente o decrescente in base alle informazioni in questa colonna. Cliccando sull'intestazione della colonna, l'elenco tornerà di nuovo allo stato originale.

Esporta registri

Una volta trovati e/o filtrati i registri, l'intero elenco può essere esportato e salvato come un nuovo file. Per esportare i registri, basta selezionare l'opzione "Esporta linee selezionate" o cliccare sull'icona di sinistra con la freccia verde. Per esportare l'intero elenco, selezionare "Esporta la lista corrente" o cliccare sull'icona con la freccia verde di destra. Nella nuova finestra visualizzata, scegliere la cartella di destinazione per il file esportato e digitare il nome del nuovo file, quindi fare cliccare su "Salva".

Impostazioni di Protezione locale

1. Messaggistica Instantanea

Programmi

Qui è possibile specificare quali files dei programmi di messaggistica istantanea devono essere controllati. Se si utilizza Windows 95/98/ME e si desidera proteggere il programma Trillian, è necessario inserire il percorso per il file di configurazione, “talk.ini” (è possibile utilizzare il pulsante Sfoglia). Alcuni programmi possono essere protetti solo se si utilizza Windows NT, 2000, XP, 2003, Vista o 2008.

2. Posta elettronica

Nelle pagine "POP", "SMTP", "IMAP" e "NNTP" è possibile specificare se controllare le e-mail in entrata e/o in uscita e le news. Se un virus è stato rilevato, un avviso sarà inserito nel messaggio coinvolto. È inoltre possibile inserire una nota di conferma nei messaggi liberi da qualsiasi infezione virus.

Reindirizza

Questa pagina permette di impostare la scansione trasparente delle e-mail. Ogni e-mail che passa attraverso le porte selezionate sarà controllata. Questa funzione è disponibile solo su NT sistemi operativi (Windows NT/2000/XP/2003/Vista/2008).

- Reindirizzamento porte.

i numeri delle porte predefinite sono standard per i quattro protocolli e-mail di base: Se si utilizza una porta (o porte) diversa/e devono essere inseriti qui. Diversi valori devono essere separati da virgole.

- Indirizzi ignorati.

Qui potete inserire gli indirizzi dei server di posta o le porte specifiche che si desidera escludere dalla scansione. Questa funzione può essere utile quando si vuole eseguire solo la scansione i messaggi da o verso un particolare account(e ignorare il resto). Ad esempio, se si entra insmtp.server.com, avast! non effettuerà la scansione dei messaggi (SMTP) in uscita per l’account corrispondente.

- Ignora comunicazione locale.

Questa opzione dovrebbe di norma essere selezionata. Se è deselezionata, avast! esplorerà anche la comunicazione locale (che di solito è sicura), operazione che potrebbe rallentare leggermente le prestazioni del computer. Nota: non inserire numeri di porta diversi da quelli in uso per il traffico e-mail. In caso contrario, potrebbero verificarsi dei problemi.

Avanzato

- Mostra Informazioni dettagliate sull'azione in svolgimento.

  Se questa casella è selezionata, le informazioni sui file attualmente in fase di controllo verranno visualizzate nell'angolo in basso a destra dello schermo.

- Modalità silenziosa.

  Se l'azione specificata sulla pagina dei virus è predefinita, come per esempio l'opzione interattiva, e la modalità silenziosa è attiva, eventuali file infetti verranno trattati automaticamente seguendo le seguenti regole:

  > Se è selezionata, "con risposta generale Sì (OK)", qualsiasi file infetto in allegato a un messaggio di posta elettronica verrà automaticamente eliminato.

  > Se è selezionata la seconda opzione "con risposta generale No (Annulla)" tutti i files infetti verranno automaticamente trasferiti al cestino virus.

Se l'azione specificata sulla pagina virus è l'azione predefinita e questa casella viene lasciata vuota, verrà visualizzata la schermata con l'allarme virus, che chiede cosa si vuole procedere con il file infetto.

Se è selezionata qualsiasi altra azione, diversa da quella predefinita, l'opzione interattiva, selezionando questa casella non si avrà nessun cambiamento.

Si noti, tuttavia, che se un azione diversa da quella predefinita è stato anche specificata per la Protezione Standard, questa si sovrappone l'azione selezionata per il provider di posta elettronica!

- Tempo esaurito per comunicazioni Internet.

Rappresenta il tempo in secondi in attesa di risposta dal server di posta. È possibile specificare se la connessione deve essere chiusa se non si riceve

risposta in questo intervallo tempo o se desiderate ricevere la richiesta di conferma .

- Mostra l'icona sulla barra delle operazioni mentre viene esaminata la posta

Se questa casella è selezionata, una piccola icona verrà visualizzata nella barra delle applicazioni nell'angolo in basso a destra dello schermo del computer per indicare che una scansione è in corso.

Euristiche

avast! non solo effettua la scansione della posta in entrata per i virus noti, ma può anche controllare i messaggi utilizzando l'analisi euristica ed eventualmente trovare un virus che non è ancora presente nell'archivio. In questa pagina è possibile modificare le impostazioni di analisi euristica

- Sensibilità- Bassa.
  - > Controllo semplice allegati.
    Gli allegati sono verificati in base al loro nome e se un allegato contiene due estensioni, ad esempio, "Patch.jpg.exe", sarà giudicato come potenzialmente pericoloso. avast! controlla anche se l'estensione corrisponde al reale tipo di file. Ad esempio se il file "Pamela.jpg" è una foto, come ci si potrebbe aspettare, o un file COM rinominato.

    Controllo sequenza spazi bianchi
    Alcuni virus aggiungono una serie di spazi (o altri caratteri "bianchi",non visibili,) alla fine dell' estensione di un file con, seguita da una seconda, vera e propria estesione e risulta pericoloso. A causa della lunghezza del nome del file, l'utente non può vedere la seconda estensione, ma l'analisi euristica può scoprire questo trucco. Il valore massimo preselezionato, consentito per il numero di spazi bianchi consecutivi è cinque. Se vi sono più di cinque spazi, verrà visualizzato un messaggio di allarme.
- Sensibilità – Media (in aggiunta a quanto descritto sopra).
  - > Controllo approfondito allegati.

    Così come il controllo degli allegati di base, allarme può anche essere visualizzato se l'allegato ha una semplice estensione eseguibile (EXE, COM, BAT, ecc.) Non tutti questi file sono pericolosi e il livello di sensibilità può quindi generare più falsi positivi del solito.
- Sensibilità - Elevata. (in aggiunta a quanto descritto sopra)

> Controllo di una sezione HTML.

Alcuni virus possono sfruttare bug in alcuni programmi di posta (in particolare MS Outlook e Outlook Express) che rendono possibile l'avvio di un virus con la sola visualizzazione del messaggio in anteprima. avast! controlla se il codice HTML del messaggio contiene un tag che consente un tale trucco. Se è così, un messaggio di allarme viene visualizzato.

> Messaggi in uscita - Periodo di tempo di controllo
La maggior parte dei virus si diffondono via e-mail e sono inviati agli indirizzi memorizzati nella Rubrica di Windows. In un breve periodo di tempo, i messaggi vengono inviati a un gran numero di indirizzi, con lo stesso soggetto e/o allegato. avast! controlla il numero di messaggi in un determinato periodo di tempo e può anche controllare l'oggetto e/o gli allegati. Questi parametri possono essere impostati tutti insieme nella pagina euristica (Avanzato).

> Messaggi in uscita - Messaggi di massa
I virus possono diffondersi anche con l'invio di un solo messaggio a più destinatari. avast! quindi controlla il numero totale dei destinatari del messaggio. Il numero totale ammissibile di destinatari può essere impostato nella pagina euristica (Avanzato).

- Sensibilità - Personalizzata

  Cliccando su "Personalizza" è possibile selezionare quale delle componenti della analisi euristica qui sopra si desidera utilizzare.

  È possibile inoltre selezionare un "Controllo struttura Oggetto". Se questa opzione è selezionata, il soggetto dell'e-mail sarà controllato per un gran numero di caratteri privi di senso: ad esempio, se l'oggetto contiene la sequenza "<?*&$^*(^%#$%*_()", sarà visualizzato un allarme.

- URL permessi

  Cliccando su "URL permessi", è possibile definire qualsiasi URL considerato sicuro, che verrà ignorato dalla analisi euristica. Per aggiungere un URL, cliccare su "Aggiungi", quindi digitare manualmente il nome del URL. Per rimuovere un URL, cliccare su di esso per evidenziarlo, quindi su "Rimuovi".

- Modalità silenziosa

In questa pagina, è anche possibile specificare quali azioni devono essere intraprese se è rilevato un messaggio infetto.

Euristiche (Avanzate)

Questa pagina consente di modificare le impostazioni di analisi euristica per la posta in uscita. Le impostazioni vengono utilizzate solo quando la sensibilità "euristica" è impostata ad elevata o personalizzata (e può essere modificata solo con la sensibilità impostata su personalizzata).

- Controllo di durata

  avast! conta i messaggi in uscita nel corso di un determinato tempo. Le impostazioni predefinite prevedono 5 messaggi in 30 secondi. Ciò significa che se vengono inviati più di 5 messaggi nel giro di mezzo minuto, con lo stesso oggetto e/o contenenti lo stesso allegato, verrà visualizzato un allarme.

- Messaggi di massa.

  Rappresenta il numero di messaggi consentiti, con lo stesso oggetto e/o lo stesso allegato. Quando tale numero è superato, viene visualizzato un allarme.

- Controlla oggetto.

  Se impostato, i messaggi di massa saranno identificati in base al soggetto dell'e-mail.

- Controlla allegati.
  Se impostato, i messaggi di massa saranno identificati in base all'allegato.

- Conteggio assoluto.

  Rappresenta il numero massimo totale di destinatari dei messaggi, vale a dire gli indirizzi nei campi A, "Carbon Copy" (CC) e "Blind Carbon Copy" (BCC), preimpostata a 10. Se il numero è superato, un allarme verrà visualizzato.

3. Protezione di rete

Protezione di rete protegge il computer da attacchi di worm su Internet. Funziona in modo simile a un firewall, anche se non lo sostituisce.

Impostazioni

- Mostra messaggi allarme

  Se la casella è selezionata, apparirà un messaggio nell'angolo in basso a destra dello schermo ogni volta che è rilevato un attacco da parte di worm su internet.

- File di registro

  Se la casella è selezionata, la storia degli attacchi di worm viene registrata e visualizzata sulla pagina successiva "Ultimi attacchi"

Ultimi attacchi

In questa pagina, se la casella "File di registro" è stata selezionata nella pagina precedente, vengono visualizzati gli ultimi 10 attacchi di worm di rete. Le informazioni includono la data e l'ora dell' attacco, il tipo di attacco e l'indirizzo IP e la porta di provenienza.

4. Outlook/Exchange

Scanner

Per specificare il tipo di messaggi da controllare e se il i corpi stessi del messaggio devono essere controllati, nonché gli allegati.

Posta in arrivo

Qui è possibile specificare cosa fare se viene rilevato un messaggio infetto in entrata, per esempio, può essere consegnato, eliminato o reinviato a una diversa cartella di e-mail. È inoltre possibile specificare se inserire una nota nei messaggi puliti e/o infetti, e il formato della nota, vale a dire TXT o HTML. Qualsiasi file allegato infetti o contenuto in un messaggio è trattato secondo le impostazioni delle pagine "Archiviazione Virus" e "Avanzato".

Posta in uscita

Qui è possibile specificare se inserire una nota nei messaggi puliti, e il formato della nota, come indicato sopra. I messaggi infetti non saranno inviati. È inoltre possibile specificare se gli allegati devono essere controllati nel momento in cui sono inseriti, o inviati.

- **Firme**

  Utilizzando le firme, è possibile ridurre fortemente il numero di messaggi da controllare. Le firme sono piccoli "francobolli", allegati ai messaggi non infetti per confermare che siano privi di virus. Ogni firma contiene la data e l'ora della scansione.

  Le firme di MS Outlook/Exchange sono pienamente compatibili con quelli, ad esempio, di avast! Exchange Server Edition. Pertanto, i messaggi controllati da Exchange Server non saranno di nuovo controllati da Outlook/Exchange, rendendo così più veloce il trasferimento.

- **Inserisci le firme in un messaggio pulito**.

  Per inserire le firme nei messaggi puliti.

- **Non controllare i messaggi firmati.**

  Se questa casella è selezionata, i messaggi correttamente firmati saranno sempre affidabili e non verranno controllati, non importa di quanti anni sia vecchia la firma(a meno che non sia selezionata la casella "Ignora sempre le firme più vecchie del corrente database").

- **Fidati delle firme solo fino a...**

  Qui è possibile impostare l'"età" massima delle firme da ritenere sicure. Il valore qui impostato, potrebbe essere mascherato dall'opzione " Ignora sempre le firme più vecchie del corrente database" - vedere sotto.

- **Ignora tutte le firme (nessuna fiducia)**.

  Se la casella è selezionata, saranno controllati tutti i messaggi che contengano o meno una firma valida.

- **Ignora sempre le firme più vecchie del corrente database.**

  Se questa casella è selezionata, i messaggi che hanno una firma valida, verranno controllati se la firma è più vecchia dell'attuale archivio virus. L'opzione è utile, perchè un messaggio potrebbe contenere un virus che è

stato aggiunto recentemente all'archivio virus. Se il messaggio è fidato, non vien controllato e il virus può non essere rilevato.

Archiviazione Virus

Su questa schermata, è possibile scegliere che una copia di un allegato infetto venga salvata in una cartella specifica sullìhard disk del computer. È possibile utilizzare il pulsante Sfoglia per individuare e selezionare la cartella. Se si seleziona la casella "sovrascri files infetti", qualsiasi file con lo stesso nome verrà sostituito da uno nuovo.

Avanzato

- Modalità silenziosa

Se l'azione specificata nella pagina virus è predefinita, per esempio l'opzione interattiva, selezionando questa casella di controllo, qualsiasi file infetto verrà trasferito automaticamente al cestino virus.

Se l'azione specificata nella pagina virus è predefinita ma questa casella viene lasciata vuota, verrà visualizzata la schermata che chiede come si vuole affrontare il file infetto.

Se è selezionata qualsiasi altra azione, ovvero diversa dall'opzione interattiva, questa casella di controllo non avrà alcun effetto.

- Mostra informazioni dettagliate sullà azione in svolgimento.

  Se questa casella è selezionata, le informazioni sui file attualmente in fase di controllo verranno visualizzate nell'angolo in basso a destra dello schermo.

- Mostra l'icona sulla tray mentre controlla la posta elettronica.

  Se questa casella è selezionata, una piccola icona verrà visualizzata nella barra delle applicazioni nell'angolo in basso a destra dello schermo del computer per indicare che la scansione è in corso.

- Mostra splash screen intero mentre il provider sta caricando.

  Se questa casella è selezionata, lo splash screen di avast! verrà visualizzato ogni volta che è lanciato il provider di posta elettronica.

Infine, inserendo il vostro profilo MAPI e la password, questi verranno utilizzati per visualizzare le email nella struttura a cartelle, cliccando sul pulsante Sfoglia nella pagina di posta in entrata.

Euristiche

Le impostazioni sono le stesse per Posta elettronica

Euristiche (Avanzate)

Le impostazioni sono le stesse per Posta elettronica, ma con due opzioni aggiuntive:

- Conteggio relativo

  Rappresenta il numero consentito di destinatari di un unico messaggio, espresso in percentuale sul numero totale di indirizzi e-mail nella rubrica. Se tale percentuale viene superata, verrà visualizzato un messaggio di allarme.

- Conteggio minimo

  Rappresenta il numero minimo di destinatari effettivi, corrispondente al conteggio relativo, al di sotto del quale l'allarme non verrà visualizzato. In altre parole, se si supera il conteggio relativo, l'allarme non verrà visualizzato se il numero effettivo dei destinatari è inferiore al conteggio minimo. Esempio: conteggio relativo = 20%, conteggio minimo = 10. Se il numero di indirizzi è di 40 e un messaggio viene inviato a 9 destinatari, il conteggio relativo sarà superato, ma l'allarme non verrà visualizzato perchè il numero effettivo è inferiore al conteggio minimo.

5. Protezione P2P Shield

Programmi

In questa pagina è possibile scegliere da quali programmi i file ricevuti dovrebbero essere controllati. Alcuni programmi possono essere protetti solo su Windows NT, 2000, XP, 2003, Vista o 2008.

6. Protezione Standard

Analizzatore (di base)

In questa pagina si può decidere cosa controllare con questo modulo. Si consiglia di selezionare tutte le caselle presenti in questa pagina, per consentire l'individuazione dei più comuni tipi di virus.

Analizzatore (avanzato)

In questa pagina, è possibile scegliere altri tipi di file da sottoporre a scansione, in base alla loro estensione, o quando sono aperti, o quando vengono creati o modificati.

- Controlla i files all'apertura.

  Le estensioni dei file aggiuntivi da controllare devono essere separati da una virgola. È possibile utilizzare il carattere jolly "?" (ad esempio, se si desidera controllare tutti i files .htm e.html aperti da sottoporre a scansione, inserire o "htm", "html" basta utilizzare il jolly - "ht?"; in quest'ultimo caso, tuttavia, tutti i file con estensioni che contengono "ht", come "htt",verranno controllati).

  > Controllare sempre WSH-script files.

    Questa opzione garantisce il controllo di tutti gli script file (Windows Scripting Host).

  > Non controllare librerie di sistema.

    Le librerie di sistema fidate non saranno controllate all'apertura. Verrà eseguito solo un rapido controllo al fine di confermarne l'autenticità. Questa opzione può accelerare sensibilmente l'avvio del sistema.

- Controllare files nuovi o modificati.

  Se questa casella è selezionata, i file verranno controllati nel momento in cui vengono creati o modificati. È possibile inoltre specificare se l'azione deve essere applicata a:

  > Tutti i files, o

> Solo files con l'estensione selezionata

Se la casella "Imposta sulle estensioni predefinite" è selezionata, solo i file con estensioni generalmente considerate "pericolose" saranno controllati - cliccare su "Mostrare" per visualizzare l'elenco delle estensioni preimpostate. È inoltre possibile scegliere ulteriori estensioni da sottoporre a scansione.

Bloccaggio

In questa pagina, è possibile determinare che particolari operazioni sono bloccate per file con specifiche estensioni. Questo può essere applicato a " Imposta sulle estensioni predefinite " - cliccare su "Mostrare" per visualizzare l'elenco delle estensioni preimpostate, ma è anche possibile specificare ulteriori estensioni per le quali le operazioni devono essere bloccate.

È quindi possibile specificare ulteriormente le operazioni che devono essere bloccate per un determinato tipo di file ad esempio apertura, rinomina, cancellazione, o riformattazione.

Infine è possibile specificare cosa fare se l'operazione dovrebbe essere bloccata, ma avast! non è in grado di ottenere la conferma, ovvero se deve essere consentita o negata.

Avanzato

- Mostra Informazioni dettagliate sull-azione in svolgimento

  Se questa casella è selezionata, le informazioni sui file attualmente in fase di controllo verranno visualizzatoe nell'angolo in basso a destra dello schermo.

- Modalità silenziosa

  Se l'azione specificata nella pagina virus è l'azione predefinita, vale a dire l'opzione interattiva, ed è selezionata la modalità silenziosa, eventuali file infetti verranno trattati automaticamente in base alle seguenti regole:

  > Se è selezionata, "con risposta generale Sì (OK)", qualsiasi file infetto in allegato a un messaggio di posta elettronica verrà automaticamente eliminato.

> Se è selezionata la seconda opzione "con risposta generale No (Annulla)" tutti i files infetti verranno automaticamente trasferiti al cestino virus.

Se l'azione specificata sulla pagina virus è l'azione predefinita e questa casella viene lasciata vuota, verrà visualizzata la schermata con l'allarme virus, che chiede cosa si vuole procedere con il file infetto.

Se è selezionata qualsiasi altra azione, diversa da quella predefinita, l'opzione interattiva, selezionando questa casella non si avrà nessun cambiamento.

Infine, è possibile specificare aree specifiche da non controllare con questo particolare modulo. Si noti che le aree escluse dalla scansione di tutti i moduli non vengono visualizzate in questo elenco.

7. Protezione Web

La protezione Web funziona come un proxy server locale. Nei sistemi operativi NT (Windows NT/2000/XP/2003/Vista/2008) la protezione è completamente trasparente e di solito non è necessario regolare le impostazioni standard. Se si utilizza Windows 95/98/ME tuttavia, è necessario modificare le impostazioni in Opzioni Internet - in particolare, l'indirizzo e la porta del proxy locale, come segue:

Se utilizzate una rete locale (LAN):	Se utilizzate una connessione dial-up (modem):
Aprire Internet Explorer.	Aprire Internet Explorer.
Selezionare Strumenti, poi Opzioni Internet dal menu principale.	Selezionare Strumenti, poi Opzioni Internet dal menu principale.
Cliccare su Connessioni	Cliccare su Connessioni
Cliccare su Impostazioni LAN	Selezionare la vostra connessione dial-up dalla lista e cliccare su “Impostazioni”.
Selezionare l’ opzione “Utilizza un server proxy per le connessioni LAN”	Selezionare l’ opzione “Utilizza un server proxy per la connessione
Scrivere “localhost” nel campo Indirizzo (in alternativa, potete inserire l’ IP address 127.0.0.1, che è lo stesso del “localhost”). Inserire 12080 nel campo Porta.	Scrivere “localhost” nel campo Indirizzo (in alternativa, potete inserire l’ IP address 127.0.0.1, che è lo stesso del “localhost”). Inserire 12080 nel campo Porta.
Confermare cliccando OK.	Confermare cliccando OK.

Nota: Se si utilizzano più connessioni, è necessario impostare separatamente l'indirizzo e la porta del proxy locale per ogni connessione.

Di Base

- Abilita controllo Web

  Deselezionando questa casella, è possibile disattivare la funzione di scansione web senza alterareil blocco URL, che rimarrà attivo

- Usa il controllo intelligente del flusso

Se questa casella è selezionata, i file scaricati, sono controllati quasi in tempo reale. Parti di dati sono controllate non appena arrivano - e le seccessive vengono scaricate solo quando le parti precedenti sono verificate e prive di virus. Se questa funzione è disattivata, l'intero file sarà prima scaricato in una cartella temporanea, e poi controllato.

Le altre opzioni presenti questa pagina non sono disponibili su Windows 95, 98 e Millennium:

- Porte HTTP reindirizzate

  Questa impostazione è importante se si usa un qualche tipo di server proxy per accedere a Internet e si desidera effettuare la scansione di comunicazione tra il server e il computer. Se ci si connette a un server proxy utilizzando ad esempio la porta 3128, inserite questo numero nella casella. In caso contrario, avast! si aspetta che la comunicazione avvenga sulla porta 80 (impostazione predefinita) e tutto il resto verrà ignorato. Nota: non entrare in altre porte di HTTP (come ad esempio le porte di ICQ, DC ++, ecc.) Numeri di porta multipli devono essere separati da virgole.

- Indirizzi ignorati.

  Qui si devono inserire i nomi dei server o gli indirizzi IP che non verranno reindirizzati verso la Protezione Web. Più indirizzi devono essere separati da virgole.

- Ignora comunicazione locale.
  Se questa casella è selezionata, tutti le comunicazioni locali - vale a dire le comunicazioni tra i programmi in esecuzione sul computer, verranno ignorate

Controllo Web

In questa pagina, è possibile specificare quali file devono essere controllati quando vengono scaricati da Internet. È possibile decidere se tutti i file devono essere controllati o solo quelli con particolari estensioni. Se si sceglie quest'ultima opzione, si devono inserire le estensioni dei file da sottoporre a scansione, separati da virgole. È inoltre possibile inserire i tipi MIME di file da controllare. In entrambi i casi, possono essere utilizzati i caratteri jolly.

Eccezioni

Qui è possibile specificare gli oggetti che non saranno controllati dalla protezione Web. Questo può essere utile quando il download di un gran numero di file da una singola (fidata!) location.

- URLs da escludere

  Utilizzare il pulsante Aggiungi per inserire gli indirizzi URL da ignorare. Se si desidera bloccare solo una singola pagina, è necessario inserire il percorso completo. Ad esempio, se si aggiunge http://www.yahoo.com/index.html, solo le pagine index.html saranno escluse dalla scansione. Se si inserisce http://www.yahoo.com/*, tuttavia, le pagine che iniziano con http://www.yahoo.com non saranno controllate. Allo stesso modo, se si desidera escludere dalla scansione un particolare tipo di file, ad esempio, con estensione ".txt", è sufficiente inserire *.txt.

- MIME tipi da escludere

  Qui è possibile specificare i tipi/sottotipi MIME da escludere dalla scansione.

Blocco URL

La Protezione Web può anche essere usata per bloccare l'accesso a determinate pagine web. E' preimoostato come spento, tuttavia, può essere utilizzato per impedire l'accesso a pagine web "inadatte" (contenenti per esempio pornografia, software illegali, ecc..) Se per tale blocco pagina è richiesto il contributo del web browser, apparirà un messaggio annunciando che l'accesso alla pagina è stato bloccato da avast!.

La casella "Abilita il blocco URL" deve prima essere selezionate e poi si possono inserire gli indirizzi da bloccare, cliccando sul pulsante "Aggiungi" e poi inserendo gli URL. I caratteri jolly (? e *) possono essere usati, per esempio, se si entra in http://www.penthouse.com/*. Le pagine che iniziano con http://www.penthouse.com non saranno quindi visualizzate.

L'entrata degli indirizzi URL sarà completata in base alle seguenti regole:

Se l'indirizzo non inizia con http:// o con caratteri jolly * oppure ?, avast! aggiunge il prefisso http:// all'inizio dell' indirizzo e un asterisco alla fine. Quindi, se si entra in www.yahoo.com, verrà modificato con http://www.yahoo.com*.

Avanzato

- Mostra Informazioni dettagliate sullàazione in svolgimento

  Se questa casella è selezionata, le informazioni sui file attualmente in fase di controllo verranno visualizzate nell'angolo in basso a destra dello schermo.

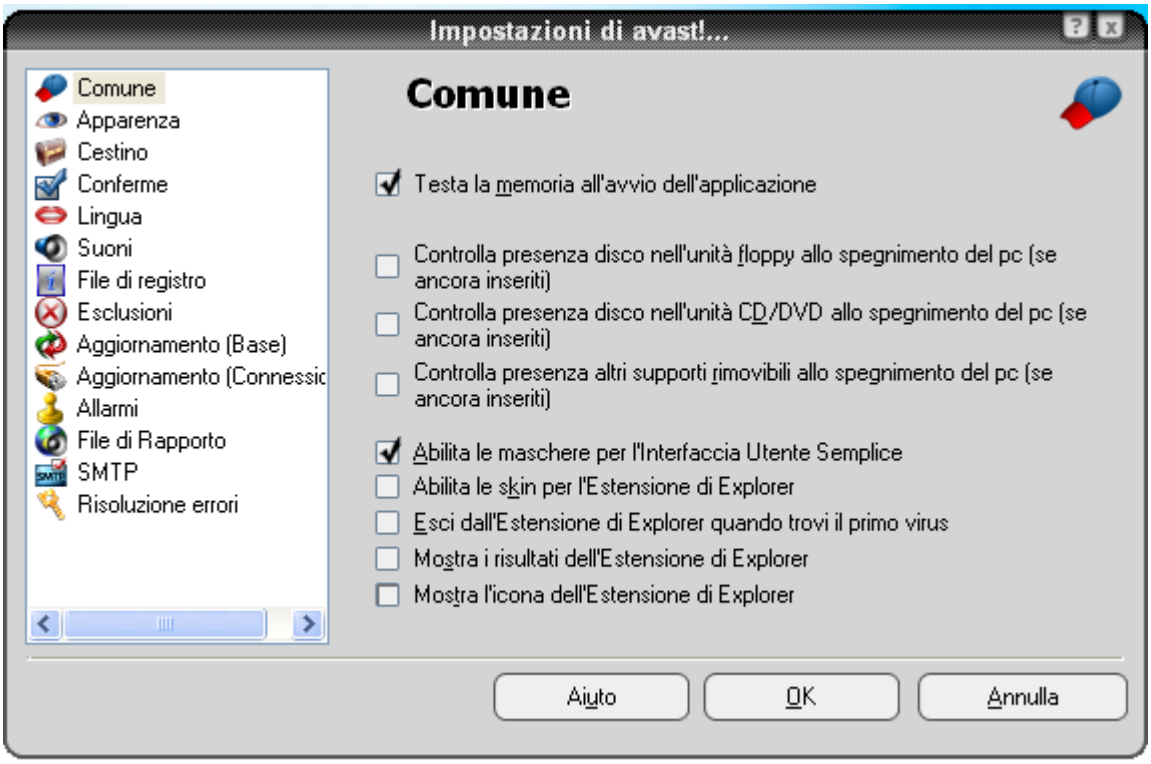
- Modalità silenziosa

  Se questa casella è selezionata, la connessione verrà terminata ogni volta che ilprogramma trova un virus

Altre impostazioni di avast!

Molte altre parti del programma avast! possono essere modificate secondo con le proprie esigenze o preferenze. Alcune di queste impostazioni sono già state descritte nelle sezioni precedenti.

Se si utilizza l'interfaccia semplice e si apre il **menu delle opzioni** (vedere **pagina 30**) e cliccando su "Impostazioni" verrà visualizzata la seguente schermata. Se si utilizza l'interfaccia utente avanzata, cliccando su "Impostazioni" apparirà un' ulteriore opzione - "Interfaccia avanzata". Le diverse impostazioni possono essere cambiate cliccando sulla voce corrispondente sul lato sinistro dello schermo:



Impostazioni "Comune"

In questa schermata è possibile specificare quali controlli devono essere effettuati in fase di avvio o quando si spegne il computer. Qui è anche possibile modificare l'aspetto del programma selezionando o meno la casella "Abilita le skin ...".

Estensione Explorer

Le ultime quattro caselle di controllo sullo schermo si riferiscono all' "estensione Explorer ". Questo permette di controllare la scansione di ogni singolo file: basta cliccare sul tasto destro del mouse su di esso e selezionare l'opzione "Controlla <nomefile>". Se l'ultima casella è selezionata, questa opzione presenterà l'icona sferica con la "a" accanto.

Apparenza

Cliccando su "Apparenza" è possibile decidere se visualizzare l'icona sferica con la "a" l'avast! nell'angolo in basso a destra dello schermo e anche se deve essere animata (in movimento), mentre è in corso la scansione.

È possibile aggiungere un effetto traslucido per la comparsa della console di avast!. Tali modifiche saranno attivate dopo il riavvio del computer.

Conferme

Questa schermata consente di ricevere conferma quando si selezionano alcune operazioni.

Queste conferme sono una caratteristica di sicurezza di avast! antivirus perchè permettono di cancellare un'operazione selezionata per errore.

Se non si desidera ricevere un particolare messaggio di conferma, basta lasciare vuota la casella di controllo adeguata. Tuttavia, se la conferma di un'operazione non è selezionata, le operazioni saranno avviate non appena l'azione corrispondente è selezionata, senza la possibilità di cancellarle.

Le seguenti conferme sono attivate come standard, ma possono essere disattivate lasciando vuote la casella di controllo corrispondente:

- ***Chiedi prima di chiudere l'interfaccia utente semplice durante la scansione***
  Se si chiude il programma mentre una scansione è in corso, la scansione verrà automaticamente interrotta.

- ***Chiedi se conservare le impostazioni cambiando lo status del provider***
  Questo messaggio verrà visualizzato se si decide di "arrestare" uno qualsiasi dei distinti moduli di protezione locale. Se attivate l'opzione, il particolare modulo rimarrà disabilitato fino a quando non viene manualmente riattivato. Se la casella rimane vuota, sarà riattivato la prossima volta che si riavvia il computer.

- ***Chiedi prima di fermare la protezione all'accesso***
  Questo messaggio verrà visualizzato se si decide di "arrestare" residenti per la protezione locale nel suo complesso (o all'avvio) - vedere a **pagina 26**. Se attivate l'opzione, la protezione residente verrà disattivata, ma sarà automaticamente riattivata la prossima volta che si riavvia il computer.

- ***Chiedere conferma prima di eliminare files dal cestino***
  Se questa casella è selezionata, il programma chiedere sempre conferma prima di eliminare qualsiasi file. Questo per impedire che i files vengano eliminati accidentalmente.

- ***Mostra messaggio quando i risultati sono stati processati con successo***

Questo messaggio conferma il completamento di una qualsiasi operazione selezionata in relazione ad un determinato file. Ad esempio eliminazione, spostamento file nel cestino virus, ecc...

- ***Mostra messaggio in caso di errore nel processare i risultati***
  Questo messaggio vi dice che l'operazione selezionata in relazione ad un file specifico potrebbe non essere effettuata.

- ***Mostra messaggio se utilizzo un vecchio file VPS***
  Questo messaggio Questo è il dovere di avvisa che l'archivio virus non è aggiornato. Per garantire la massima protezione al vostro sistema, l'archivio virus deve essere aggiornato regolarmente - vedere **pagina 43**

- ***Versione BETA attenzione***
  Questo messaggio avvisa che la versione del programma che si sta utilizzando è ancora nella fase BETA (test).

- ***Mostra messaggio quando un rapporto di errore viene inviato con successo***

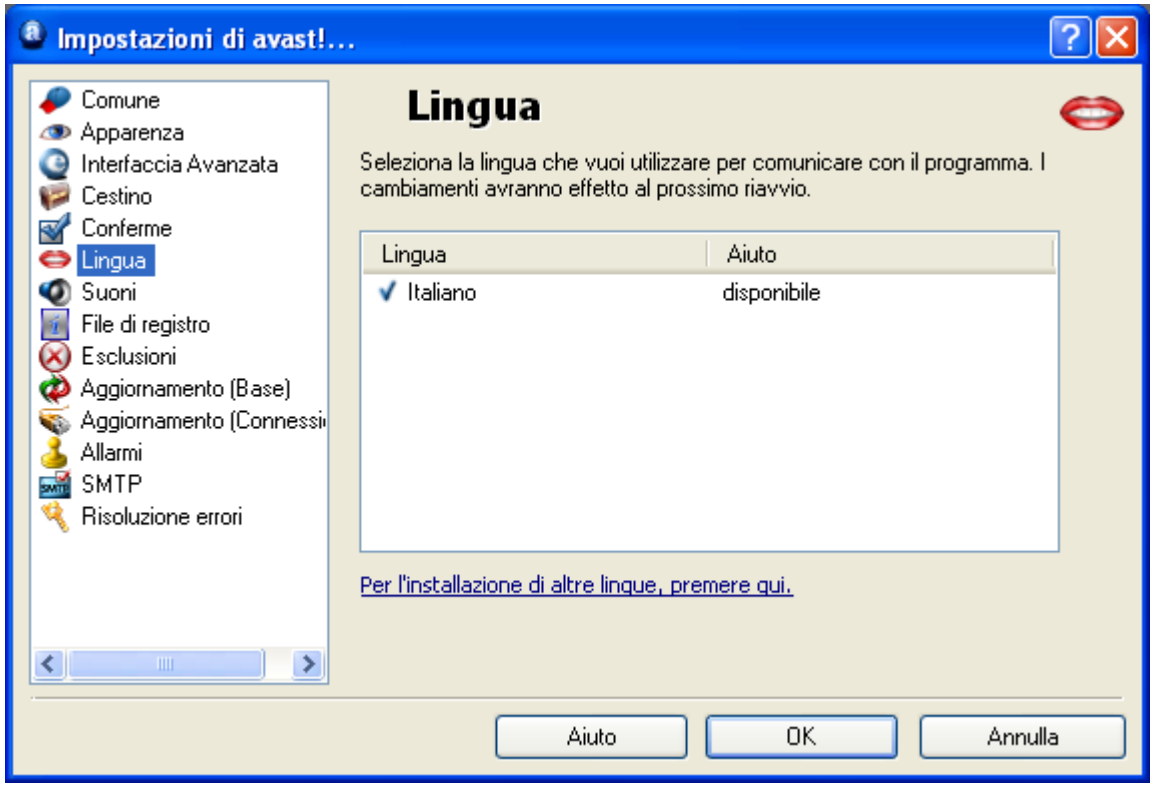
- ***Mostra la finestra di stato del cestino se l'azione è terminata OK***
  Se questa casella è selezionata, verrà visualizzato un messaggio per confermare che l'operazione selezionata è stato correttamente elaborata.

- ***Mostra messaggio quando i risultati OK sono abilitati durante la configurazione del task.***
  Quando questa casella è selezionata, verrà visualizzato un messaggio di avviso se si specifica che "OK file" deve essere incluso nella scansione dei risultati. Nota, l'opzione è valida solo alla creazione delle operazioni nell'interfaccia utente avanzata.

- ***Cancellazione dei files con estensione pericolosa***
  Questo messaggio avvisa che non c'è la certezza di poter eliminare il file in questione perchè questo tipo di file normalmente contiene dati importanti.

Scelta della lingua del programma

Se si desidera cambiare la lingua del programma, cliccare su "Lingua" , e verrà visualizzata la seguente schermata:



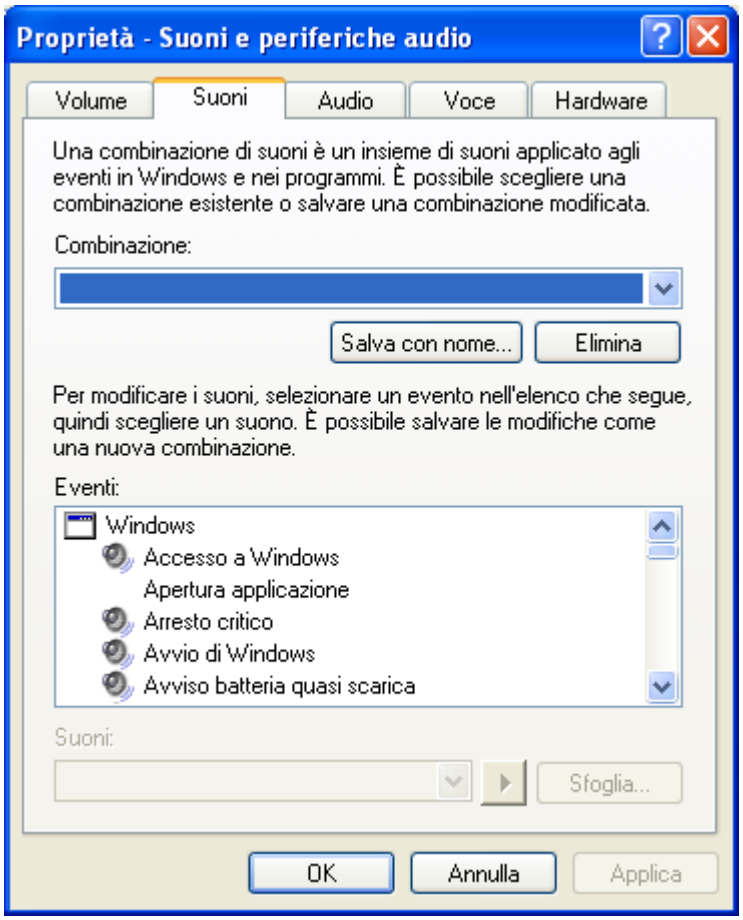
Se la lingua è indicata come "disponibile" nel riquadro a destra, clic su di essa per selezionarlo, quindi su "OK". Si dovrà chiudere il programma e la prossima volta che si avvia, la lingua verrà modificata automaticamente.

Se la lingua richiesta non è indicato come "disponibile", basta cliccare su "Per l'installazione di altre lingue premere qui." Selezionare quindi la lingua desiderata. Cliccare sul pulsante "Avanti" e il file del programma verrà installato. Al termine, cliccare su "Fine"
Sarà ora possibile selezionare la lingua desiderata.

Suoni

In questa sezione è possibile regolare le impostazioni audio del programma o si possono spegnere completamente tutti i suoni.

Attraverso "Impostazioni", visualizzerete una schermata dove sarà possibile regolare le impostazioni audio per tutti i programmi di Windows. Nella metà inferiore dello schermo, è presente una sezione denominata "Eventi" - vedere sotto.



A metà dell'elenco, si trovano le opzioni per i suoni di l'avast! antivirus. Se si desidera assegnare un nuovo suono a un evento, basta cliccare sul relativo evento e poi su "Sfoglia". Dalla lista delle opzioni disponibili, selezionare il suono desiderato e confermare su "OK".

Si torna quindi alla tabella mostrata sopra dove si dovrà cliccare su "Applica" e poi "OK".

Questo vi porterà indietro alla schermata principale "Suoni". Per terminare cliccare su "OK".

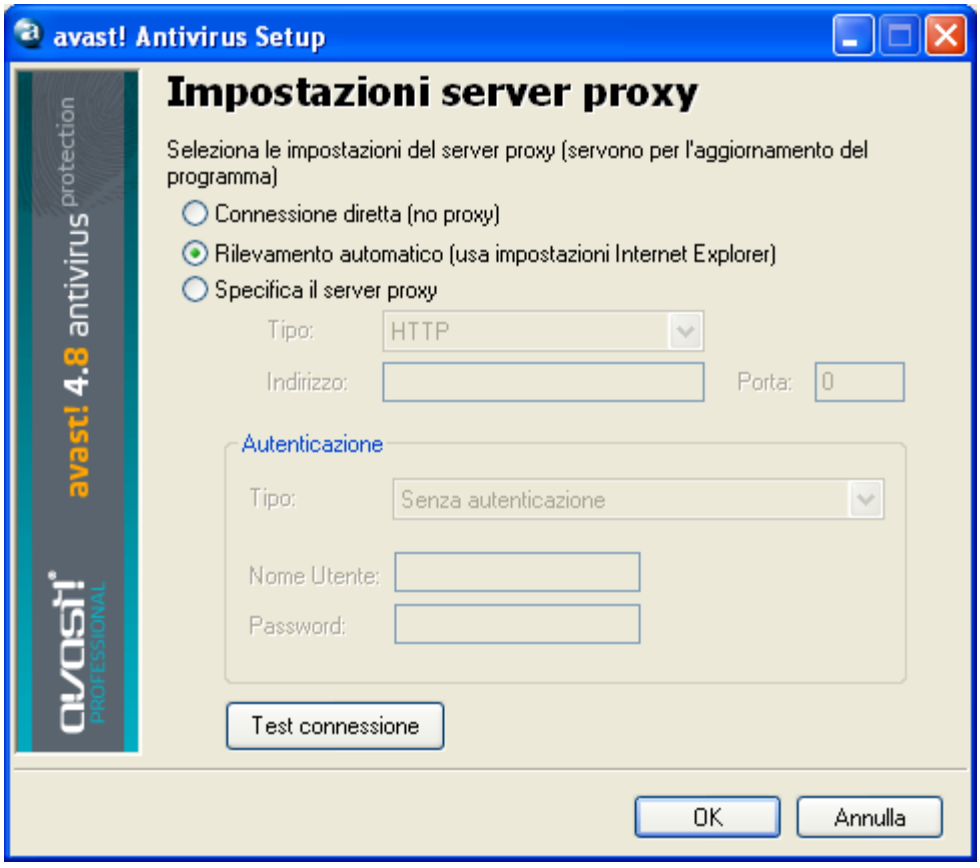
Aggiornamento (Connessioni)

Sulla schermata successiva, è possibile specificare il tipo di connessione a Internet selezionando l'apposita casella:

- Mi connetto a Internet utilizzando una connessione di tipo dial-up, o
- Il computer è costantemente connesso a Internet

L'opzione permette di ottimizzare il modo in cui avast! cerca gli aggiornamenti e di rendere più affidabile il processo.

Dopo aver specificato il tipo di connessione, cliccare sul pulsante "Proxy". Si aprirà una nuova finestra nella quale sarà possibile inserire le impostazioni del server proxy. Le impostazioni del server proxy sono importanti quando avast! deve accedere a Internet, ad esempio, durante il processo di aggiornamento.



- Se ci si connette direttamente a Internet (cioè non attraverso un proxy), di solito per gli utenti dial-up, selezionare l'opzione "Connessione diretta (no proxy)"

  Se non siete sicuri di utilizzare un server proxy, o quale server, selezionare

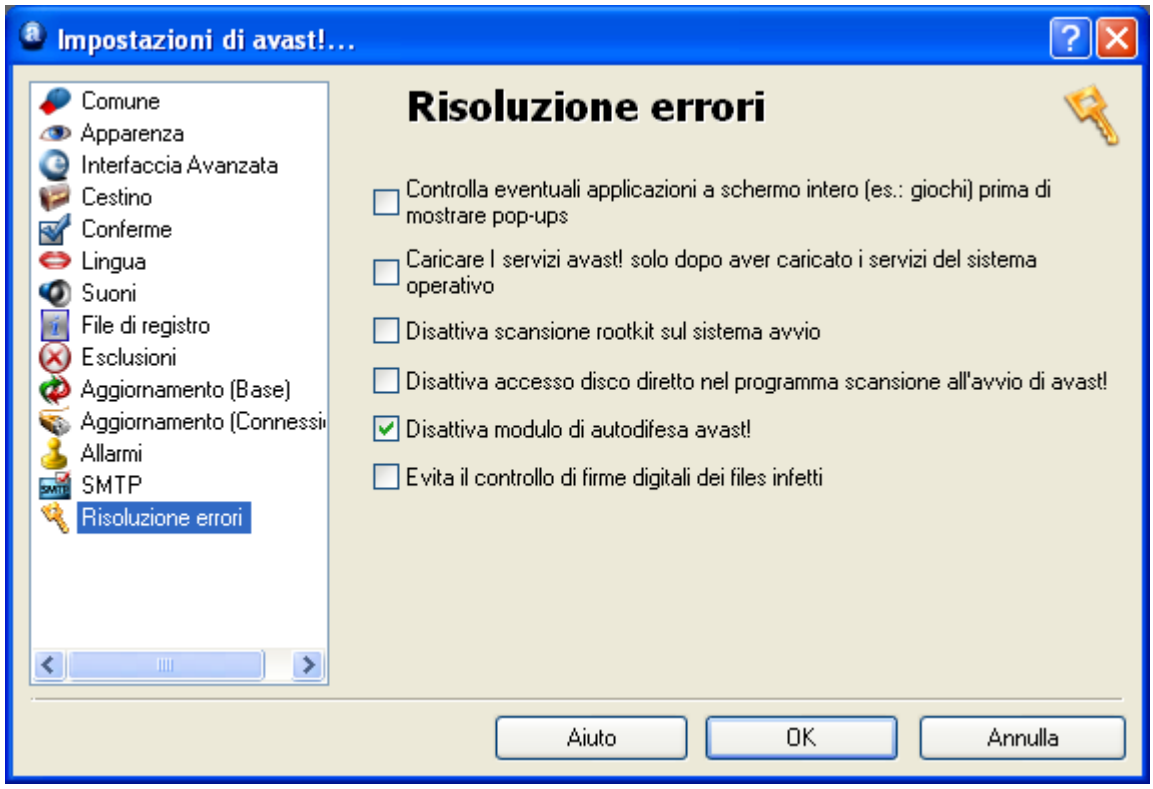
"Rilevamento automatico (usa impostazioni Internet Explorer)", o chiedete al vostro Internet provider o all'amministratore di rete.

Se si conosce l'indirizzo e la porta del server proxy, selezionare "Specifica il server proxy" e inserite i dettagli proxy richiesti come segue:

- **Tipo**. O HTTP o SOCKS4
- **Indirizzo**. Inserire l'indirizzo del vostro server proxy.
- **Porta**. Inserire la porta che usa il vostro server proxy.
- **Autenticazione**. Specificare se l'accesso ad Internet attraverso il vostro server proxy richiede l'autenticazione utente e di che tipo.
- **Nome utente e password**. Da inserire se è richiesta l'autenticazione.

Infine, cliccate su "Test connessione" per verificare se la connessione a Internet (in base alle impostazioni di cui sopra) funziona.

Risoluzione errori



Cambiare le impostazioni in questa pagina può aiutare a risolvere alcuni problemi specifici. Tuttavia, queste impostazioni non dovrebbero essere modificate senza un valido motivo. In caso di dubbio, si prega di contattare avast!.

Controlla eventuali applicazioni a schermo intero (es. giochi), prima di mostrare pop-ups.
Secondo la vostro configurazione di avast!, possono essere visualizzati vari messaggi quando il computer è in esecuzione (ad esempio, quando l'archivio virus è stato aggiornato, quando un' e-mail in entrata viene controllata, ecc.) Normalmente, i messaggi vengono visualizzati quando l' evento corrispondente si verifica. Ciò, tuttavia, può causare l'interruzione di applicazioni a schermo pieno(ad esempio giochi) - Windows passa dalla modalità a tutto schermo alla modalità finestra normale quando appare il messaggio. Se si seleziona questa opzione, avast! cercherà di individuare la presenza di eventuali applicazioni in esecuzione a pieno schermo, prima di visualizzare un messaggio. In presenza di un'applicazione di quato tipo, avast! non visualizza il messaggio.

Caricare i Servizi avast! solo dopo aver caricato i servizi del sistema operativo.
avast! è di solito attivato molto presto durante processo di avvio. Occasionalmente, ciò può causare problemi quando sono in avvio altri servizi di sistema - come il blocco temporaneo (per pochi secondi o minuti) del sistema subito dopo l'avvio. Questa opzione permette di ritardare l'avvio di avast! di per permettere il caricamento completo degli altri servizi.

Disattiva scansione rootkit sul sistema avvio.
avast! controlla la presenza di eventuali rootkit ogni volta che si avvia il sistema operativo. Selezionate questa casella se desiderate disattivare questo tipo di scansione.

Disattiva accesso disco diretto nel programma scansione all'avvio di avast!.
Durante la scansione all'avvio, avast! utilizza un metodo speciale di accesso al disco, che permette al programma di rilevare anche i virus che nascondono i propri file. Qui è possibile disattivare questa funzione - avast! utilizzerà il metodo standard di accesso al disco.

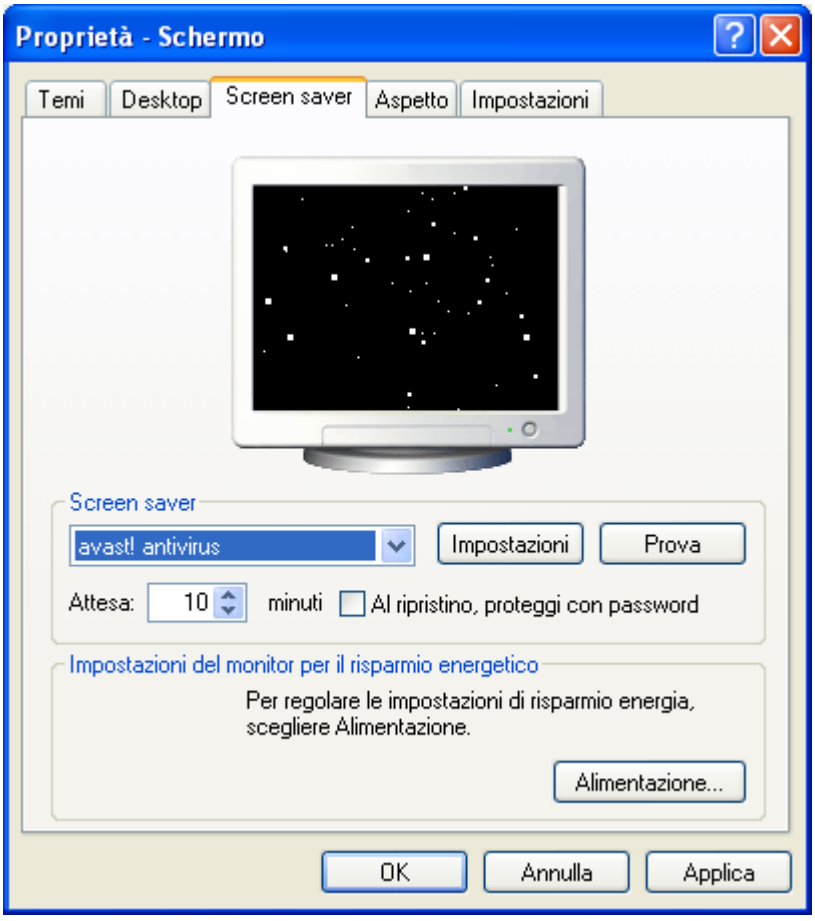
Disattiva modulo di autodifesa avast!.
Alcuni virus sono in grado di disattivare il software antivirus e chiudere i processi, eliminando o modificando files di vitale importanza. avast! contiene delle caratteristiche di auto-difesa che bloccano questi attacchi. Per disabilitare questo modulo di auto-difesa, selezionare questa casella.

Evita il controllo di firme digitali dei files infetti.
Per evitare segnalazioni di falsi positivi, avast! controlla i files infetti con firme digitali. Se un file viene rilevato come infetto, ma contiene anche una firma digitale proveniente da un' autorità di fiducia (ad esempio Microsoft), è probabile che si tratti di un falso positivo - avast! quindi lo ignorerà. Selezionando questa casella si disattiverà il controllo supplementare - avast! riferirà tutte le infezioni che trova.

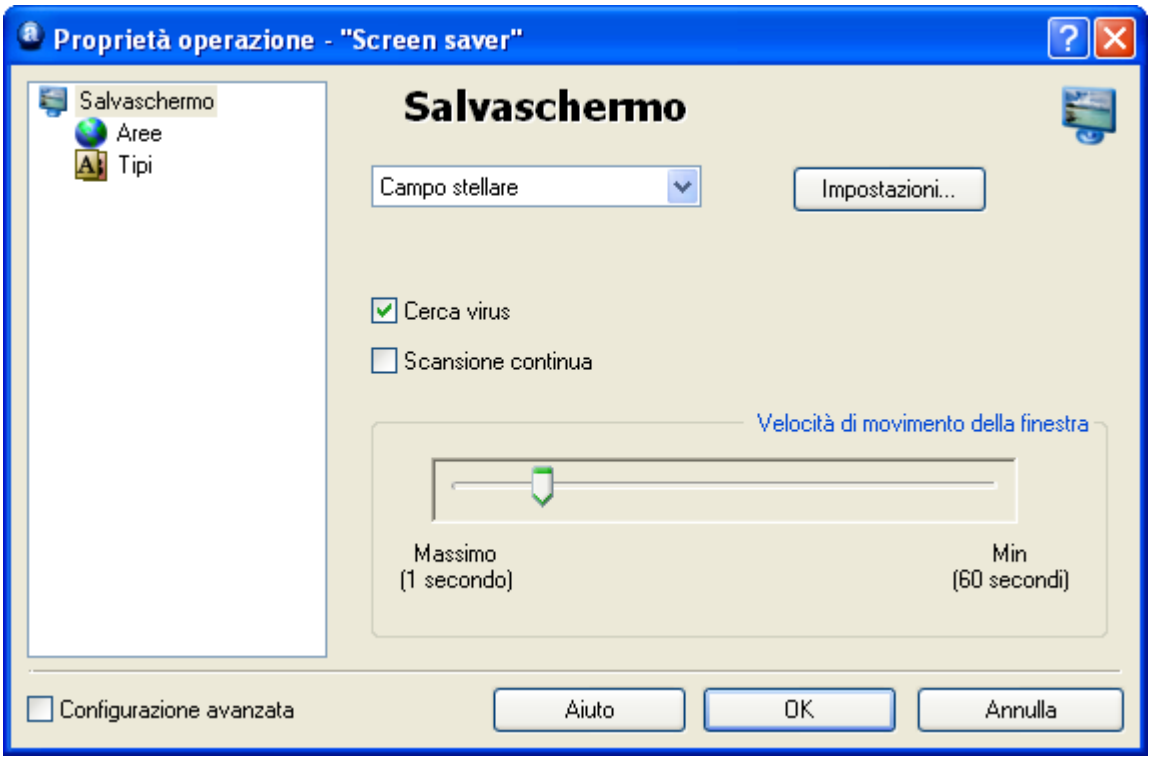
Come attivare lo screen saver dell' antivirus avast!

L' antivirus avast! è in grado di eseguire la scansione del computer per i potenziali infezioni da virus durante i periodi in cui il computer non è in uso e lo screen saver viene attivato. Durante questo tempo, una piccola finestra viene visualizzata all'interno dello screen saver, che informa l'utente sullo stato della scansione.

Per attivare lo screen saver di avast!, clic sul pulsante "Start" nell'angolo in basso a sinistra dello schermo e selezionare "Impostazioni". Quindi "Pannello di controllo" e doppio clic su "Visualizza" e "Screen saver" Cliccare su "avast! antivirus ". Nella casella sottostante, è anche possibile cambiare il numero di minuti dopo i quali verrà attivato lo screen saver, e se è necessario immettere la password per continuare.



Cliccando su "Impostazioni" in questa schermata, potete selezionare il normale screen saver dentro verrà visualizzata la finestra di messaggio di avast! che mostra lo stato della scansione - vedere la pagina successiva.



Se volete controllare il computer ogni volta che lo screen saver è attivo, selezionate la casella "Cerca virus". Se questa casella non è selezionata, lo screen saver funzionerà solo come un normale screen saver.

Selezionando la casella "Scansione continua" farà in modo che la scansione sia effettuata più di una volta e che tutti i settori siano controllati.

Modifica della velocità di movimento della finestra interesserà la frequenza di cambiamento della casella dello stato di scansione sullo schermo.

Cliccando su "Impostazioni" potrete regolare di nuovo lo screen saver.

Cliccando su "**Aree**" ", è possibile specificare quali aree del vostro computer devono essere controllati. Le aree da sottoporre a scansione includono automaticamente "Tutti i dischi rigidi". Se non si desidera controllare tutti i dischi rigidi, basta cliccarci sopra e poi su "Rimuovi". È quindi possibile specificare le aree da sottoporre a scansione facendo cliccando su "Sfoglia" e selezionando con le apposite caselle l'area scelta. Cliccando su "Aggiungi" è possibile selezionare un certo numero di aree pre-definite .

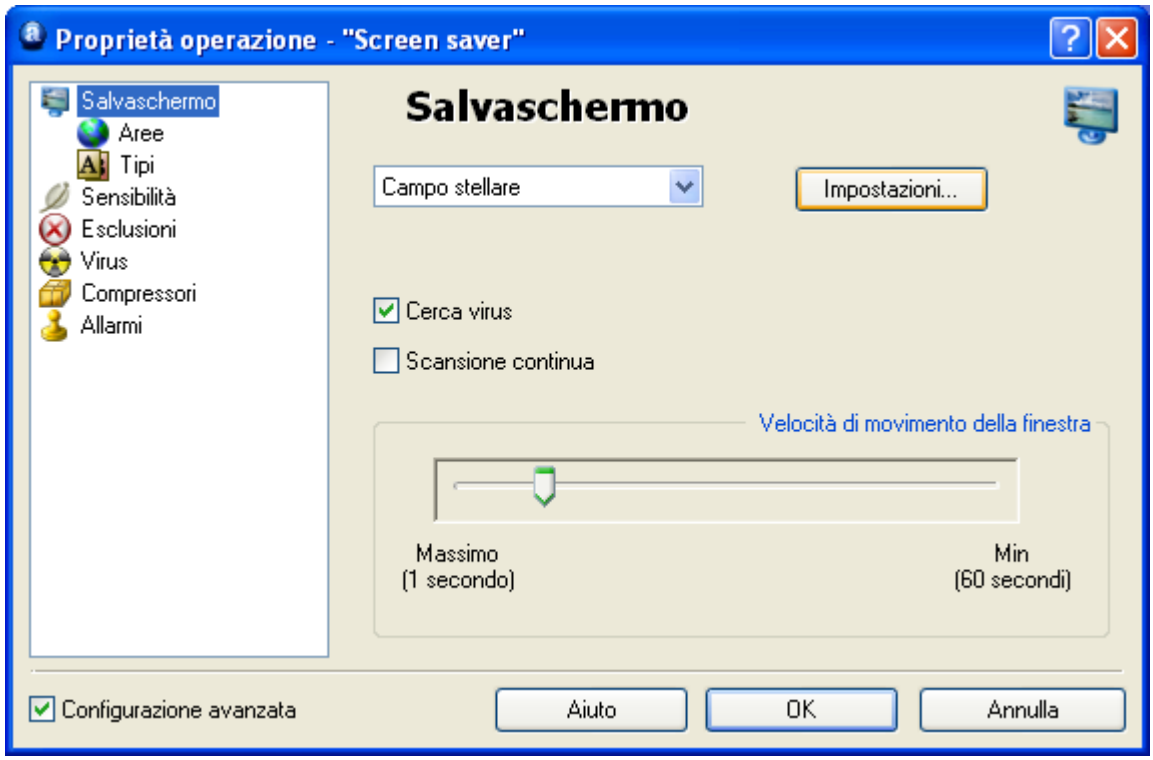
Una volta selezionate le aree da controllare, cliccare su "**Tipi**" ", e sarà possibile specificare quali file devono essere controllati. I files possono essere riconosciuti come sospetti a seconda del loro contenuto, o in base alla loro estensione.

Se si sceglie la scansione “basata sul contenuto”, è possibile specificare tutti i file da controllare con la casella "Esamina tutti i file". Se si seleziona questa casella, anche i file che di solito non contengono virus, come file contenenti immagini, saranno controllati. Se si lascia questa casella vuota, questi file non verranno controllati e nei risultati finali saranno riportati come "file saltati ".

Se si seleziona una scansione basata sull’estensione , è necessario specificare le estensioni da ritenere sospette.

Per eseguire la scansione dei file basata su uno o più estensioni specifiche, cliccare su "Sfoglia". Apparirà un elenco delle estensioni. Se si riesce a trovare l'estensione che si desidera aggiungere, cliccare sulla stessa estensione e premere "OK" per aggiungerlo alla lista. Se l'estensione che si desidera aggiungere non è nella lista, è possibile aggiungerla manualmente. Cliccare su "Aggiungi" quindi digitare l'estensione del file che si desidera aggiungere. Per aggiungere un'altra estensione, cliccare di nuovo su "Aggiungi". Se si vuole rimuovere un estensione dalla lista, è sufficiente cliccare su di essa per evidenziarla e poi su "Rimuovi".

Se la casella "Esamine le estensioni predefinite" è selezionata, le estensioni di solito ritenute "pericolose" verranno automaticamente controllate.
Se si seleziona la casella "Configurazione avanzata", è possibile specificare una serie di impostazioni aggiuntive come di seguito:



- ***Sensibilità***

Selezionando la casella "Controlla i file per intero (l'operazione può essere molto lenta per file di grandi dimensioni)", non solo le parti più frequentemente colpite dal virus, ma l'intero file verrà controllato. La maggior parte dei virus si trovano o all'inizio, o alla fine di un file. Selezionando questa casella la scansione sarà più accurata, ma anche più lenta.

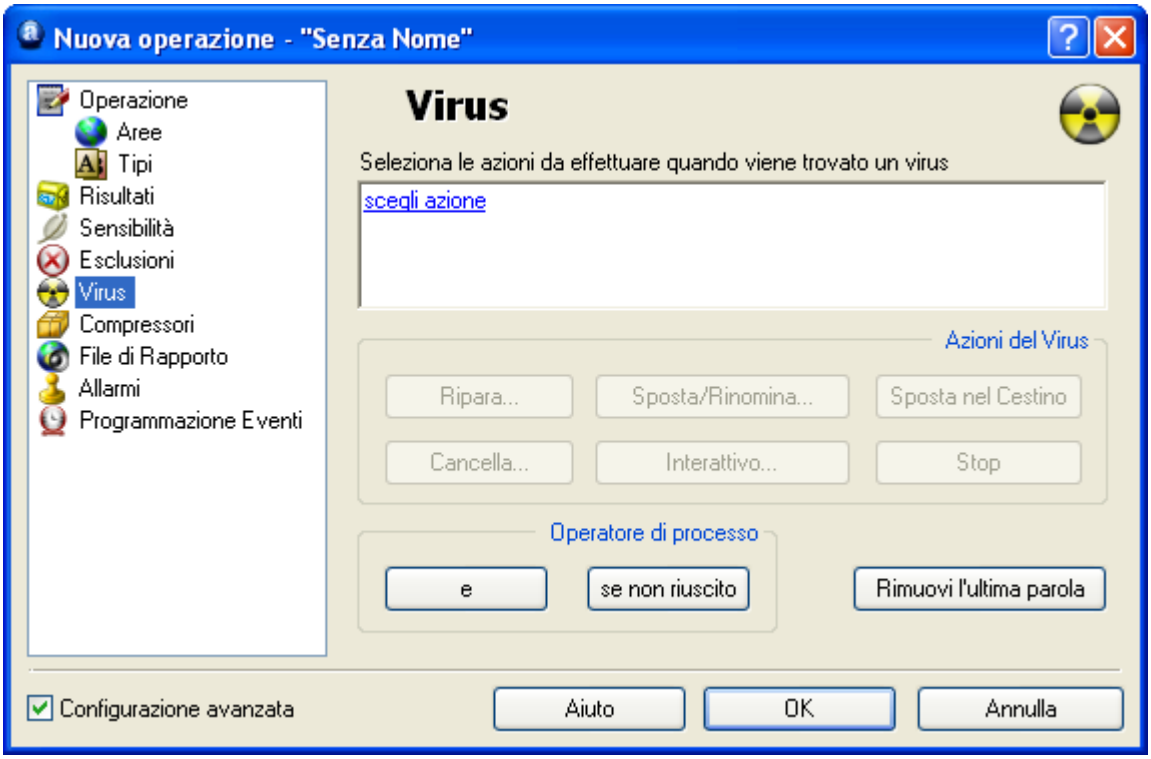
Selezionando la casella "Ignora virus bersaglio" avrà come conseguenza il file verrà controllato rispetto a tutti i virus dell'archivio. Se la casella rimane vuota il controllo avverrà solo nei confronti deii virus che colpiscono un determinato tipo di file. Ad esempio, il programma non cercherà i virus che infettano i file con l'estensione ". Exe" nei files con estensione ". Com".

- ***Esclusioni***

Qui è possibile escludere determinati file o cartelle dalla scansione. Questo funziona esattamente come descritto a **pagina 47**, con l'eccezione che qui, le esclusioni impostate sono valide solo per l'operazione specifica. File o cartelle non presenti nel menu "Operazioni" saranno automaticamente esclusi da tutte le scansioni. I file esclusi, saranno riportati nei risultati come "file saltati"

- ***Virus***

Cliccando su "Virus" appare la seguente schermata:



In questa schermata, è possibile specificare quali azioni devono essere intraprese quando è stato rilevato un virus. L'opzione predefinita è "scegli l'azione". Questa è la l'opzione "interattiva".

Se si lascia l'opzione preselezionata, ogni volta che un file sospetto viene rilevato, verrà presentato un elenco di possibili opzioni. Questo significa che è possibile specificare quali azioni intraprendere individualmente per ciascun file sospetto.

Cliccando su "Scegli azione" si visualizzano le opzioni che saranno presentate ogni volta che un file sospetto viene rilevato: Cancella, ripara, Manda nel cestino, Sposta/Rinomina, o Stop. Solo le opzioni con la casella selezionata saranno disponibili. Se una qualsiasi opzione non è selezionata, non sarà presentata come opzione disponibile quando un file sospetto viene rilevato.
Queste opzioni sono descritte a **pagina 37** nella sezione "Cosa fare se viene rilevato un virus".

Selezionando"Scegli azione" , se è stato rilevato un virus, la scansione viene sospesa, fino a quando non vengono specificate le misure da adottare. Pertanto, si raccomanda di selezionare una delle altre azioni, come ad esempio "Manda nel cestino", specialmente se le operazioni sono effettuate in automatico in un momento in cui siete lontani dal computer.

Per selezionare un'azione diversa, cliccare su "Rimuovi l'ultima parola". L'azione predefinita sarà cancellata e le sei possibili azioni saranno evidenziate nel centro dello schermo. L'azione selezionata azione sarà poi applicata a tutti i file sospetti che vengono rilevati. Per rimuoverla, è sufficiente cliccare di nuovo su "Rimuovi l'ultima parola".

Le prime quattro azioni sono descritte in dettaglio a **pagina 37**. Cliccando su "Interattivo" si inserisce automaticamente "scegliere l'azione". Cliccando poi su stop, la scansione verrà interrotta non appena un file sospetto viene rilevato.

È possibile selezionare più di una azione, utilizzando il pulsante "e". Ad esempio, è possibile specificare che eventuali file infetti vengano riparati e spostati in un'altra posizione: "Ripara" poi "e", quindi" Sposta/Rinomina".

E' inoltre possibile scegliere azioni alternative che dovrebbero essere prese se la prima scelta dovesse fallire. Ad esempio, è possibile selezionare "Ripara", come azione preferita, ma cliccando su "Se non riuscito" e "Manda nel cestino" si ha la certezza che tutti i file che non possono essere riparati vengano spostati nel cestino virus - vedere **pagina 57** .

Nota - se si seleziona "Cancella", si dovrà specificare se il file deve essere eliminato in modo permanente (azione predefinita), o semplicemente spostato nel Cestino. Se si seleziona "Cancella file(s) definitivamente", si potrà anche selezionare "Se necessario, cancella file (s) al prossimo riavvio".

- ***Compressori***

In questa pagina è possibile selezionare il controllo dei file compressi. L'impostazione predefinita vale solo per i files auto-estraibili. È possibile specificare ulteriori formati, anche se quest'operazione rallenta la scansione. Con l'opzione "Tutti i formati" il controllo avverrà per tutti i file.

- ***Allarmi***

Gli allarmi possono essere generali, ovvero inviati ogni volta che un virus è stato rilevato, oppure generati solo quando è stato rilevato un virus in una operazione particolare.

Gli allarmi che possono essere aggiunti all'operazione, sono indicati nella sezione "Allarmi disponibili".
Gli allarmi generale vengono creati cliccando su "Impostazioni" e "Allarmi", come descritto a **pagina 52**, ma allarmi creati in questo modo non possono essere collegati al salvaschermo.

Se la segnalazione che si desidera aggiungere è presente, basta evidenziarla e poi cliccare su "→". L'operazione sposterà l'allarme su "Allarmi usati" casella, collegandolo in questo modo ad una operazione.

Se l'allarme che si desidera aggiungere non viene visualizzato, cliccare su "Nuovo".

È possibile assegnare un nome all'allarme, per esempio, un nome che lo collega all'operazione con la possibilità di aggiungere anche dei commenti. La segnalazione viene creata esattamente come descritto a **pagina 52**

Dopo aver creato il nuovo allarme, cliccare su OK e sarà aggiunto automaticamente alla lista "Allarmi usati".

Per rimuovere un allarme dalla lista "Allarmi usati" basta cliccare su di esso per evidenziarlo, quindi su "←" che vi porta indietro ad "Allarmi disponibili".

Per modificare o eliminare un allarme, cliccare su "Modifica" o "Cancella" dopo aver selezionato l'allarme stesso.

Se avete bisogno di creare un allarme SMTP, non dimenticate di inserire anche i dettagli SMTP, cliccando sul pulsante "Impostazioni" e "SMTP".

Si noti che gli avvisi legati al salvaschermo, saranno inviati se un virus è stato rilevato da quest'ltimo. Questi non saranno inviati se il virus è stato rilevato da un modulo differente. Se si desidera ricevere un allarme ogni volta che è stato

rilevato un virus da qualsiasi modulo, si deve creare un allarme generale, come descritto a **pagina 52**
Per confermare tutte le impostazioni, cliccare su "OK", quindi su "Applica" e poi di nuovo "OK".
La prossima volta che lo screensaver è attivo, sarà effettuata la scansione antivirus.

Come effettuare l' "upgrade" ad avast! Professional Edition

L'upgrade da Home Edition a Professional Edition è molto semplice.

Non è necessario disinstallare la versione attuale del programma così come non sono necessario ulteriori download. Dovete solo acquistare Professional Edition, per ottenere la chiave di licenza ed inserirla nel programma attuale. Le altre componenti verranno scaricate automaticamente e il programma verrà aggiornato immediatamente alla versione Professional.
La chiave di licenza può essere acquistata per 12, 24, o 36 mesi – basta visitare **www.avast.com**e cliccare su "Acquisto".

Come disinstallare l'antivirus avast!

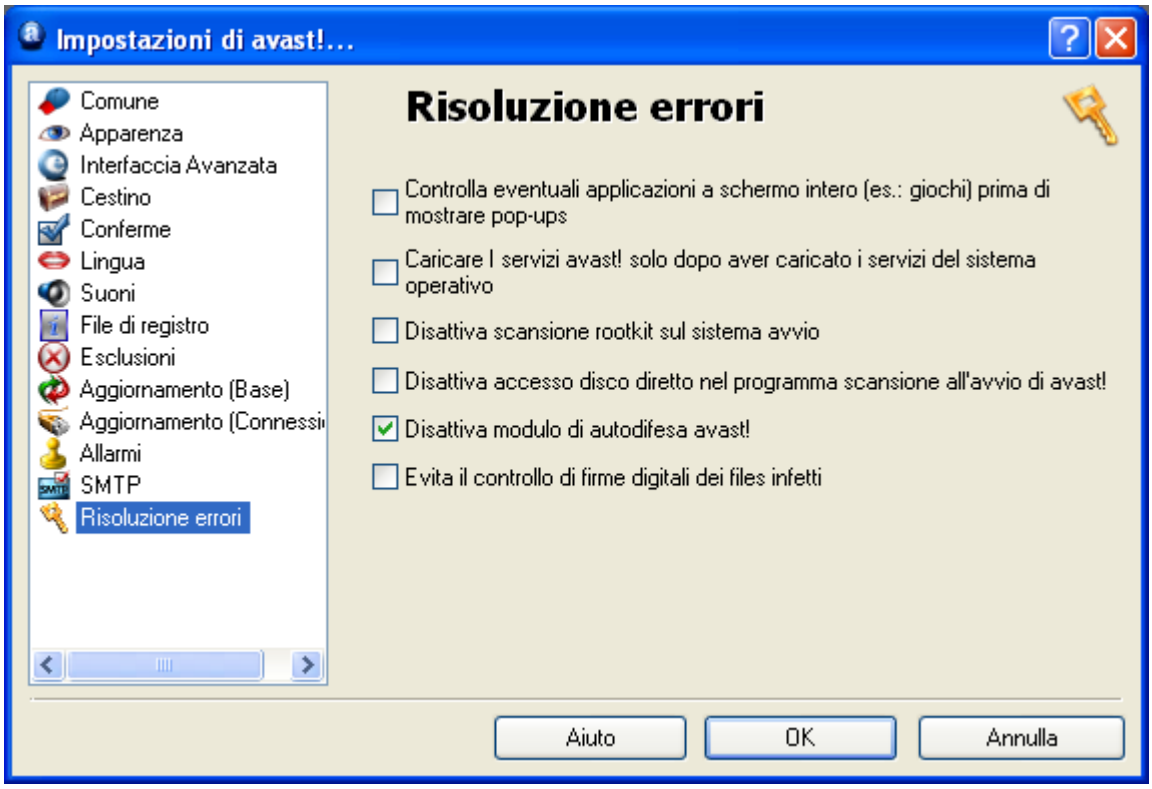
Alcuni virus sono progettati per disattivare i software antivirus sul computer. Per questo avast! antivirus possiede un forte modulo di auto-difesa (SD) che impedisce di essere modificato o disattivato da tale virus. Per questo potrebbe essere più difficile rimuovere avast! rispetto alle precedenti versioni. Al fine di rimuovere avast!, è indispensabile seguire la corretta procedura.

Prima di tentare di disinstallare l'antivirus avast!, si consiglia di chiudere tutte le altre applicazioni in esecuzione sul computer. Per disinstallare il programma la procedura è la seguente.

1. Disattivare il modulo di autodifesa

- Cliccare con il tasto destro del mouse sull'icona di avast! in basso a destra dello schermo del computer e dalle opzioni del menu, selezionare "Impostazioni Programma".

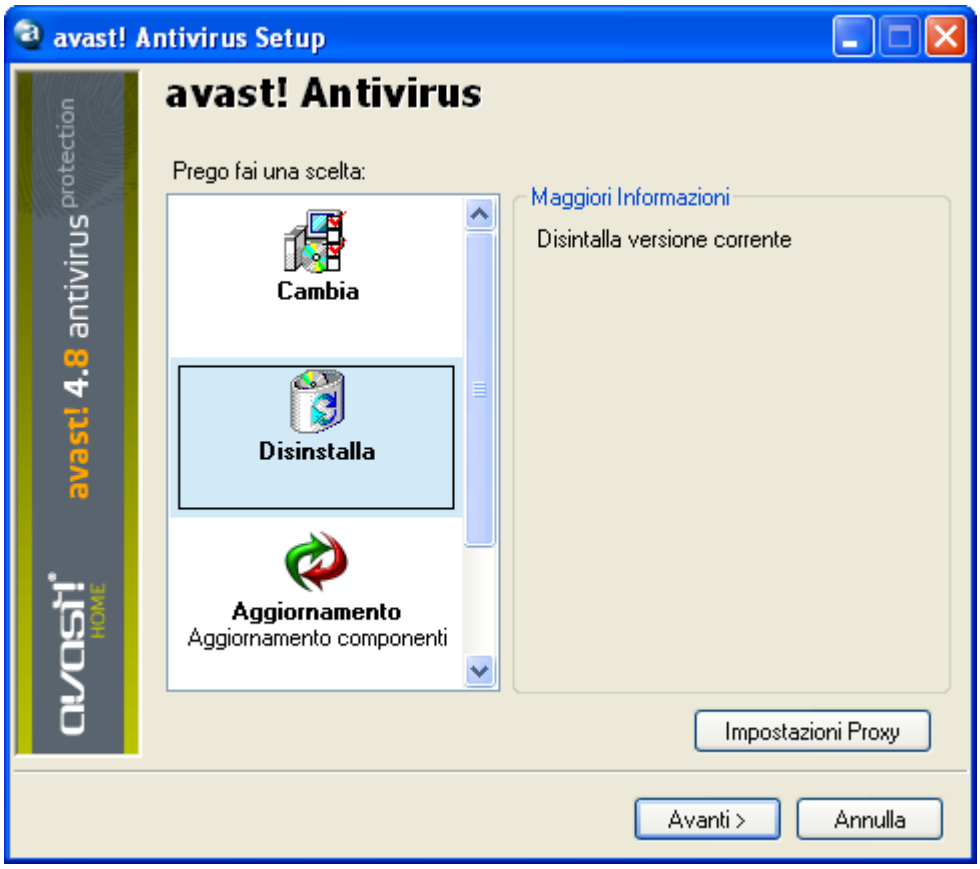
- Cliccare su on "Risoluzione errori" (ultima opzione del menu).



- Selezionare ”Disattiva il modulo di autodifesa avast! and cliccare su “OK”
- Il modulo di autodifesa avast! è ora disattivato

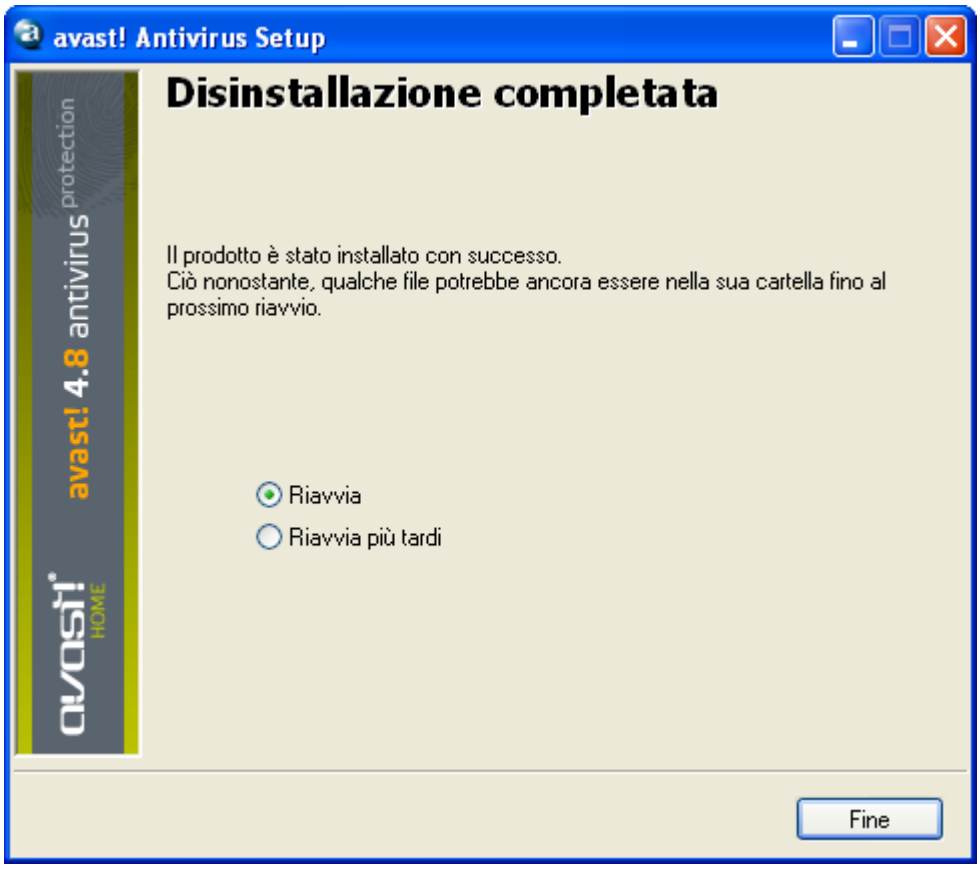
2. Rimozione del programma

- Cliccare su "Start" nell'angolo in basso a sinistra dello schermo del computer e aprire il pannello di controllo. Se non riuscite a vedere nel menu Start, basta cliccare su Impostazioni.
- Nel pannello di controllo cliccare su “Cambia/Rimuovi Programmi”.
- Viene visualizzato l’ elenco di tutti i programmi attualmente installati.
- Selezionare “avast! antivirus” cliccandoci sopra e quindi su “Cambia/Rimuovi”
- Apparirà la seguente schermata:



Cliccare su “Disinstalla” e poi su “Avanti”

Il programma sarà quindi disinstallato:



Per completare il processo di disinstallazione, è necessario riavviare il computer. Con "Riavvia" selezionato, cliccare su "Fine" e il computer viene automaticamente riavviato.